CONTRACT NUMBER PS66640
STATE OF NEW YORK AGREEMENT FOR HOSTED MARKETPLACE
CATALOG & E-INVOICING SOLUTION (STATEWIDE)
WITH PERFECT COMMERCE, LLC
AMENDMENT #1

THIS AMENDMENT (hereinafter Amendment #1) is made as of this 27 day of January, 2016 by and between the State of New York, acting by and through the Office of General Services (hereinafter "OGS" or the "State"), with offices at 41st Floor, Corning Tower, The Governor Nelson A. Rockefeller Empire State Plaza, Albany, New York, 12242 and Perfect Commerce, LLC (hereinafter "Contractor"), with offices at One Compass Way, Suite 120, Newport News, VA 23606. The State and the Contractor are collectively referred to as the "Parties."

WHEREAS, the Parties entered into the above referenced Contract, effective October 20, 2014 (the "Contract"), for a Hosted Marketplace Catalog & e-Invoicing Solution; and

WHEREAS, the Parties now wish to amend the Contract as set forth below; and

NOW, THEREFORE, in consideration of the mutual covenants, terms and conditions set forth in this Amendment #1, the Parties agree to the following amendment to the Contract:

1. The Parties agree that the last paragraph of Section 4.10, *Payment Schedule*, is deleted and replaced with the following:

   Notwithstanding the foregoing, Contractor or the State may request that any Deliverable or any individual task within a Deliverable be delivered in a different order than the Payment Schedule identified in this section. Upon the mutual written agreement of the Parties, which may be evidenced by email, and subject to the approval of the Catalog MarketPlace and eInvoicing Committee, which shall not be unreasonably withheld and also may be evidenced by email, the Payment Schedule may be amended in accordance with such requested and approved changes.

   Notwithstanding the foregoing, the parties accept the following modifications:

Deliverable	**Sub-deliverable**	**Status/Change**
Deliverable 1: Modified Implementation Plan	No changes	Completed and Accepted. Paid Invoice Number PCI-0000025223

Deliverable 2: Interfaces with SFS and FileNet	Interface with SFS: Catalog Integration and return shopping cart to SFS, Dispatch PO from SFS to Perfect Commerce, Deliver PO to Supplier, Return POR Acceptance or Rejection to SFS	Completed and Accepted. Billed July 31, 2015 Invoice Number PCI-0000026104.*
	Interface with FileNet	Moved to Deliverable 8.
Deliverable 3: MarketPlace Catalog	Provide General functionality: searches, filters, variables, user display and functionality	Completed and Accepted. Billed July 1, 2015 Invoice Number PCI-0000025973.*
	Provide sample punchout catalog with a live supplier	
	Develop State Marketplace catalog	
	Provide access to catalog via SFS	
	Provide access to catalog and payment via PCard	
	Conduct live website demonstration of functionality	
	Provide standard reporting	Validation by OGS is Tabled/Moved to Deliverable #8
	Contract Manager review, edit and change functionality workflow	Completed
	Provide Supplier registration review, edit and change functionality workflow	Completed and Accepted. Billed July 1, 2015 Invoice Number PCI-0000025973.*
	Completed User Acceptance Test and identified defects	
	Resolved Critical defects from User Acceptance test	
	Functionality requests identified and tracked	
	Data verified – Catalog Content	
Deliverable 4: eInvoicing	Supplier registration and submittal of invoices in multiple formats - e.g., purchase order (PO) flip	Completed and Accepted. Billed July 31, 2015 Invoice

	Vendor interface	Number PCI-0000026104.*
	Out of the box reporting	Validation by OGS Tabled/Moved to Deliverable #8
	General functionality: searches, filters, variables, user display and functionality	Completed
	Acceptance of a non-PO invoice	Moved to Deliverable 8.
	Supplier and invoice for data validation for PO and non-PO invoices	Partially Completed. Moved to Deliverable 8.
	Ability to upload supporting documentation to an invoice, e.g., file attachment	
	Business rule development and integration	Completed and Accepted. Billed July 31, 2015 Invoice Number PCI-0000026104.*
	Invoice hold function	
	User Acceptance Test defects identified	
	User Acceptance Test critical defects resolved	
	New functionality requests identified and tracked	Tabled/Moved to Deliverable #8
	Supplier registration and submittal of invoices in multiple formats - e.g., purchase order (PO) flip	Completed.
Deliverable 5: System, Accessibility and Load Testing	No changes.	No updates.
Deliverable 6: Training and Communication	Add Sub-deliverables identified above in Deliverables 3 and 4.	No updates.
Deliverable 7: Go Live	No changes.	No updates.
Deliverable 8: Go Live Acceptance (Reserve Amount)	Add Sub-deliverables identified above in Deliverable 2.	No updates.
* Upon execution of this Amendment, these invoices are considered due.		

Except as herein modified, all other terms and conditions of the Contract shall remain in full force and effect.

IN WITNESS WHEREOF, each of the Parties hereto has caused this Amendment to be executed as of the date first written above, and the persons signing this Agreement represent and warrant that they are duly authorized to sign on behalf of the respective Parties.

PERFECT COMMERCE, LLC.

By: _____

NAME: Charles Shannon
TITLE: COO
DATE: 1/27/16

THE STATE OF NEW YORK

By: _____

NAME:
TITLE:
DATE:

Susan M. Filburn
Deputy Chief Procurement Officer
1/29/2016

INDIVIDUAL, CORPORATION, PARTNERSHIP, OR LLC ACKNOWLEDGMENT

STATE OF Virginia }
: **SS.:**
COUNTY OF Newport News }

On the 27 day of January in the year 2016, before me personally appeared Charles Shannon, known to me to be the person who executed the foregoing instrument, who, being duly sworn by me did depose and say that _he maintains an office at Newport News, City/Town of Newport News, County of Neport News, State of Virginia; and further that:

[Check One]

(☐ **If an individual):** _he executed the foregoing instrument in his/her name and on his/her own behalf.

(☐ **If a corporation):** _he is the _____ of _____, the corporation described in said instrument; that, by authority of the Board of Directors of said corporation, _he is authorized to execute the foregoing instrument on behalf of the corporation for purposes set forth therein; and that, pursuant to that authority, _he executed the foregoing instrument in the name of and on behalf of said corporation as the act and deed of said corporation.

(☐ **If a partnership):** _he is the _____ of _____, the partnership described in said instrument; that, by the terms of said partnership, _he is authorized to execute the foregoing instrument on behalf of the partnership for purposes set forth therein; and that, pursuant to that authority, _he executed the foregoing instrument in the name of and on behalf of said partnership as the act and deed of said partnership.

(☑ **If a limited liability company):** _he is a duly authorized member of Perfect Commerce Holdings, LLC, the limited liability company described in said instrument; that _he is authorized to execute the foregoing instrument on behalf of the limited liability company for purposes set forth therein; and that, pursuant to that authority, _he executed the foregoing instrument in the name of and on behalf of said limited liability company as the act and deed of said limited liability company.

Sworn to me before this 27 day of January, 2016

MICHELLE D. MCMILLAN
NOTARY PUBLIC
REG. #202151
COMMONWEALTH OF VIRGINIA
MY COMMISSION EXPIRES SEPT. 30, 2019

Notary Public
Registration No.

AGREEMENT FOR

HOSTED MARKETPLACE CATALOG &

E-INVOICING SOLUTION (STATEWIDE)

BY AND BETWEEN

NEW YORK STATE

OFFICE OF GENERAL SERVICES

AND

PERFECT COMMERCE LLC

CONTRACT NUMBER PS66640

Table of Contents

1. OVERVIEW 6

1.1 OVERVIEW 6
1.2 SCOPE 6
1.3 CURRENT ENVIRONMENT 7
1.4 CONTRACT PERIOD AND RENEWALS 8
1.5 DEFINITIONS 8

2. CONTRACT TERMS AND CONDITIONS 11

2.1 CONFLICT OF TERMS 11
2.2 APPENDIX A 11
2.3 APPENDIX B 11
2.4 APPENDIX C 13
2.5 APPENDIX D 13
2.6 CONTRACTOR REQUIREMENTS 14
2.7 SCOPE OF PROJECT SERVICES 16
2.8 PARTICIPATION BY MINORITY GROUP MEMBERS AND WOMEN WITH RESPECT TO STATE CONTRACTS: REQUIREMENTS AND PROCEDURES 18
2.9 AUTHORITY 21
2.10 SHORT TERM EXTENSION 21
2.11 EXTENSION OF USE 21
2.12 EXTENSION OF USE COMMITMENT 21
2.13 CENTRALIZED CONTRACT MODIFICATIONS 22
2.14 PERFORMANCE AND BID BONDS 22
2.15 NON-STATE AGENCIES PARTICIPATION IN CENTRALIZED CONTRACTS 22
2.16 NEW YORK STATE VENDOR RESPONSIBILITY QUESTIONNAIRE FOR-PROFIT BUSINESS ENTITY 22
2.17 NOTE TO AUTHORIZED USERS 23
2.18 POOR PERFORMANCE 23
2.19 CONTRACT ADVERTISING 23
2.20 OVERLAPPING CONTRACT ITEMS 24
2.21 WEB ACCESSABILITY 24
2.22 SECURITY 24
2.23 ADDITIONAL REQUIREMENTS 26
2.24 INSURANCE REQUIREMENTS 26
2.25 EMERGENCY PURCHASING 26
2.26 TAX LAW SECTION 5-A 27
2.27 EMPLOYEE INFORMATION REQUIRED TO BE REPORTED FOR CERTAIN CONSULTANT CONTRACTORS AND SERVICE CONTRACTORS 27
2.28 CONTRACT CANCELLATION 29

3 PROJECT PHASES 29

3.1 IMPLEMENTATION CONSIDERATIONS 29
3.2 PROPOSED PHASES 29
3.3 CONTINUAL SOLUTION SUPPORT 29
3.4 PAYMENT TERMS AND INCENTIVES 29
3.5 ACCEPTANCE CRITERIA 29
3.6 WARRANTY PERIOD 29

4 DELIVERABLES (LOT I) AND PAYMENT SCHEDULE 30

4.1 OVERVIEW 30
4.2 DELIVERABLE #1: Modified Implementation Plan 30
4.3 DELIVERABLE #2: Interfaces with SFS and FileNet 30
4.4 DELIVERABLE #3: MarketPlace Catalog 30
4.5 DELIVERABLE #4: eInvoicing 30
4.6 DELIVERABLE #5: System, Accessibility and Load Testing 31
4.7 DELIVERABLE #6: Training and Communication 31
4.8 DELIVERABLE #7: Go Live 31
4.9 DELIVERABLE #8: Go Live Acceptance 31

4.10 PAYMENT SCHEDULE 32
4.11 PRICING SCHEDULE 32
4.12 PRICING UPDATES 33
4.13 LOWER PRICING 33

5 PROJECT MANAGEMENT 33

5.1 PROJECT OVERSIGHT 33
5.2 APPROVAL ROLE 33
5.3 PROJECT ROLES AND RESPONSIBILITIES 33
5.3.1 STATE PROJECT MANAGER 33
5.3.2 CONTRACTOR PROJECT MANAGER 33
5.3.3 CONTRACTOR ENGAGEMENT MANAGER 34
5.3.4 ANTICIPATED STAFFING ROLES 34
5.3.5 STAFF MANAGEMENT 34
5.4 PROJECT PLAN MANAGEMENT 34
5.5 COMMUNICATIONS MANAGEMENT 35
5.6 ISSUE MANAGEMENT 35
5.7 RISK MANAGEMENT 35
5.8 CHANGE MANAGEMENT PROCESS 35

6 SAAS TERMS AND CONDITIONS 36

6.1 SAAS PRODUCTS ACCESS 36
6.2 SCOPE, AVAILABILITY AND MODIFICATIONS 36
6.3 PROPRIETARY RIGHTS 37
6.4 TERMINATION/SUSPENSION 37
6.5 RETURN OF MATERIAL 38
6.6 SERVICE LEVEL AGREEMENT AND PENALTIES 38
6.7 STATEMENTS OF WORK (LOT II) 38
6.8 NO IMPLIED WARRANTIES 38
6.9 IP INDEMNIFICATION 38
6.10 SOURCE CODE ESCROW 38
6.11 SAAS AND DATA SECURITY 38

7 GENERAL PROVISIONS 39

7.1 NOTICES 39
7.2 CAPTIONS 39
7.3 SEVERABILITY 39
7.4 COUNTERPARTS 39
7.5 ENTIRE AGREEMENT 39

CONTRACTOR SIGNATURE PAGE 40

APPENDICES

APPENDIX A – *Standard Clauses for New York State Contracts (January 2014)*

APPENDIX B – *General Specifications (June 2014)*

APPENDIX C – *Pricing Schedule*

APPENDIX D – *Service Level Agreement*

APPENDIX E – *Minority and Women-Owned Business Enterprises and Equal Employment Opportunity Policy Statement*

APPENDIX F – *Insurance Requirements*

APPENDIX G – *Implementation Plan*

APPENDIX H – *Consensus Assessment Initiative Questionnaire (CAIQ) v.1.1*

APPENDIX I – *Contract Modification Procedures*

STATE OF NEW YORK
OFFICE OF GENERAL SERVICES
AGREEMENT #PS66640
CENTRALIZED CONTRACT FOR HOSTED MARKETPLACE
CATALOG & E-INVOICING SOLUTION

THIS AGREEMENT (hereinafter the "Contract" or the "Agreement") is made by and between the People of the State of New York, acting by and through the Commissioner of the Office of General Services (OGS), whose office is on the 41st Floor, Tower Building, Governor Nelson A. Rockefeller Empire State Plaza, Albany, New York 12242 (hereinafter referred to as the "State" or "OGS") and Perfect Commerce LLC, having its principal place of business at One Compass Way, Suite 120, Newport News, VA 23606, (hereinafter referred to as the "Contractor"). OGS and the Contractor are collectively referred to as the "Parties."

WHEREAS, OGS is statutorily authorized to enter into centralized procurement contracts for services for use by New York State agencies, departments, public authorities, political subdivisions and any other entities authorized by statute to utilize its centralized contracts (hereinafter "Authorized Users"), and

WHEREAS, OGS has identified a need by New York State agencies and other Authorized Users for a centralized contract for a Hosted MarketPlace Catalog and eInvoicing Solution, as further described herein, and

WHEREAS, OGS issued a solicitation, referred to as Request for Proposal #22816 ("the RFP") for a Hosted MarketPlace Catalog and eInvoicing Solution, which was advertised on April 24, 2014 in the New York State Contract Reporter, as required by New York State Economic Development Law, and

WHEREAS, OGS conducted a competitive procurement to identify the bidder which could provide the Hosted MarketPlace Catalog & eInvoicing Solution at the best value, and

WHEREAS, one award was made to the bidder who submitted the best value responsive proposal, and

WHEREAS, the State has determined: that the Contractor submitted the best value responsive proposal; that the Contractor is a responsible vendor; and that the Contractor is willing to provide the services set forth herein under the terms and conditions contained herein, and

NOW THEREFORE, in consideration of the terms contained herein and the mutual covenants and obligations moving to each party hereto from the other, the Parties hereby agree as follows:

1. OVERVIEW

1.1 OVERVIEW

This Contract sets forth the terms and conditions for the provision of a Hosted MarketPlace Catalog and eInvoicing Solution from Contractor to Authorized Users of the Contract on a statewide basis. References to the State and its Agencies or Non-State Agencies as Authorized Users under this centralized Contract encompass and include all such entities within the definition of "Authorized User" set forth in State Finance Law §163(1)(k). This Contract is comprised of two (2) Lots, which are specified below and described in further detail herein.

1.2 SCOPE

Lot I – Under Lot I, the Contractor will establish, operate and maintain a Hosted MarketPlace Catalog Site for use by New York State agencies, municipalities and other Authorized Users to seamlessly purchase goods and services from NYSPro centralized contract suppliers in one collaborative online environment that will interface with New York State's existing Statewide Financial System (SFS). The SFS system is a customized on-premise solution based on a PeopleSoft 9.0 platform. The Contractor's solution will also automate accounts payable through an Electronic Purchase Order (PO) dispatch and supplier invoice submission (eInvoicing) solution for use by the Business Services Center (BSC) that will interface with SFS and the State's document management solution, IBM FileNet P8 Content Manager 5.1. The eInvoicing solution will enable suppliers to submit invoices to the State electronically and provide reporting capabilities to enable the State to track purchases and electronic invoices. The solutions procured under this Contract are intended to work with, not replace, SFS. The solutions will:

- Create a more efficient and streamlined procurement business process
- Access and purchase from statewide contracted supplier catalogs via an online site
- Provide better management of statewide contract suppliers, products, items and pricing
- Better analyze spend data to identify best savings opportunities
- Create paperless invoicing and invoice processing by enabling suppliers to submit invoices electronically
- Create the ability to process invoices with greater efficiency and accuracy, supporting timely payment settlement

Lot II – Under Lot II, Authorized Users will have the option to implement their own "end-to-end" procurement solution which will include the Contractor's full menu of offerings. Under this Lot, New York State Agencies or other Authorized Users will be able to establish their own MarketPlace Catalog Site or purchase from a full menu of end-to-end procurement solutions offered by the Contractor on a centralized Contract basis. The Contractor's full menu of offerings will include, but is not limited to:

- eSourcing – automated sourcing or bid process
- Contract Management – automated supplier contracting process
- Vendor Management – automated supplier validation, documentation and tracking
- MarketPlace Catalog – establish an online hosted catalog site of goods and/or services
- Purchase Requisition – the integration with online vendor catalogs, which includes approving products, displaying pricing and contract terms
- Requisition Approval – once a purchase requisition is created, it is routed for approval based on the business rules and criteria defined by the Authorized User
- Workflow Management – the management, creation of user roles, rights and permissions to follow defined business rules
- Purchase Order Delivery – the creation of Purchase Orders from approved requisitions and transmission of orders from Authorized Users to suppliers.
- Receiving and Reconciliation – flipping Purchase Orders into invoices and/or delivering invoices to the Authorized Users in an automated goods receipt and reconciliation process. This includes the

enablement of two or three way matching between Purchase Orders, invoices and goods receipt documents.

- Reporting and Analysis – the ability of the solution to generate standard and customized queries and reports providing visibility into the transactions across Authorized Users and suppliers.

1.3 CURRENT ENVIRONMENT

Statewide Financial System (SFS)

New York State is currently operating on an Enterprise Resource Planning (ERP) system that is Oracle's PeopleSoft software, which is referred to as the Statewide Financial System (SFS). SFS is currently on PeopleSoft Financials version 9.0 Bundle 18, operating on PeopleTools version 8.49.33. The State is planning to upgrade to PeopleSoft Financials version 9.2, operating on PeopleTools version 8.53 by approximately April, 2015, with a "freeze" period (no changes to version 9.0) planned prior to such date. SFS supports requisition-to-payment processing and financial management functions. The eProcurement application specifically supports the requisitioning process for State Agencies to procure goods and services. The application provides catalog integration capabilities; however, the State is not currently utilizing this functionality to support the requisition creation process. The State will be implementing the PeopleSoft Inventory module in the near future to track inventory items within the item master table. Further information regarding business processes, interfaces, and file layouts may be found at: www.sfs.ny.gov and http://www.osc.state.ny.us/agencies/guide/MyWebHelp/.

Purchasing Process Overview

At Present, NYSPro manages approximately 1300 centralized procurements, which includes contracts that have been awarded to multiple vendors. NYSPro also supports contracting activities for over 60 State Agencies, as well as approximately 4,000 local government entities and other Authorized Users.

The acquisition mechanism and buying function for State Agencies is generally decentralized with each agency responsible for individual interaction with contractors. Requests for goods and services are generally processed via the State's PeopleSoft eProcurement application. State Agencies are currently not required to utilize the eProcurement requisition application unless the agency is being supported by the Business Services Center (BSC). However, agencies are required to generate purchase orders when buying from centralized contracts unless certain criteria exist (e.g., transactions fall under a certain dollar threshold), in which case, goods and services may be purchased and settled directly via Procurement Cards (P-Card).

NYSPro has implemented leading practices to support the State's mission to deliver and sustain savings to taxpayers. To support this initiative, it is critical that reporting metrics be captured to track purchases made to suppliers against statewide contracts.

The State is able to capture certain contract spending metrics against purchases made by State Agencies that are processed through the SFS. The State is able to track spending by capturing the vendor contract number on purchase order and voucher transactions; however the vendor contract number cannot be captured on transactions settled via Procurement Card (P-Card). In addition, local government entities do not utilize the SFS and must purchase directly from centralized contracts, thus NYS is unable to track spend against such purchases and must rely on metrics provided from the suppliers themselves. In order to procure goods and services at the best prices, as well as achieve savings goals, the State must be able to capture the most accurate contract spending metrics possible.

Invoice Process Overview

The BSC is intended to be New York's central office for processing human resource and financial transactions on behalf of over 64 State Agencies. Currently, the BSC has approximately 90 FTEs that manually process an estimated 15,000 invoices, 3250 utilities vouchers, 8250 PO vouchers, and 3500 inter-agency vouchers per month. Once all agencies are on-boarded by the end of 2014, the BSC accounts payable service line is projected to have 450 staff processing slightly less than 57,000 invoices per month. NYS Prompt Payment guidelines require invoices to be paid in accordance with State Finance Law.

The state's accounts payable business process consists of invoice receipt, scanning/imaging, routing to agencies for approval to pay/inquiries, data entry in the SFS Accounts Payable (A/P) module, 2-Way and 3-Way matching

(PO vouchers only), budget checking (automated in SFS), release for payment disbursement and posting accounting entries to the SFS General Ledger. Currently it is a manual, paper-based process.

Fiscal Year	Estimated Number of Invoices
2012-13	165,000
2013-14	615,000 – 750,000
2014-15	675,000 – 825,000
2015-16	675,000 – 825,000

1.4 CONTRACT PERIOD AND RENEWALS

This Contract shall commence after receipt of all necessary approvals, and shall become effective upon mailing of final Contract Award Notice by OGS in accordance with Appendix B § 26(i), *Contract Creation/Execution*. The Contract shall be in effect for a term of two (2) years. If mutually agreed between OGS and the Contractor, the Contract may be renewed, under the same terms and conditions, for up to one (1) additional five (5) year period, not to exceed a total Contract term of seven (7) years.

1.5 DEFINITIONS

Terms used in this Contract or Attachments that have a capitalized first letter shall be defined in accordance with Appendix B, § 2, *Definitions*. In addition, the following definitions shall apply:

"Ability to" means capable of. Certain abilities or functionalities are dependent upon Supplier cooperation to enable.

"Authorized Administrator" shall refer to an individual who is an authorized power user of the SaaS solution on behalf of a State Agency or other Authorized User entity.

"Authorized User" shall have the same meaning as that term is defined in Appendix B, §2, Definitions.

"Business Services Center (BSC)" shall refer to a division of the New York State Office of General Services that serves as New York's central office for processing HR and finance transitions on behalf of Executive State Agencies.

"Business Day" shall refer to Monday through Friday from 8:00 AM – 5:00 PM ET, excluding New York State or Federal holidays.

"CAIQ" shall refer to the Consensus Assessments Initiative Questionnaire v.1.1, as established by the Cloud Security Alliance (CSA). Contractor's response to the CAIQ Questionnaire is included as Appendix H of the Contract.

"Content" means any data, information or materials provided to Contractor by a Supplier including, parametric information regarding products such as item descriptions, product and service attributes, units of measures, categories, price, payment methods, photographs, drawings, audio, video, technical specifications, and any associated marketing literature or point of purchase information, including any updates, revisions, and corrections thereto. Content does not include Transaction Information.

"Contract" shall refer to the final version of any contractually binding agreement between the State and the Contractor relating to the subject matter of RFP #22816; references to the Contract include all exhibits, attachments and other documents attached thereto or incorporated therein by reference.

"Contractor" shall refer to the entity which has submitted a bid in response to the RFP and has been awarded a contract and has executed a contract with the State.

"Critical Defect" shall refer to a defect that causes the SaaS Product to be unavailable or a defect in significant functionality of the SaaS Product that causes operations to cease because no workaround exists.

"Deliverable" shall refer to a project outcome or output to be achieved, produced or provided by Contractor as part of its responsibilities under the Contract. Lot I deliverables are specified in Section 4 of this Contract. Lot II deliverables will be established and identified in any applicable Statement of Work.

"DOB" shall refer to the New York State Division of the Budget.

"EEO" shall refer to Equal Employment Opportunity.

"Electronic Invoicing (eInvoicing)" shall refer to the ability for statewide contracted suppliers to submit standardized invoices electronically to the State which may be via a third party solution that provides the technological capability to integrate invoices with the NYS Statewide Financial System (SFS), PeopleSoft (version 9.x) Accounts Payable module and FileNet.

"Enterprise Resource Planning (ERP)" shall refer to all software applications used to integrate internal and external management of information across all State agencies.

"ET" shall refer to prevailing Eastern Standard Time.

"FileNet" shall refer to the State's document management solution - IBM FileNet P8 Content Manager 5.1.

"Intellectual Property Rights" means any patent rights, copyrights, trade secrets, trade names, service marks, trademarks, moral rights, know-how and any other similar rights or intangible assets recognized under any laws or international conventions, and in any country or jurisdiction in the world, as intellectual creations to which rights of ownership accrue, and all registrations, applications, disclosures, renewals, extensions, continuations or reissues of the foregoing now or hereafter in force.

"ITS" shall refer to the New York State Information Technology Services.

"Lot" shall refer to a subcategory of RFP #22816 and this resulting Contract, as further described herein.

"Marketplace Catalog (eCatalog)" shall refer to a seamless, online "Marketplace Shopping Site" available for all State entities to view and purchase goods and services from statewide contracted suppliers.

"MarketPlace Catalog and eInvoicing Committee" shall refer to a committee which will include staff from New York State Procurement (NYSPro), the Business Services Center (BSC), Information Technology Services (ITS), the Division of the Budget (DOB) and the Statewide Financial System (SFS), and will serve as the overall governance of this implementation.

"Market Statistics" means aggregated, non-attributable statistical information associated with Transaction Information, but does not include information or the presentation of information from which could be reasonably determined: (a) the identity of specific transactions or parties, (b) Transaction Information, or (c) SKU-level pricing contained in specific Content.

"M/WBE" shall refer to a business certified with Empire State Development (ESD) as a Minority and/or Women-owned Business Enterprise.

"May" denotes the permissive in a clause or specification of the RFP or this Contract. Also see "Must," "Should," and "Shall."

"Must" denotes the imperative in a clause or specification of the RFP or this Contract. "Must" is synonymous with "required." Also see "Shall," "Should," and "May."

"N/A" is a common abbreviation for *not applicable* or *not available*, used to indicate when information in a certain field or on a table is not provided, either because it does not apply to a particular case in question or because it is not available.

"New York State Procurement (NYSPro)"(formerly known as Procurement Services Group (PSG)" shall mean a division of the New York State Office of General Services which is authorized by law to issue centralized, statewide contracts for use by New York agencies, political subdivisions, schools, libraries and others authorized by law to participate in such contracts.

"Non-State Agencies" shall refer to political subdivisions and other entities authorized by law to make purchases from New York State centralized contracts other than those entities that qualify as State Agencies. This includes all entities permitted to participate in centralized contracts per Appendix B, §27(b), *Non-State Agency Authorized Users* and §27(c), *Voluntary Extension* and State Finance Law Section 163(1)(k).

"NYS Holidays" shall refer to the legal holidays for State Employees in the Classified Service of the Executive Branch, as more particularly specified on the website of the NYS Department of Civil Service. This includes the following: New Year's Day; Martin Luther King Day; Washington's Birthday (observed); Memorial Day; Independence Day; Labor Day; Columbus Day; Veteran's Day; Thanksgiving Day; and Christmas Day. Available at: http://www.cs.ny.gov/attendance_leave/TM_39.cfm

"NYS Vendor ID" shall refer to the ten-character identifier issued by New York State when a Contractor or vendor is registered on the Vendor File.

"OGS" shall refer to the New York State Office of General Services.

"OSC" shall refer to the New York State Office of the State Comptroller.

"Payment Card Industry Data Security Standards (PCI-DSS)" shall refer to the standards set forth by the Payment Card Industry Standards Council, with more information available at: https://www.pcisecuritystandards.org.

"Procurement Card (P-Card)" shall refer to a method of procuring goods and services and settling the purchases by New York State Agencies and other Authorized Users.

"Project Manager (PM)" shall refer to the individual assigned to lead the project and oversee the completion of all work under the project.

"Preferred Source" shall refer to a designation maintained by certain New York State vendors, contractors, or suppliers. All State agencies, political subdivisions and public benefit corporations (which includes most public authorities), are required to purchase certain approved products and services from preferred sources in accordance with the procedures and requirements described in the Preferred Source Guidelines, available at: http://www.ogs.ny.gov/procurecounc/pdfdoc/psguide.pdf

"Punch-out" shall refer to the industry accepted seamless process of leaving the hosted catalog environment to allow the user to shop in a Supplier hosted catalog designated by Supplier and then return the shopping basket back into the hosted catalog shopping environment.

"Records" shall have the meaning defined in Appendix A, except that such definition shall only apply to Appendix A and shall exclude any Content and Transaction Information which is not directly pertinent to Contractor's performance under the Contract.

"Software as a Service (SaaS)" shall refer to a multi-tenant software delivery model in which software and associated data are centrally hosted, maintained, and updated on the cloud and accessed via a web browser. The software applications will be hosted by the Contractor where the State does not take ownership of the software and is instead purchasing access to the application and support via the Internet. "Software as a Service" may also be referred to as "Software as a Solution."

"SaaS Product" or "SaaS Products" means the Software as a Service products provided by Contractor and Affiliates to the State and/or Authorized Users pursuant to this Contract and as described herein, including any successor or replacement services offering the same or more functionality than its predecessor.

"Small Business Enterprise (SBE)" shall refer to a "New York State Small Business," which is defined as a company that is a resident to New York State, independently owned and operated, with 100 or fewer employees, and not dominant in its field. See State Finance Law §160(8).

"System Development Life Cycle (SDLC)" shall refer to, at a minimum, the planning, design, build, training, testing, deployment, and project closeout cycle of a software implementation solution.

"Statewide Financial System (SFS)" shall refer to the New York State Enterprise Resource Planning (ERP) system that is Oracle's PeopleSoft software.

"Shall" denotes the imperative in a clause or specification of the RFP or this Contract. "Shall" is synonymous with "required." Also see "Must," "Should," and "May."

"Should" denotes the permissive in a clause or specification of the RFP or this Contract. Also see "May," "Shall," and "Must."

"Service Level Agreement (SLA)" shall refer to a negotiated agreement between the Contractor and the State that contains service performance metrics with corresponding service level objectives.

"Solution" shall refer to the Contractor's proposed products and/or services to be provided to the State under this Contract.

"Statement of Work (SOW)" shall refer to a description of products, services and/or deliverables to be provided by the Contractor to an Authorized User under this Contract. Statements of Work will be required under Lot II of this Contract.

"State" shall refer to the State of New York.

"State Agency or State Agencies" shall have the same meaning as "Agency" or "Agencies" in Appendix B, §2, Definitions.

"Supplier" shall refer to an existing holder of an OGS Centralized contract, a preferred source vendor designated by the State, or a utility company or other entity that holds an agreement with the State.

"Transaction Information" means the specific pricing, quantities, parties and terms and conditions of any contract, order, bid or proposal disclosed directly or indirectly to Contractor through the use of the SaaS Products, but shall not include any information which was at the time of disclosure intended to be disclosed by Contractor to a bidder or other intended recipient on behalf of the Authorized User.

2. CONTRACT TERMS AND CONDITIONS

This section sets forth the terms and conditions of the Contract.

2.1 CONFLICT OF TERMS

Conflicts among the documents shall be resolved in the following order of precedence:

A. Appendix A, *Standard Clauses for New York State Contracts*;
B. The base Contract (the portion of this document preceding the signature of the parties);
C. Appendix B, *General Specifications*;
D. Appendix C, *Pricing Schedule;*
E. Appendix D, *Service Level Agreement, and*
F. Appendix E, *Minority and Women-Owned Business Enterprises and Equal Employment Opportunity Policy Statement*
G. Other attachments and appendices as deemed necessary

2.2 APPENDIX A

Appendix A, *Standard Clauses for New York State Contracts*, dated January 2014, attached hereto, is hereby expressly made a part of this Contract as fully as if set forth at length herein.

2.3 APPENDIX B

Appendix B, *Office of General Services General Specifications*, dated June 2014, attached hereto, is hereby expressly made a part of this Contract as fully as if set forth at length herein.

2.3.1 APPENDIX B AMENDMENTS

The following amendments are hereby made to Appendix B, *Office of General Services General Specifications*:

Section 10, *Prevailing Wage Rates – Public Works and Building Services Contracts*, paragraphs (c) and (d) are deleted in their entirety.

Section 15, *Remanufactured, Recycled, Recyclable or Recovered Materials*, is deleted in its entirety.

Section 17(f), *Best Pricing Offer*, is amended as follows:

During the Contract term, if substantially the same Product is sold by the Contractor outside of this Contract upon the same or similar terms and conditions as this Contract at a lower price to a U.S. federal, state or local governmental entity of similar size and total annual operating budget and with a similar scope of work, then the ongoing price under this Contract, at the discretion of the Commissioner, shall be immediately reduced to the lower price.

Section 19, *Site Inspection*, is deleted in its entirety.

Section 21, *Samples*, is deleted in its entirety.

Section 35, *Shipping/Receipt of Product*, paragraphs (a) and (b) are deleted in their entirety.

Section 37, *Re-Weighing Product*, is deleted in its entirety.

Section 39, *Rejected Product*, is amended by adding the following:

Nothing in this Section 39 shall be deemed a property transfer or copyright license or other form of software license to any of Contractor's intellectual property.

Section 40, *Installation*, is deleted in its entirety.

Section 41, *Repaired or Replaced Parts*, is deleted in its entirety.

Section 45, *Performance/Bid Bond*, is deleted in its entirety.

Section 56, *Security*, is amended as follows:

Contractor warrants, covenants and represents that it will comply fully with all reasonable security procedures of the Authorized User(s) in performance of the Contract including but not limited to physical, facility, documentary and cyber security rules, procedures and protocols, provided that notice of such procedures has been given to Contractor.

Section 59, *Warranties*, is amended as follows:

The last paragraph of Section 59 (a), *Product Performance*, is deleted in its entirety.

Paragraph (c), *Product Warranty for Deliverables*, is amended as follows:

c. Product Warranty for Deliverables. During the Project warranty period, defects in the materials or workmanship of components or deliverables specified and furnished by or through Contractor shall be repaired or replaced by Contractor at no cost to the Authorized User.

Section 65, *Software/License Grant*, is deleted in its entirety.

Section 66, *Product Acceptance*, is amended as follows:

Unless otherwise provided by mutual agreement of the Authorized User and the Contractor, Authorized User(s) shall have sixty (60) days from the date of delivery to accept Products.

Unless otherwise provided by mutual agreement of the Authorized User and the Contractor, Authorized User shall have the option to run reasonable testing on the Product prior to acceptance, such reasonable tests and data sets to be specified by User. Where using its own data or tests, Authorized User must have the tests or representative set of data available upon delivery. This demonstration will take the form of a documented installation test, capable of observation by the Authorized User, and shall be made part

of the Contractor's standard documentation. The test data shall remain accessible to the Authorized User after completion of the test.

In the event that the documented installation test cannot be completed successfully within the specified acceptance period, and the Contractor or Product is responsible for the delay, Authorized User shall have the option to cancel the order in whole or in part, or to extend the testing period for an additional thirty (30) day increment. Authorized User shall notify Contractor of acceptance upon successful completion of the documented installation test. Such cancellation shall not give rise to any cause of action against the Authorized User for damages, loss of profits, expenses, or other remuneration of any kind.

If the Authorized User elects to provide a deficiency statement specifying how the Product fails to meet the reasonable specifications within the testing period, Contractor shall have thirty (30) days to correct the deficiency, and the Authorized User shall have an additional sixty (60) days to evaluate the Product as provided herein. If the Product does not meet the specifications at the end of the extended testing period, Authorized User, upon prior written notice to Contractor, may then reject the Product and return all defective Product to Contractor, and Contractor shall refund any monies paid by the Authorized User to Contractor therefor. Costs and liabilities associated with a failure of the Product to perform in accordance with the functionality tests or product specifications during the acceptance period shall be borne fully by Contractor to the extent that said costs or liabilities shall not have been caused by negligent or willful acts or omissions of the Authorized User's agents or employees. Said costs shall be limited to the amounts set forth in the Limitation of Liability Clause for any liability for costs incurred at the direction or recommendation of Contractor. When Product is not accepted, it must be removed by the Contractor from the premises of the Authorized User within ten calendar days of notification of non-acceptance by the Authorized User. Rejected items not removed by the Contractor within the ten calendar day period shall be regarded as abandoned by the Contractor and the Authorized User shall have the right to dispose of Product as its own property. The Contractor shall promptly reimburse the Authorized User for any costs incurred in storage or effecting removal or disposition after the ten calendar day period.

Section 67, *Audit of Licensed Product Usage*, is deleted in its entirety.

Section 68, *Ownership/Title to Project Deliverables*, is amended as follows:

Paragraph (b), *Title to Project Deliverables*, is amended as follows:

b. Title to Project Deliverables. Contractor acknowledges that it is commissioned by the Authorized User to perform the services detailed in the Purchase Order. Unless otherwise specified in writing in the Bid or Purchase Order, the Authorized User shall have ownership and license rights as follows:

Custom Products: Effective upon creation of Custom Products, Authorized User takes a non-exclusive perpetual license to Custom Products. In such case, Licensee on behalf of all Authorized Users shall be granted a non-exclusive perpetual license to use, execute, reproduce, display, and perform Custom Product.

Paragraphs (d), *Sale or License of Custom Products Involving Tax-Exempt Financing (i.e., Certificates of Participation - COPS)* and (e), *Contractor's Obligation with Regard to ISV (Third Party) Product* are deleted in their entirety.

Section 69, *Proof of License*, is deleted in its entirety.

2.4 APPENDIX C

Appendix C, *Pricing Schedule*, is hereby expressly made a part of this Contract as fully as if set forth at length herein.

2.5 APPENDIX D

Appendix D, *Service Level Agreement,* is hereby expressly made a part of this Contract as fully as if set forth at length herein.

2.6 CONTRACTOR REQUIREMENTS

The Solution implemented by the Contractor must comply with the following requirements:

1. Ability to integrate with PeopleSoft 9.x and establish a node-to-node interface with PeopleSoft Integration Broker using encrypted HTTP protocols (SSL/TLS) - (current is PeopleTools 8.53)
2. Ability to integrate with FileNet P8 Content Manager 5.1
3. Ability to establish a secure log-in mechanism, with credentials, for Authorized Users (e.g., Local Government users) to access the MarketPlace Catalog directly without navigating to the site via PeopleSoft
4. Ability to enable State SFS users to access the MarketPlace Catalog through a seamless integration via single sign-on access through PeopleSoft eProcurement module based on standard PeopleSoft User Management functionality
5. Ability to support roundtrip catalog punch-out requests originating from PeopleSoft through PeopleSoft Integration Broker and return back into the Statewide Financial System (SFS) with shopping cart information
6. Ability to create a requisition and transfer information, including but not limited to:
    - Item ID – Item number from the State's Item Master list
    - Unit Price – Contracted unit price for the items
    - Unit of Measure - as defined from the NYS Standard Unit of Measure Conversion List (dynamic)
    - Category Code – UNSPSC compliant and as defined by the NYS Item Master
    - Item Description – Description of the product (256 character limit)
    - Quantity – Quantity of items selected for order
    - Contract Supplier Item ID – Supplier specific item number
    - Contract Number – New York State assigned contract number
    - Contract Line
    - Quantity
7. Ability to provide an extract conforming to SFS PeopleSoft specifications to update the Item Master within PeopleSoft, provide Item Master updates to PeopleSoft using Catalog Interchange Format (CIF) standards, and provide updates through PeopleSoft enterprise integration points (EIP) ITEM_SYNC and ITEM_FULLSYNC
8. Ability to delineate and transmit electronic invoices into SFS PeopleSoft, using OAG protocols through PeopleSoft Integration Broker, and into FileNet (delineation will be whether the invoice is for the Business Service Center (FileNet) or other State agency (SFS))
9. Ability to accept and process PO and non-PO invoices, in multiple formats, including but not limited to XML, PDF, CSV, via a vendor hosted service solution and create an electronic invoice
10. Ability for suppliers to create and/or submit an invoice from an eCatalog transaction
11. Ability for the solution to enforce data validation on submitted electronic invoices for multiple data fields
12. Ability to convert lines on a single PO into multiple invoices
13. Ability for suppliers to upload supporting invoice related detail and attachments (such as packing slips), and associate these with an original invoice after the original submission (e.g., follow-up requested documentation)
14. Ability to customize business rules for invoice line items
15. Ability for the solution to transfer invoices real-time to the NYS Statewide Financial System (SFS), and batch in the case of real time failures or delays
16. Ability to create validation rules (e.g., identify duplicate invoices) and invoice rules (e.g., flag an invoice for special treatment) for eInvoices
17. Ability to search for invoices by multiple criteria, including but not limited to Supplier Name, Supplier ID, Line Items, PO# , Contract#, Agency, etc.
18. Ability to view and report on metrics in real time, including but not limited to invoice transaction events, changes in status, date, timestamp, etc.
19. Ability to provide an integration point from the supplier network to SFS PeopleSoft ERP System via a SaaS-based platform
20. Ability to provide online training to Authorized Users and suppliers, provide Train-the-Trainer sessions and publish/post online help and training materials to support the solution roll-out

21. Ability to create and implement formal, documented backup and redundancy measures to ensure continuity of service and preservation of State data
22. Ability to configure approval rules, requiring approval prior to settlement of transactions, for transactions to be settled via P-Card (e.g., municipalities, towns, cities, etc.)
23. Ability for Authorized Administrator(s) to maintain assigned catalog, to include: review and approve/reject contract item and price updates submitted by suppliers prior to placing updates into production, receive an electronic alert when a supplier initiates an action that requires approval (e.g., updated catalog content), maintain an archive of edits for catalogs, create a continuous queue for tasks to be completed, and act as a proxy for suppliers to upload a new catalog
24. Ability to configure controllable catalog views across the enterprise (e.g., associate the correct catalogs and/or items with the appropriate purchasing user/organization)
25. Ability to configure validation rules to ensure loaded supplier catalog data is in compliance with unit-of-measure standards, classifications, and other required data elements
26. Ability to group and organize items by commodity, UNSPC, NIGP code or other defined classification
27. Ability to configure and associate reportable attributes with supplier profile (e.g., MWBE, Veteran-owned, SBE, Preferred Source, etc.) and catalog items (e.g., lowest price).
28. Ability for item search results to be displayed at the top of the list based on preferred criteria (e.g., items from Preferred Source suppliers display at the top of the search results list followed by remaining supplier items)
29. Ability for NYS to post procurement information on the MarketPlace Catalog Homepage, including hyperlinks to other NYS procurement related websites (e.g., NYS OGS website)
30. Ability to have an established dashboard that includes item detail, including but not limited to the following examples: Contract number, Contract start date, Contract end date, Supplier item number, Volume discount price break for each item, Distributor name and number, Item specifications (could be a URL link), Recycled content percentage, Recycled content type, Manufacturer name, Manufacturer part number, Unit of measure, Alternate unit of measure, Minimum order quantity, Quantity, Geographic designation (County, State Highway District, Zone, other), Lead time for delivery, Shipping and handling requirements, Commodity codes/NIGP code, UPC code, Item code, Long description (at least 8,000 alphanumeric characters) per line item, Short description (at least 255 alphanumeric characters) per line item, Price and effective dates, Historical price information (e.g., YTD average price), Substitute/Alternate items, Agency and associate an image to a catalog item (as available), spend analytics and performance metrics
31. Ability to add, change or remove custom fields to be used for data capture (e.g., dates, free-form text, numeric values, currency values, etc.)
32. Ability to generate and/or export/print various reports (standard, custom and ad hoc), including: hosted MarketPlace Catalog purchasing data, supplier outsourcing data by attribute (e.g., MWBE, Veteran-Owned, SBE, Preferred Source), spend analytics and performance analytics
33. Ability to provide a standardized Excel/CSV catalog template to enable suppliers to upload catalog content to the site based on system requirements
34. Ability to allow Authorized Users to settle transactions via Procurement Card (P-Card)
35. Ability to filter and sort item search results view to include but not be limited to the following:
    - Supplier
    - Manufacturer
    - Category
    - Price Range
    - Attribute (e.g., MWBE, Veteran-owned, etc.)
    - Image (as applicable)
36. Ability to support tiered pricing, regional pricing, volume discounting structures, and minimum order quantity
37. Ability for items selected within a cart to be printed or downloaded to a file (e.g., Excel)
38. Ability for Authorized Users to save or maintain frequently purchased items (e.g., favorites) when returning to the site and create a new order
39. Ability to create and add a non-catalog line item to the shopping cart

40. Ability to search and view catalogs for items using natural language and including: keywords, filter, drill-down, view items, defined attributes (preferred sources, MWBE, etc.)
41. Ability to view supplier terms for catalog items (e.g., minimum order quantity)
42. Ability to search for an item and have the search results aggregated from all catalog sources display in a single list on the hosted catalog results page, and include images (as applicable) (e.g., item search results from hosted and punch-out sites can display in a single list)
43. Ability for Authorized User to hold, cancel or delete items in a shopping cart before submission (e.g., incomplete request)
44. Ability to provide an internet based application/web page to allow Authorized Users/Entities that do not utilize the State's PeopleSoft system to search and view all Statewide contract items and pricing
45. Ability to provide an online interface (e.g., portal) for suppliers to establish accounts, profiles and maintain their catalog data/content (pending Authorized Administrator(s) approval)
46. Ability to configure and maintain purchasing business rules (e.g., supplier priority, spending limits, etc.) when buying from hosted or punch-out catalogs
47. Ability to support formal issue resolution and tracking process for invoice problems (e.g., pricing errors, incorrect order), including required actions and status notifications
48. Ability to post or transmit messages to the supplier community and post procurement information including hyperlinks to other NYS procurement related websites (e.g., NYS OGS website)
49. Ability to create an eInvoice from a Purchase Order within one (1) business day unless an otherwise approved outage occurred
50. Ability to provide a change management approach, including but not limited to communication, knowledge transfer, change vision and strategy, change request management, transition planning, etc.

2.7 SCOPE OF PROJECT SERVICES

2.7.1 General

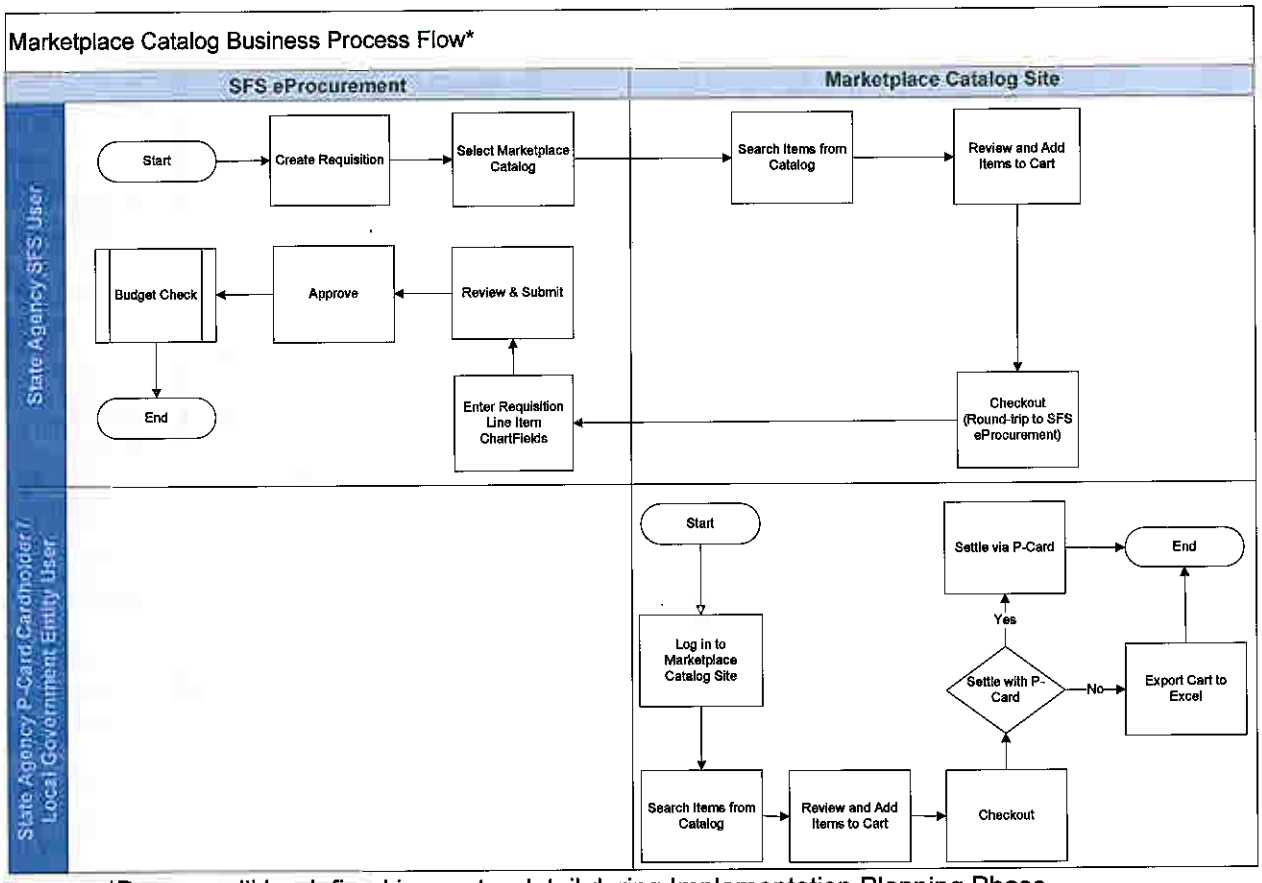
- The objectives of the Solution are to allow for State Agencies and other Authorized Users to efficiently manage their procurement and invoice business processes, to lower agency costs and optimize efficiencies by reducing staff time and streamlining business processes.
- The Contractor is expected to employ standard project management operating procedures to manage a successful implementation through all phases of the System Development Life Cycle (SDLC) and shall provide public sector specific application knowledge and expertise to the State.
- The Contractor is expected to implement the MarketPlace Catalog and eInvoicing solutions concurrently. The Contractor is required to comply with all information technology provisions as defined in Section 2.22.
- The Contractor shall make no changes to State systems or to interfaces with those systems without the express written permission of the State project management team.
- The Contractor shall be strictly prohibited from using State data in any manner other than as specifically required herein.

2.7.2 Hosted MarketPlace Catalog

The key objectives of the MarketPlace Catalog solution include:

- Establish an online hosted catalog site of goods and services provided by the State's centralized contract suppliers
- Provide technical capability to integrate the hosted catalog site functionality with the Statewide Financial System (SFS), PeopleSoft ERP (version 9.x) eProcurement software functionality
- Provide an internet based application/web page that will allow State entities that do not utilize the State's PeopleSoft system (i.e. local governments) to see all centralized contract pricing in the MarketPlace, and be able to purchase items from and settle transactions via Procurement Card (P-Card)
- Post all centralized contract information on the hosted catalog site to support a "one-stop-shop"
- Provide online catalog development, implementation, and maintenance to include establishing connections to State supplier punch-out sites
- Provide HelpDesk services and support for the online MarketPlace Catalog environment

The following diagram depicts the high-level business process flow for the MarketPlace Catalog solution*:



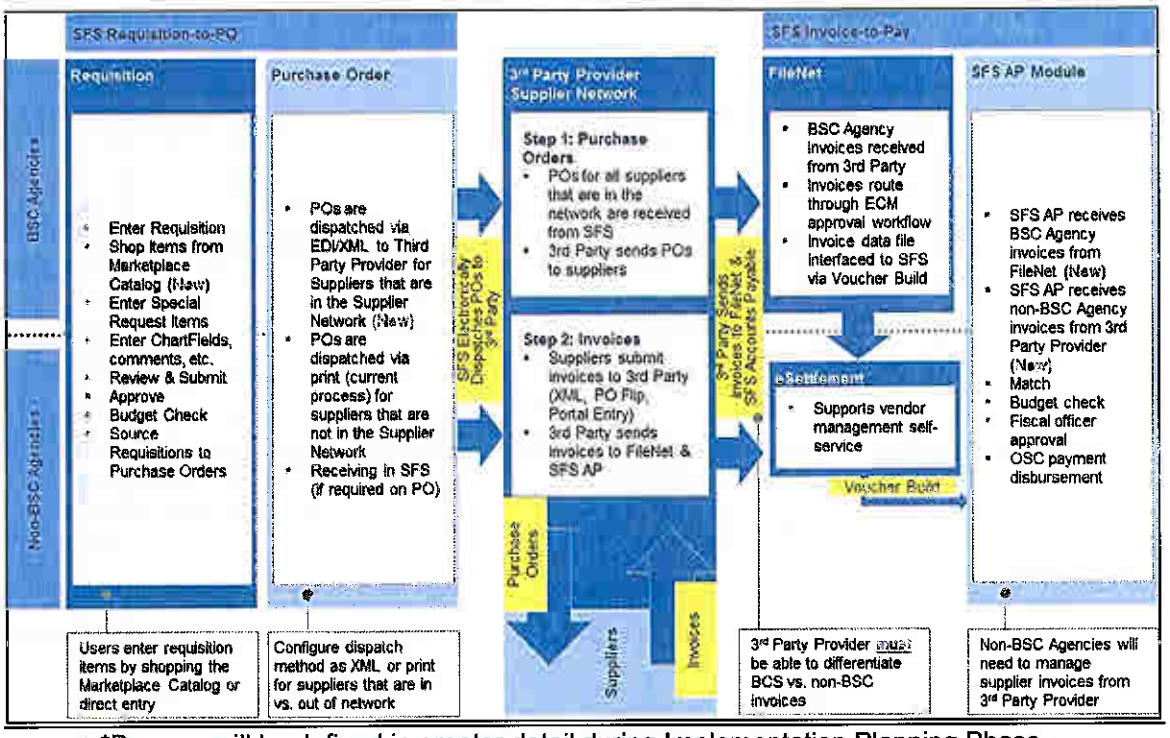
*Process will be defined in greater detail during Implementation Planning Phase

2.7.3 <u>eInvoicing and Management</u>

The key objectives of the eInvoicing solution include:

- Enable suppliers to submit standardized invoices electronically to the State
- Integrate invoices with the NYS Statewide Financial System (SFS), PeopleSoft (version 9.x) Accounts Payable module via the eSettlements module.
- Integrate with the State's document management solution, IBM FileNet P8 Content Manager 5.1.
- Provide outreach and support for NYS designated suppliers to engage and train them on the operation of the eInvoicing solution.
- Provide eInvoicing performance reporting and intelligence capabilities

The following diagram depicts the high-level business process flow for the eInvoicing solution*:



*Process will be defined in greater detail during Implementation Planning Phase

2.7.4 Reporting

The State is dedicated to reducing expenditures and improving operations to deliver and sustain savings to taxpayers. For this, it is critical that reporting metrics are captured. Reporting capabilities are integral to improving visibility into contract spend, evaluating vendor performance, ensuring compliance with State directives, and improving the accountability and audit ability for State contract purchases and invoices. It is the State's desire for the Statewide Financial System (SFS) to be the "one source of truth" for all data reporting and it is not the intent for State users to access reports from the MarketPlace Catalog and create shadow systems to capture and report on information separate from SFS.

2.8 PARTICIPATION BY MINORITY GROUP MEMBERS AND WOMEN WITH RESPECT TO STATE CONTRACTS: REQUIREMENTS AND PROCEDURES

I. General Provisions

A. OGS is required to implement the provisions of New York State Executive Law Article 15-A and 5 NYCRR Parts 142-144 ("MWBE Regulations") for all State contracts as defined therein, with a value (1) in excess of $25,000 for labor, services, equipment, materials, or any combination of the foregoing or (2) in excess of $100,000 for real property renovations and construction.

B. The Contractor agrees, in addition to any other nondiscrimination provision of the Contract and at no additional cost to OGS, to fully comply and cooperate with OGS in the implementation of New York State Executive Law Article 15-A. These requirements include equal employment opportunities for minority group members and women ("EEO") and contracting opportunities for New York State Certified minority and women-owned business enterprises ("MWBEs"). Contractor's demonstration of "good faith efforts" pursuant to 5 NYCRR §142.8 shall be a part of these requirements. These provisions shall be deemed supplementary to, and not in lieu of, the nondiscrimination provisions required by New York State Executive Law Article 15 (the "Human Rights Law") or other applicable federal, state or local laws.

C. The Contractor further agrees to be bound by the provisions of Article 15-A and the MWBE Regulations. If any of these terms or provisions conflict with applicable law or regulations, such laws and regulations shall supersede these requirements.

D. Failure to comply with all of the requirements herein may result in a finding of non-responsiveness, non-responsibility and/or a breach of contract, leading to the withholding of funds or such other actions, liquidated damages pursuant to subsection VII of this section or enforcement proceedings as allowed by the Contract.

II. Contract Goals

A. OGS hereby establishes an overall goal of 20% for MWBE participation, 10% for Minority-Owned Business Enterprises ("MBE") participation and 10% for Women-Owned Business Enterprises ("WBE") participation (based on the current availability of qualified MBEs and WBEs). The total contract goal can be obtained by utilizing any combination of MBE and /or WBE participation for subcontracting and supplies acquired under this Contract.

B. For purposes of providing meaningful participation by MWBEs on the Contract and achieving the Contract Goals established in Section II-A hereof, Contractor should reference the directory of New York State Certified MBWEs found at the following internet address: https://ny.newnycontracts.com/frontend/diversityusers.asp. Additionally, Contractor is encouraged to contact the Division of Minority and Women's Business Development ((518) 292-5250; (212) 803-2414; or (716) 846-8200) to discuss additional methods of maximizing participation by MWBEs on the Contract.

C. Pursuant to 5 NYCRR § 142.8, Contractor must document "good faith efforts" to provide meaningful participation by MWBEs as subcontractors or suppliers in the performance of the Contract and ensure that the MWBEs utilized under the Contract perform commercially useful functions. Pursuant to 5 NYCRR § 140.1(f), a MWBE performs a commercially useful function when it is responsible for execution of the work of the contract and is carrying out its responsibilities by actually performing, managing, and supervising the work involved. To perform a commercially useful function, a MWBE must, where applicable and in accordance with any State Agency specifications, also be responsible, with respect to materials and supplies used on the contract, for ordering and negotiating price, determining quality and quantity and installing. A MWBE does not perform a commercially useful function if its role adds no substantive value and is limited to that of an extra participant in a transaction, contract, or project through which funds are passed in order to obtain the appearance of participation. OGS will assess whether a MWBE is performing a commercially useful function by considering the following:
(1) the amount of work subcontracted;
(2) industry practices;
(3) whether the amount the MWBE is to be paid under the contract is commensurate with the work it is to perform;
(4) the credit claimed towards MWBE utilization goals for the performance of the work by the MWBE; and
(5) any other relevant factors.

D. In accordance with Executive Law Section 316-aand 5 NYCRR §142.13, the Contractor acknowledges that if it is found to have willfully and intentionally failed to comply with the MWBE participation goals set forth in the Contract, such a finding constitutes a breach of contract and the Contractor shall be liable to OGS for liquidated or other appropriate damages, as set forth herein.

III. Equal Employment Opportunity (EEO)

A. Contractor shall comply with the following provisions of Article 15-A:
   1. Contractor and Subcontractors shall undertake or continue existing EEO programs to ensure that minority group members and women are afforded equal employment opportunities without discrimination because of race, creed, color, national origin, sex, age, disability or marital status. For these purposes, EEO shall apply in the areas of recruitment, employment, job assignment, promotion, upgrading, demotion, transfer, layoff, or termination and rates of pay or other forms of compensation.
   2. The Contractor certifies by entering into this Contract that the text set forth in clause 12 of Appendix A, attached hereto and made a part hereof is Contractor's equal employment opportunity policy.

B. Form EEO 100 - Staffing Plan.
   To ensure compliance with this Section, the Contractor shall submit a staffing plan to document the composition of the proposed workforce to be utilized in the performance of the Contract by the specified categories listed, including ethnic background, gender, and Federal occupational categories. Contractors shall complete the Staffing plan form and submit it as part of their contract.

C. Form EEO 102 - Workforce Employment Utilization Report ("Workforce Report")
Contractor and OGS agree that Contractor is unable to separate out the workforce utilized in the performance of the Contract from Contractor's and/or subcontractor's total workforce and that the information provided on the previously submitted Staffing Plan is Contractor's total workforce during the subject time frame, not limited to work specifically under the Contract.

D. Contractor shall comply with the provisions of the Human Rights Law, all other State and Federal statutory and constitutional non-discrimination provisions. Contractor and subcontractors shall not discriminate against any employee or applicant for employment because of race, creed (religion), color, sex, national origin, sexual orientation, military status, age, disability, predisposing genetic characteristic, marital status or domestic

violence victim status, and shall also follow the requirements of the Human Rights Law with regard to non-discrimination on the basis of prior criminal conviction and prior arrest.

IV. MWBE Utilization Plan

A. Contractor certifies that it has submitted a MWBE Utilization Plan on Form MWBE 100 to OGS and will follow such Plan for the performance of MWBEs on the Contract pursuant to the prescribed MWBE goals set forth in Section II-A of this Appendix.
B. Contractor further certifies that the MWBEs included in its Utilization Plan will perform commercially useful functions under the Contract. Contractor understands that making false representations or including information evidencing a lack of good faith as part of, or in conjunction with, the submission of a Utilization Plan is prohibited by law and may result in penalties including, but not limited to, termination of a contract for cause, loss of eligibility to submit future bids, and/or withholding of payments. Contractor further understands and agrees that MWBEs that do not perform commercially useful functions may not be counted as meeting the MWBE goals of this Contract.
C. Contractor further agrees that a failure to submit and/or use such MWBE Utilization Plan shall constitute a material breach of the terms of the Contract. Upon the occurrence of such a material breach, OGS shall be entitled to any remedy provided herein, including but not limited to, a finding of Contractor non-responsiveness.

V. Waivers

A. If the Contractor, after making good faith efforts, is unable to comply with MWBE goals, the Contractor may submit a Request for Waiver form (BDC 333) documenting good faith efforts by the Contractor to meet such goals. If the documentation included with the waiver request is complete, the OGS shall evaluate the request and issue a written notice of acceptance or denial within twenty (20) days of receipt.
B. If the OGS, upon review of the MWBE Utilization Plan and updated Quarterly Workforce Reports determines that Contractor is failing or refusing to comply with the Contract goals and no waiver has been issued in regards to such non-compliance, the OGS may issue a notice of deficiency to the Contractor. The Contractor must respond to the notice of deficiency within seven (7) business days of receipt. Such response may include a request for partial or total waiver of MWBE Contract Goals.

VI. Monthly MWBE Contractor Compliance Report

A. Contractor is required to report Monthly MWBE Contractor Compliance to OGS during the term of the Contract for the preceding month's activity, documenting progress made towards achievement of the Contract MWBE goals. OGS requests that all Contractors use the New York State Contract System (NYSCS) to report subcontractor and supplier payments made by Contractor to MWBEs performing commercially useful functions under the Contract. The NYSCS may be accessed at https://ny.newnycontracts.com/. This is a New York State-based system that all State agencies and authorities will be implementing to ensure uniform contract compliance reporting throughout New York State.
B. When a Contractor receives a payment from a State Agency Authorized User following a purchase from an OGS NYSPro contract, it is the Contractor's responsibility to pay its subcontractors and suppliers in a timely manner. On or after the first day of each month, the Contractor will receive an e-mail or fax notification ("audit notice") indicating that a representative of its company needs to log-in to the NYSCS to report the company's MWBE subcontractor and supplier payments for the preceding month. The Contractor must also report when no payments have been made to a subcontractor or supplier in a particular month with entry of a zero dollar value in the NYSCS. Once subcontractor and supplier payments have been entered into the NYSCS, the subcontractor(s) and supplier(s) will receive an email or fax notification advising them to log into the NYSCS to confirm that they actually received the reported payments from the Contractor. It is the Contractor's responsibility to educate its MWBE subcontractors and suppliers about the NYSCS and the need to confirm payments made to them in the NYSCS.
C. To assist in the use of the NYSCS, OGS recommends that all Contractors and MWBE subcontractors and suppliers sign up for the following two webinar trainings offered through the NYSCS: **"Introduction to the System for Vendors"** and "**Contract Compliance Reporting - Vendor Training"** to become familiar with the NYSCS. To view the training schedule and to register visit: https://ny.newnycontracts.com/events.asp
D. As soon as possible after the Contract is approved, Contractor should visit https://ny.newnycontracts.com and click on **"Account Lookup"** to identify the Contractor's account by company name. Contact information should be reviewed and updated if necessary by choosing **"Change Info."** It is important that the staff member who is responsible for reporting payment information for the Contractor be listed as a user in the NYSCS. Users who are not already listed may be added through **"Request New User."** When identifying the person responsible, please add **"- MWBE Contact"** after their last name (i.e John Doe – MWBE Contact) to ensure

that the correct person receives audit notices from the NYSCS. NYSCS Technical Support should be contacted for any technical support questions by clicking on the links for "Contact Us & Support" then "Technical Support" on the NYSCS website.

E. If Contractor is unable to report MWBE Contractor Compliance via the NYSCS, Contractor must submit a Monthly MWBE Contractor Compliance Report on Form MWBE 102 to OGS, by the 10th day of each month during the term of the Contract, for the preceding month's activity to: OGS MWBE Office, 29th floor Corning Tower, Empire State Plaza, Albany, NY 12242. Phone: 518-486-9284; Fax: 518-486-9285.

F. It is the Contractor's responsibility to report subcontractor and supplier payments. Failure to respond to payment audits in a timely fashion through the NYSCS, or by paper to OGS, may jeopardize future payments pursuant to the MWBE liquidated damages clause in Section VII below.

VII. Liquidated Damages - MWBE Participation

A. Where OGS determines that Contractor is not in compliance with the requirements of the Contract and Contractor refuses to comply with such requirements, or if Contractor is found to have willfully and intentionally failed to comply with the MWBE participation goals, Contractor shall be obligated to pay to the OGS liquidated damages.

B. Such liquidated damages shall be calculated as an amount equaling the difference between:
   1. All sums identified for payment to MWBEs had the Contractor achieved the contractual MWBE goals; and
   2. All sums actually paid to MWBEs for work performed or materials supplied under the Contract.

C. In the event a determination has been made, after Contractor has been afforded the process that it is due, which requires the payment of liquidated damages and such identified sums have not been withheld by the OGS, Contractor shall pay such liquidated damages to the OGS within sixty (60) days after such determination unless prior to the expiration of such sixtieth day, the Contractor has filed a complaint with the Director of the Division of Minority and Women's Business Development pursuant to Subdivision 8 of Section 313 of the Executive Law in which event the liquidated damages shall be payable if the Director renders a decision in favor of the OGS.

ALL FORMS ARE AVAILABLE AT: http://www.ogs.ny.gov/MWBE/Forms.asp

2.9 AUTHORITY

Contractor shall be registered with the NYS Department of State as an entity authorized to conduct business in New York State. Contractor represents and warrants that, as of the date of Contract execution, Contractor has completed, obtained and/or performed all registrations, filings, approvals, authorizations, consents and examinations required by any governmental authority for the provision of the Services and that Contractor will, in order to perform the Services during the term of the Contract, comply with any requirements imposed upon it by law during the Contract term.

2.10 SHORT TERM EXTENSION

In the event a replacement contract has not been issued, this Contract may be extended unilaterally by the State for an additional period of up to one (1) year upon notice to the Contractor with the same terms and conditions as the original Contract. This extension terminates should the replacement contract be issued in the interim.

2.11 EXTENSION OF USE

This Contract may be extended to additional States or governmental jurisdictions upon mutual written agreement between New York State (the lead contracting State) and the Contractor. Political subdivisions and other authorized entities within each participating State or governmental jurisdiction may also participate in this Contract if such State normally allows participation by such entities. New York State reserves the right to negotiate additional discounts based on any increased volume generated by such extensions.

2.12 EXTENSION OF USE COMMITMENT

Contractor agrees to honor all orders from State Agencies, political subdivisions and others authorized by law to participate in this Contract, which are in compliance with the pricing, terms, and conditions contained herein.

Any unilateral limitations or restrictions imposed by the Contractor and/or manufacturer on eligible Authorized Users will be grounds for cancellation of the Contract. If a Contract, or any portion thereof, is canceled for this reason, any additional costs incurred by the eligible purchaser will be borne by the Contractor.

2.13 CENTRALIZED CONTRACT MODIFICATIONS

A. OGS, an Authorized User, or the Contractor may suggest modifications to the Centralized Contract or its Appendices. Except as specifically provided herein, modifications to the terms and conditions set forth herein may only be made with mutual written agreement of the Parties. Modifications may take the form of an update or an amendment. "Updates" are changes that do not require a change to the established Centralized Contract terms and conditions. A request to add new products at the same or better price level is an example of an update. "Amendments" are any changes that are not specifically covered by the terms and conditions of the Centralized Contract, but inclusion is found to be in the best interest of the State. A request to change a contractual term and condition is an example of an amendment.

B. Updates to the Centralized Contract and the Appendices may be made in accordance with the contractual terms and conditions to incorporate new products or services, make price level revisions, delete products or services, or to make such other updates to the established Centralized Contract terms and conditions, not resulting in a change to such terms and conditions, which are deemed to be in the best interest of the State.

C. OGS reserves the right to consider modifications which are not specifically covered by the terms of the Centralized Contract, but are judged to be in the best interest of the State. Such modifications are deemed amendments to the Centralized Contract and may require negotiations between Contractor and OGS before execution.

D. All modifications proposed by Contractor, shall be processed in accordance with Appendix I, *Contract Modification Procedure*. The Contractor shall submit all requests in the form and format contained in Appendix I, *Contract Modification Procedure*. The form contained within Appendix I *Contract Modification Procedure* is subject to change at the sole discretion of OGS.

E. Modifications proposed by OGS or an Authorized User, including updates and amendments, shall be processed in accordance with the terms of the Centralized Contract and Appendix B, §28.

2.14 PERFORMANCE AND BID BONDS

There are no bonds for this Contract. In accordance with Appendix B, §45 *Performance/Bid Bond*, the Commissioner of OGS has determined that no performance, payment or Bid bond, or negotiable irrevocable letter of credit or other form of security for the faithful performance of the Contract shall be required at any time during the term of the Contract.

2.15 NON-STATE AGENCIES PARTICIPATION IN CENTRALIZED CONTRACTS

New York State political subdivisions and others authorized by New York State law may participate in Centralized Contracts. These include, but are not limited to local governments, public authorities, public school and fire districts, public and nonprofit libraries, and certain other nonpublic/nonprofit organizations. See Appendix B, §27 *Participation in Centralized Contracts*.

Upon request, all eligible non-State agencies must furnish Contractor with the proper tax exemption certificates and documentation certifying eligibility to use State contracts. Questions regarding an organization's eligibility to purchase from New York State Contracts may also be directed to OGS NYSPro's Customer Services at 518-474-6717.

2.16 NEW YORK STATE VENDOR RESPONSIBILITY QUESTIONNAIRE FOR-PROFIT BUSINESS ENTITY

If it is found by the State that the Contractor's responses to the Vendor Responsibility Questionnaire were intentionally false or intentionally incomplete, on such finding, OGS may terminate the Contract. Contractor agrees it shall recertify its Questionnaire no later than the end of the eleventh month of each Contract year.

The Contractor shall at all times during the Contract term remain responsible. The Contractor agrees, if requested by the Commissioner of OGS or her designee, to present evidence of its continuing legal authority to do business in New York State, integrity, experience, ability, prior performance, and organizational and financial capacity.

The Commissioner of OGS or her designee, in his or her sole discretion, reserves the right to suspend any or all activities under this Contract, at any time, when he or she discovers information that calls into question the responsibility of the Contractor. In the event of such suspension, the Contractor will be given written notice outlining the particulars of such suspension. Upon issuance of such notice, the Contractor must comply with the terms of the suspension order. Contract activity may resume at such time as the Commissioner of OGS or her designee issues a written notice authorizing a resumption of performance under the Contract.

Upon written notice to the Contractor, and a reasonable opportunity to be heard with appropriate OGS officials or staff, the Contract may be terminated by the Commissioner of OGS or her designee at the Contractor's expense where the Contractor is determined by the Commissioner of OGS or her designee to be non-responsible. In such event, the Commissioner of OGS or her designee may complete the contractual requirements in any manner he or she may deem advisable and pursue available legal or equitable remedies for breach.

In no case shall such termination of the Contract by the State be deemed a breach thereof, nor shall the State be liable for any damages for lost profits or otherwise, which may be sustained by the Contractor as a result of such termination.

2.17 NOTE TO AUTHORIZED USERS

When placing Purchase Orders under the Contract, the Authorized User should be familiar with and follow the terms and conditions governing its use. The Authorized User is accountable and responsible for compliance with the requirements of public procurement processes. The Authorized User, when purchasing from OGS contracts, should hold the Contractor accountable for Contract compliance and meeting the Contract terms, conditions, specifications, and other requirements. Also, in recognition of market fluctuations over time, Authorized Users are encouraged to seek improved pricing whenever possible. Authorized Users have the responsibility to document purchases which should include:

A. a statement of need and associated requirements;
B. obtaining all necessary prior approvals;
C. a summary of the Contract alternatives considered for the purchase; and
D. the reason(s) supporting the resulting purchase (e.g., show that basis for the selection among multiple contracts at the time of purchase was the most practical and economical alternative and was in the best interests of the State).

2.18 POOR PERFORMANCE

Authorized Users should notify NYSPro Customer Services promptly if the Contractor fails to meet the requirements of this Contract. Performance which does not comply with requirements or is otherwise unsatisfactory to the Authorized User should also be reported to Customer Services:

Office of General Services
New York State Procurement
Customer Services Coordination
38th Floor Corning Tower
Empire State Plaza
Albany, NY 12242

Tel: 518-474-6717
Fax: 518-474-2437
E-mail: customer.services@ogs.ny.gov

2.19 CONTRACT ADVERTISING

In addition to the requirements set forth in Appendix B, §13 *Advertising Results*, any Contractor advertisements, promotional literature and/or Contract description(s) of Contract awards must be reviewed and approved by NYSPro prior to issuance. The parties agree that any press releases, public announcements, confirmation or

other information regarding this Agreement or the transactions contemplated hereby shall be made only after each Party has approved in writing the time, form and content of any such information to be disseminated to third parties or the public. Requests for issuance of press releases or public announcements and requests for the State to act as a reference shall be reviewed in accordance with OGS and/or NYSPro policy. Notwithstanding the foregoing, nothing herein shall limit the Contractor from actively marketing its Lot II solutions to Authorized Users.

2.20 OVERLAPPING CONTRACT ITEMS

Products or services available under this Contract may also be available from other New York State contracts. Authorized Users will be advised to select the most cost effective procurement alternative that meets their program requirements and to maintain a procurement record documenting the basis for this selection.

2.21 WEB ACCESSABILITY

Any web-based information and applications development, or programming delivered pursuant to the contract or procurement, will comply with New York State Enterprise IT Policy NYS-P08-005, Accessibility of Web-Based Information and Applications as such policy may be amended, modified or superseded, which requires that state agency web-based information and applications are accessible to persons with disabilities. Web-based information and applications must conform to New York State Enterprise IT Policy NYS-P08-005 as determined by quality assurance testing. Such quality assurance testing will be conducted by OGS and the results of such testing must be satisfactory to OGS before web-based information and applications will be considered a qualified deliverable under the contract or procurement.

2.22 SECURITY

The solution must comply with all policies, standards and guidelines of the New York State Office of Information Technology Services (ITS), in addition to all provisions contained herein. To the extent that compliance with any newly promulgated policy, standard or guideline would require significant expense, Contractor may seek a waiver, which shall not be unreasonably withheld.

1. Data ownership

   All State data is owned exclusively by the State and shall remain the property of the State for the term of the Contract. All State data shall be considered Confidential Information subject to the terms of the Contract and shall not be released to any third party without explicit written permission from the New York State Office of General Services (OGS). Any request, subpoena or court order seeking State data shall be immediately forwarded to OGS in order that they may respond to the inquiry. Contractor may access the associated System, including State data, solely to respond to system or technical problems; or at OGS's request; or for any work associated with hosting such data in connection with the provision of the System to OGS and Authorized Users. Contractor shall comply fully with all security procedures of the State communicated to it in the performance of this Contract. Contractor shall have robust compartmentalization of job duties, perform background checks, require/enforce non-disclosure agreements, and limit staff knowledge of State data to that which is absolutely needed to perform job duties.

   a. OGS shall have the right - at any time - to require that Contractor remove from interaction with OGS any Contractor Representative who OGS believes is detrimental to its working relationship with Contractor. The State will provide Contractor with notice of its determination, and the reasons it requests the removal. If OGS signifies that a potential security violation exists with respect to the request, Contractor shall immediately remove such individual. Contractor shall not assign the Representative to any aspect of the Contract or future work orders without OGS's consent.

   b. Contractor shall use industry standard security measures, including standard encryption protocols, to protect and guard the availability and security of all State data, and adhere to all the State's commercially reasonably security policies within a reasonable amount of time.

   c. Contractor shall be strictly prohibited from using State data in any manner other than as provided herein. There may be instances whereby OGS will communicate security procedures necessitated by State information technology operations and Contractor shall use reasonable efforts to implement. In the event Contractor does not implement or communicates that it cannot or will not implement such security procedures, a written dispute will be issued as per the Contract Dispute Resolution process.

d. Contractor shall warrant that their Representatives are properly informed and trained regarding security standards and are prohibited from disclosing technical and business Confidential Information to any persons without a need to know. If applicable, Contractor shall warrant that State data that is dormant, in transit and in backup will be encrypted. Contractor shall work cooperatively with the State so the application is accessed by the single sign-on service provided by New York State Directory Services.

e. Contractor may be asked to provide recent independent audit reports on security controls during the term of this Contract. With reasonable notice, the State and any regulatory authority having jurisdiction over OGS shall have the right to send its officers and employees into the offices and plants of Contractor for inspection of the facilities and operations used in the performance of any work under the Contract, provided that such individuals comply with the reasonable security procedures of Contractor. To the extent that such officers and/or employees may have access to data of other customers, Contractor may require such individuals to submit to security checks and confidentiality agreements. On the basis of such inspection, specific measures may be required in cases where the Contractor is found to be noncompliant with Contract safeguards.

f. Contractor shall comply fully with all of the security requirements specific to the information technology services Contractor is providing to OGS under this Contract. If any software application vulnerabilities or any other security risks related to this Contract are realized, Contractor is responsible for ensuring those vulnerabilities and risks are remediated to the reasonable satisfaction of OGS.

g. Contractor shall provide industry standard security against hacker attack, viruses, Trojans, etc., though Contractor is not expected to prevent all such attacks or exposures.

h. Contractor shall mask State authorized user P-Card information, if applicable.

i. Contractor shall enforce industry standard password verification against user password authentication protocol.

j. Contractor shall have the system be scalable to maintain performance during peak user access intervals.

k. Contractor shall provide a configurable password policy for access control (e.g., expiration threshold, minimum character length, naming convention requirements).

l. Contractor shall authenticate user login credentials.

m. Contractor shall make reasonable efforts to ensure information being displayed on the website or transmitted over the internet has not been altered in any way by any unauthorized party.

n. Ability to create and implement formal, documented backup and redundancy measures to ensure continuity of service and preservation of State data

2. Information Security Breach And Notification Act

In accordance with the Information Security Breach and Notification Act (ISBNA) (General Business Law, §889-aa; State Technology Law, §208), Contractor shall be responsible for complying with the provisions of the ISBNA and the following terms contained herein with respect to any private information (as defined in ISBNA) received by Contractor under this Contract (Private Information) that is within the control of the Contractor either on OGS's information security systems or the Contractor's information security systems. In the event of a breach of the security of the System (as defined by ISBNA) Contractor shall immediately commence an investigation, in cooperation with OGS, to determine the scope of the breach and restore the security of the System to prevent any further breaches. Contractor shall also notify OGS of any breach of the security of the System immediately following discovery of such breach. Except as otherwise instructed by OGS, Contractor shall, to the fullest extent possible, first consult with and receive authorization from OGS prior to notifying any individuals, the Department of State (DOS), the Office of the Attorney General (OAG) or any consumer reporting agencies of a breach of the security of the System or concerning any determination to delay notification due to law enforcement investigations. Contractor shall be responsible for providing the notice to all such required recipients and for all costs associated with providing such notice. Nothing herein, shall in any way impair the authority of the OAG to bring an action against Contractor to enforce the provisions of ISBNA or limit Contractor's liability for any violations of the ISBNA. In the event that Contractor is advised by a law enforcement agency - pursuant to GBL §899-aa (4) - to delay the notice under GBL §899-aa (3), Contractor shall provide the notice under GBL §899-aa (3) to the State not more than twenty-four hours after Contractor has been advised by the law enforcement agency that notice under GBL §899-aa (3) can be provided.

3. CAIQ

The Consensus Assessments Initiative Questionnaire (CAIQ) provides a series of "yes or no" control assertion questions regarding a vendor's security, intended to help organizations build the necessary assessment process for engaging with cloud providers. Contractor's response to the CAIQ is attached as Appendix H. The State reserves the right to request updated responses to the CAIQ (or latest revision thereof) throughout the term of the Contract.

4. General

In addition, the Solution implemented by the Contractor must comply with the following additional requirements:

- Must have sufficient data storage capacity to house all contract data.
- Must be able to access the solution from any of the most commonly-available web browsers on any basic configured PC or MAC computer.
- Must be able to enable transfer of data in high volumes and frequency to meet the State's procurement demands.
- Must have SLA plans that define minimum levels of system performance and availability of technological support for invoicing process requirements of a State organization.
- Must have proper measures in place to ensure that data records are transported, stored and accessed in a secure manner. All Content data is the property of the State of New York or its Suppliers.
- Must have authentication methods that must protect against access from unauthorized individuals and entities.
- Must have internet security practices that include regular intrusion detection system (IDS), firewalls, and layered security including anti-virus and anti-spam protection.
- The criteria for Disaster Recovery situations and procedures for managing disaster recovery situations must be agreed upon by both parties.
- The system must be PCI/DSS compliant.
- Must utilize formal, documented back-up and redundancy measures to ensure continuity of service and preservation of customer data. Upon request, Contractor must provide Recovery Time Objectives and Recovery Point Objectives.
- Ability to support Security Assertion Markup Language (SAML)
- Ability to, at the end of the contract period, deliver to the State , in a reasonable format, time, and method dictated by the State, all State data pertaining to this Contract.
- Ability to wipe all data from the vendor solution, backup, and system in general, all data products at the end of the contract period.
- Ability to communicate a change/release management plan for introducing product upgrades (including formal tests, Quality Assurance plans, etc.)
- All State data shall be hosted at a location or facility within the contiguous 48 states of the United States.
- Ability to transmit data to the Statewide Financial System and FileNet using SFTP and SMTP.

2.23 ADDITIONAL REQUIREMENTS

For reasons of safety and public policy, the use of illegal drugs and/or alcoholic beverages by the Contractor or its personnel shall not be permitted while performing any phase of the work under this Contract.

The State will not be liable for any expense incurred by the Contractor for any parking fees or as a consequence of any traffic infraction or parking violations attributable to employees of the Contractor.

2.24 INSURANCE REQUIREMENTS

Contractor agrees to comply with the Insurance Requirements as described in Appendix F, *Contractor Insurance Requirements*. If requested by NYSPro, Contractor must provide proof of current insurance, certifications, compliance, etc. throughout the Contract term.

2.25 EMERGENCY PURCHASING

In the event that a disaster emergency is declared by Executive Order under § 28 of Article 2-B of the Executive Law, or that the Commissioner determines pursuant to his/her authority under § 163(10)(b) of the State Finance Law that an emergency exists requiring the prompt and immediate delivery of products or services, the

Commissioner reserves the right to obtain such products or services from any source, including but not limited to a contract, as the Commissioner in his/her sole discretion determines will meet the needs of such emergency. Contractor shall not be entitled to any claim or lost profits for products or services procured from other sources pursuant to this paragraph.

2.26 TAX LAW SECTION 5-A

Section 5-a of the Tax Law, as amended, effective April 26, 2006, requires certain Contractors awarded State Contracts for commodities, services and technology valued at more than $100,000 to certify to the Department of Taxation and Finance (DTF) that they are registered to collect New York State and local sales and compensating use taxes. The law applies to Contracts where the total amount of such Contractors' sales delivered into New York State are in excess of $300,000 for the four quarterly periods immediately preceding the quarterly period in which the certification is made, and with respect to any affiliates and subcontractors whose sales delivered into New York State exceeded $300,000 for the four quarterly periods immediately preceding the quarterly period in which the certification is made. This law imposes upon certain Contractors the obligation to certify whether or not the Contractor, its affiliates, and its subcontractors are required to register to collect State sales and compensating use tax and Contractors must certify to DTF that each affiliate and subcontractor exceeding such sales threshold is registered with DTF to collect New York State and local sales and compensating use taxes. The law prohibits the State Comptroller, or other approving Agency, from approving a Contract awarded to a Contractor meeting the registration requirements but who is not so registered in accordance with the law. Contractor is required to file the completed and notarized Form ST-220-CA with OGS certifying that the Contractor has filed the ST- 220-TD with the NYS Department of Taxation and Finance (DTF). Please note that the NYS Department of Taxation and Finance should receive the completed Form ST-220-TD, not OGS. OGS should only receive the Form ST-220-CA.

Proposed Contractors should complete and return the certification forms within five (5) business days of request (if the forms are not completed and returned with bid submission). Failure to make either of these filings may render a Bidder non-responsive. Each Bidder shall take the necessary steps to provide properly certified forms within a timely manner to ensure compliance with the law. Website links to the Contractor certification forms and instructions are provided below.

Form No. ST-220-TD must be filed with and returned directly to DTF and can be found at http://www.tax.ny.gov/pdf/current_forms/st/st220td_fill_in.pdf. Unless the information upon which the ST-220-TD is based changes, this form only needs to be filed once with DTF. If the information changes for the Contractor, its affiliate(s), or its subcontractor(s), a new Form No. ST-220-TD must be filed with DTF.

Form ST-220-CA must be submitted to OGS. This form provides the required certification that the Contractor filed the ST- 220-TD with DTF. This form can be found at http://www.tax.ny.gov/pdf/current_forms/st/st220ca_fill_in.pdf.

Vendors may call DTF at 518-485-2889 for any and all questions relating to Section 5-a of the Tax Law and relating to a company's registration status with DTF. For additional information and frequently asked questions, please refer to the DTF web site: http://www.tax.ny.gov.

2.27 EMPLOYEE INFORMATION REQUIRED TO BE REPORTED FOR CERTAIN CONSULTANT CONTRACTORS AND SERVICE CONTRACTORS

Chapter 10 of the Laws of 2006 amended the Civil Service Law and the State Finance Law, relative to maintaining certain information concerning Contract Employees working under State Agency service and consulting Contracts. State Agency consultant Contracts are defined as "Contracts entered into by a state Agency for *analysis, evaluation, research, training, data processing, computer programming, engineering, environmental health and mental health services, accounting, auditing, paralegal, legal, or similar services*" ("covered consultant Contract" or "covered consultant services"). The amendments also require that certain Contract Employee information be provided to the state Agency awarding such Contracts, OSC, DOB and CS. The effective date of these amendments is June 19, 2006. The requirements will apply to covered Contracts awarded on and after such date.

To meet these new requirements, the Contractor agrees to complete:

Form A - Contractor's Planned Employment Form, if required. Note: State Agencies are required to furnish this information but may require a Contractor to submit the information as part of its bid response.

Form B - Contractor's Annual Employment Report. Throughout the term of the Contract by May 15th of each year the Contractor agrees to report the following information to the State Agency awarding the Contract, or if the Contractor has provided Contract Employees pursuant to an OGS centralized Contract, such report must be made to the State Agency purchasing from such Contract. For each covered consultant Contract in effect at any time between the preceding April 1st through March 31st fiscal year or for the period of time such Contract was in effect during such prior State fiscal year Contractor reports the:

1. Total number of Employees employed to provide the consultant services, by employment category.
2. Total number of hours worked by such Employees.
3. Total compensation paid to all Employees that performed consultant services under such Contract.*

*NOTE: The information to be reported is applicable only to those Employees who are directly providing services or directly performing covered consultant services. However, such information shall also be provided relative to Employees of Subcontractors who perform any part of the service Contract or any part of the covered consultant Contract. This information does not have to be collected and reported in circumstances where there is ancillary involvement of an Employee in a clerical, support, organizational or other administrative capacity.

Contractor agrees to simultaneously report such information to CS and OSC as designated below:

Department of Civil Service	**Office of the State Comptroller** - Bureau of Contracts
Alfred E. Smith State Office Building	110 State St., 11th Floor
Albany, NY 12239	Albany, New York
	Attn: Consultant Reporting

Contractor is advised herein and understands that this information is available for public inspection and copying pursuant to §87 of the New York State Public Officers Law (Freedom of Information Law). In the event individual Employee names or social security numbers are set forth on a document, the State Agency making such disclosure is obligated to redact both the name and social security number prior to disclosure.

Further information is available in the Office of the State Comptroller's Bulletin G-226 regarding the Contractor Consultant Law requirements and report Forms A and B at http://osc.state.ny.us/agencies/guide/MyWebHelp/

INSTRUCTIONS FOR COMPLETING FORM A AND B:
Form A and Form B should be completed for Contracts for consulting services in accordance with OSC's policy and the following:

Form A - Contractor's Planned Employment Form (available from and submitted to the using Agency, if necessary.)

Form B - Contractor's Annual Employment Report (to be completed by May 15th of each year for each consultant Contract in effect at any time between the preceding April 1st through March 31st fiscal year and submitted to the CS, OSC and procuring Agency.)

Scope of Contract: choose a general classification of the single category that best fits the predominate nature of the services provided under the Contract.

Employment Category: enter the specific occupation(s), as listed in the O*NET occupational classification system, which best describes the Employees providing services under the Contract.
*(Note: Access the O*NET database, which is available through the US Department of Labor's Employment and Training Administration, on-line at* online.onetcenter.org *to find a list of occupations.)*

Number of Employees: enter the total number of Employees in the employment category employed to provide services under the Contract during the report period, including part time Employees and Employees of subcontractors.

Number of Hours: enter the total number of hours worked during the report period by the Employees in the employment category.

Amount Payable under the Contract: enter the total amount paid by the State to the State Contractor under the Contract, for work by the Employees in the employment category, for services provided during the report period.

2.28 CONTRACT CANCELLATION

If the Contract is cancelled, the State reserves the right to make award on another bid meeting requirements, but is not obligated to do so.

3 PROJECT PHASES

3.1 IMPLEMENTATION CONSIDERATIONS

The State is planning for a maximum two-year phased implementation approach to deploy the MarketPlace Catalog and eInvoicing solutions. Contractor has been advised to consider the following potential issues in its Implementation Plan: (a) the upgrade of SFS from version 9.0 to 9.2, anticipated to be implemented approximately April, 2015, (b) integration with the BSC's FileNet, and (c) SFS Item Master Project. The Contractor's Solution must include integration to the State's environment for SFS and FileNet throughout the life of the Contract.

3.2 PROPOSED PHASES

Contractor proposes a two-year phased implementation in accordance with Appendix G - Implementation Plan, with the MarketPlace Catalog and eInvoicing solutions targeted to be initially deployed approximately 10 months after project initiation. Upon Contract execution, Contractor will develop a mutually agreeable Implementation Plan, describing and detailing the overall project schedule and detailed steps and activities for each phase.

3.3 CONTINUAL SOLUTION SUPPORT

The State considers support of the solution both during and after implementation to be critical. The State requires the Contractor to serve as the single point of contact for support from User Acceptance of the first project phase through completion of the warranty period. Throughout the implementation, the Contractor will coordinate with the State on Service Level Agreements. In addition, the Contractor will ensure the State staff is properly trained and informed on the Solution.

3.4 PAYMENT TERMS AND INCENTIVES

As part of the State's risk mitigation approach, the State will not pay "up-front" money for the Implementation. All payments will be based upon predetermined project deliverables as outlined in Section 4 of this Contract. No payment for a deliverable will be made until the deliverable has been completed by the Contractor and accepted in writing by the State Project Manager or the MarketPlace Catalog and eInvoicing Committee. The Contractor is obligated to complete the implementation even if its actual costs exceed those on the cost proposal submitted with the Contractor's bid. The Contractor will be prohibited from charging any fees or additional costs to suppliers for participation in the eCatalog/eInvoicing Solution. The foregoing sentence shall not prohibit Suppliers from purchasing advanced services from Contractor (in the case of Lot I, Integration Services, and in the case of Lot II, Integration or Roundtrip Services, depending upon the scope of the particular Lot II purchase).

The State intends to reserve 30% of the total implementation budget ("the Reserve") until the end of the implementation period. If at that time, the system is fully implemented and functional, as documented herein, the 30% reserve will be released to the Contractor. The State will allow a reduction of the hold of 5% if the Contractor successfully completes Deliverable #2 (as outlined in Section 4), more than 1 week ahead of schedule. In addition, the State will allow a reduction of the hold of 5% if the Contractor successfully completes Deliverable #7 more than 1 week ahead of schedule. The Reserve is fully earned at acceptance of Go-Live.

3.5 ACCEPTANCE CRITERIA

The purpose of the acceptance criteria is to ensure that the performance requirements and essential conditions of the deliverables are included, and that the Contractor delivers on its specifications in a manner that meets the business needs and requirements of the State. Acceptance shall be based on satisfactory completion of the deliverables contained herein, the Implementation Plan and each Phase appended thereto. Acceptance of the deliverables can only be approved by the MarketPlace Catalog and eInvoicing Committee.

3.6 WARRANTY PERIOD

The warranty period for the integrated Solution will commence upon the final acceptance by the State of all deliverables and will extend for a period of 12 months. Phase 1 implementation must be warrantied for 12 months.

After Phase 1, any changes to the interfaces or solution must be warrantied for an additional 12 months at no charge to the State. All warranty periods will be extended until all defects arising during the warranty periods are remedied by the Contractor. During all warranty periods, the Contractor will remedy all defects in a timely manner and without additional cost to the State.

4 DELIVERABLES (LOT I) AND PAYMENT SCHEDULE

4.1 OVERVIEW

The initial phase of the Solution will focus on creating the interfaces with SFS and FileNet, the development of the MarketPlace Catalog and eInvoicing solutions, and onboarding suppliers of OGS NYSPro. The State prefers minimal customization. It is required that the Contractor provide training necessary to the number of power-users and State test staff mutually agreed upon in the Implementation Plan at no additional costs.

4.2 DELIVERABLE #1: Modified Implementation Plan

- Gantt Chart defining staff roles, state action points, timelines, and dependencies
- Design documents represent the detailed plan for how to implement the business rules and requirements that are identified and documented during each iterative interface configuration
- Process Flows
- User Interface Designs (Screen Mockups)
- Information Architecture (a high-level web site map of each user interface)
- Change Management Plan (included)
- Risk Management Plan (included)
- Communication Plan (included)

4.3 DELIVERABLE #2: Interfaces with SFS and FileNet

A key factor in the implementation of this solution is the interfaces of the hosted solution with SFS and FileNet. Success to all future phases will not be possible without this successful conclusion. The Contractor will work with SFS personnel to determine the exact requirements needed to interface with SFS. In addition, the Contractor will work with ITS and BSC personnel to determine the exact requirements for FileNet. At no time will Contractor personnel alter, modify or change the SFS or FileNet systems in any way without express written permission of the MarketPlace and eInvoicing Committee. The plan must provide details of the build of the interfaces, including risk and mitigation strategies, parallel test environment (as applicable and approved by the Committee) and any State dependencies. The plan must also include documentation of the interfaces, including diagrams.

4.4 DELIVERABLE #3: MarketPlace Catalog

- General functionality: searches, filters, variables, user display and functionality
- Sample punch-out catalog with a live supplier as determined by the State Project Manager
- State MarketPlace catalog developed
- Access catalog using SFS
- Access catalog from web with payment of P-Card
- Live website demonstration
- Basic Out of the Box Reporting
- Contract Manager review, edit and change functionality workflow
- Supplier registration and submittal of catalog changes workflow
- User Acceptance Test defects identified
- User Acceptance Test Critical Defects resolved
- Functionality requests identified and tracked
- Data verification

4.5 DELIVERABLE #4: eInvoicing

- Supplier registration and submittal of invoices in multiple formats – e.g., Purchase Order (PO) flip
- Vendor interface
- Out of the Box Reporting
- General functionality: searches, filters, variables, user display and functionality
- Acceptance of a non-PO invoice
- Supplier and invoice for data validation for PO and non-PO invoices
- Ability to upload supporting documentation to an invoice, e.g., file attachment

- Business rule development and integration
- Invoice hold function
- User Acceptance Test defects identified
- User Acceptance Test Critical Defects resolved
- New functionality requests identified and tracked

4.6 DELIVERABLE #5: System, Accessibility and Load Testing

- The Contractor will conduct system accessibility, integration and load testing to confirm the functionality of its configuration when used with sources and systems, e.g., SFS tests platform with the solution's production environment.
- Accessibility Report
- Integration Test Report - the formal reporting of the results of integration testing. Integration testing brings together all released application components and tests their interoperability, including but not limited to the ability to complete a P-card transaction. Additionally, integration testing will confirm the quality of interactions with the State legacy data sources, legacy applications, and third-party systems.
- Load Test Report - intended to validate that the system is able to process data and transaction volumes using both online and batch system processes within operational processing timeframes.
- Performance Test Report - intended to confirm that end user online transaction entry and processing can be completed within reasonable timeframes.
- Quality Assurance Plan
- System/Integration test defects identified
- System/Integration test Critical Defects resolved

4.7 DELIVERABLE #6: Training and Communication

- Online Help and Training Materials: The Contractor will tailor and publish online help and training materials to support this release. The Online Help and Training Materials are business user focused descriptions and depictions of what the solution can do and how a user can use the system to perform daily business activities. All training materials become property of the State with unrestricted use and modification. These materials and online help will include:

    - Annotated screen shots
    - Descriptions of business processes
    - Hints and tips
    - Screen level support

- Train-the-Trainer Sessions: The Contractor will conduct the train-the-trainer courses at State specified locations to teach power users and Authorized Administrators how to use the new system. This may include up to the following:

Focus Area	Session Duration	# of times class conducted	Max recommended # of attendees
Formal/Informal Solicitations	3 hours	3	15
Reports	1 hour	3	15
Approval Module	1 hour	3	15
Identified during the Project	2 hours	3	15

- Communication materials to roll-out the new capabilities to State Agencies and Authorized Users.

4.8 DELIVERABLE #7: Go Live

The full system will be integrated with the SFS system and released to all State staff and Authorized Users.

4.9 DELIVERABLE #8: Go Live Acceptance

Acceptance for this deliverable will be held for 90 days after Go Live to ensure full functionality, as specified. Any Critical Defects will result in reports to the MarketPlace Catalog and eInvoicing Committee with proposed mitigation plan. The 90 day period will re-start from the acceptance of the resolution of these issues, as reported to the Committee.

4.10 PAYMENT SCHEDULE

The Total First Two-Year Cost is $1,284,000. Payments from the State to the Contractor will be deliverable-based in accordance with the schedule below. The State will not pay "up-front" money for implementation work. No payment for a deliverable will be made until the deliverable has been completed by the Contractor and accepted in writing by the State Project Manager or the MarketPlace Catalog and eInvoicing Committee. The Contractor is obligated to complete the implementation even if its actual costs exceed those on the cost proposal submitted with the Contractor's bid. The Contractor will be prohibited from charging any fees or additional costs to suppliers for participation in the eCatalog/eInvoicing Solution.

Upon satisfactory completion of each project deliverable and written acceptance by the State Project Manager, payments will be made from the State to the Contractor in accordance with the following payment schedule:

Deliverable	Percentage of First Two Year Cost	Payment Amount
Deliverable 1: Modified Implementation Plan	5%	$64,200
Deliverable 2: Interfaces with SFS and FileNet	5%	$64,200
Deliverable 3: MarketPlace Catalog	10%	$128,400
Deliverable 4: eInvoicing	10%	$128,400
Deliverable 5: System, Accessibility and Load Testing	20%	$256,800
Deliverable 6: Training and Communication	10%	$128,400
Deliverable 7: Go Live	10%	$128,400
Deliverable 8: Go Live Acceptance (Reserve Amount)	30%	$385,200
	Total First Two-Year Cost	**$1,284,000**

Notwithstanding the foregoing, Contractor may request that Deliverables be delivered in a different order, subject to the approval of the Catalog MarketPlace and eInvoicing Committee, which shall not be unreasonably withheld.

4.11 PRICING SCHEDULE

The Contractor shall provide a Contract Pricing Schedule to NYSPro based on the Contractor's bid. The Pricing Schedule submitted to NYSPro shall include all offerings under the Contract, including a description and price of each offering. The Pricing Schedule shall be made available to Authorized Users and posted publically on the OGS Web site. The Pricing Schedule is included as Appendix C of this Contract.

Notwithstanding the foregoing, where an Authorized User does not have the capability to access Contract information electronically, it shall be the Contractor's responsibility, upon Authorized User request, to furnish, without charge, the Pricing Schedule, including any changes (price changes, additions, deletions, etc.) pursuant to the Contract, to Authorized Users who request them.

The Pricing Schedule may be furnished to Authorized Users in either hard-copy or electronic format. If available in both formats, they shall be furnished in the format preferred by the requesting Authorized User. Upon request, the Contractor shall assist Authorized Users in the use of the Pricing Schedule.

4.12 PRICING UPDATES

The Contractor or OGS may request a pricing change (increase or decrease), based upon fluctuations in the latest published copy of the National Consumer Price Index for All Urban Consumers (CPI-U) Northeast region starting in year 4 of the Contract. The index is also available through the Internet at the Bureau of Labor Statistics web site at http://stats.bls.gov/. In no case will the increase exceed 5% in any year.

4.13 LOWER PRICING

The State reserves the right to negotiate lower pricing, or to advertise for bids, whichever is in the State's best interest as determined by the Commissioner, in the event of a significant decrease in market price of any Product or Service offered under the Contract. In addition, if the Contractor's normal pricing to the public or to the trade in general is less than the price offered to the State under the Contract, then the normal pricing to the public or to the trade in general shall also be granted by Contractor to Authorized Users. Price decreases to the Authorized User are permitted at any time, and do not need prior approval by NYSPro.

5 PROJECT MANAGEMENT

5.1 PROJECT OVERSIGHT

The State has established a MarketPlace Catalog & eInvoicing Committee. This team includes staff from New York State Procurement (NYSPro), Business Services Center (BSC), Information Technology Services (ITS), the Division of the Budget (DOB) and the Statewide Financial System (SFS). This Committee may change composition over time as determined by the State. This Committee will provide an overall governance of this solution.

5.2 APPROVAL ROLE

The MarketPlace Catalog & eInvoicing Committee will be responsible for reviewing any requests from New York State Agencies seeking to establish their own marketplace catalog solutions under Lot II of the resulting contract. It is the responsibility of the State Agency seeking to implement its own marketplace catalog to submit a written request and justification to the Committee. Such written request and justification will be reviewed in accordance with New York State internal policy. Approval of the Committee shall be required prior to a New York State Agency using the centralized contract to establish its own marketplace catalog.

5.3 PROJECT ROLES AND RESPONSIBILITIES

5.3.1 STATE PROJECT MANAGER

The day-to-day project manager for the implementation on behalf of the State will be a representative from NYSPro who will report directly to the Chief Procurement Officer (CPO) and the Director of the BSC. Below are the specific responsibilities of the State Project Manager:

- Work closely with the Contractor's Project Manager to ensure successful completion of the project
- Consult with the Contractor's Project Manager to develop the Project Management Plan
- Review weekly status reports and schedule weekly meetings with the Contractor, as necessary
- Coordinate participation from other agencies, Committee staff, and/or vendors as required during the project
- Acquire additional project team members as needed
- Coordinate the State's review of the deliverables and sign off on deliverable acceptance
- Report project status to State Senior Leadership

5.3.2 CONTRACTOR PROJECT MANAGER

The Contractor is expected to provide a single Project Manager for this engagement. Any changes to the position of Project Manager must be approved by the MarketPlace Catalog and eInvoicing Committee. The Contractor Project Manager will:

- Serve as a liaison between the State Project Manager and Contractor personnel (including any subcontractors) participating in this project
- Develop and maintain the Implementation Plan, in consultation with the State Project Manager
- Facilitate regular communication with the State Project Manager, including weekly status reports/updates, and review the project performance against the project plan
- Facilitate weekly project status meetings for the duration of the project

- Update the project plan on a weekly basis and distribute at weekly meetings for the duration of the project
- Be responsible for the management and deployment of Contractor personnel, including any subcontractors
- Serve as the single-point of responsibility for Contractor activities, the activities of its staff, and the activities of its subcontractors
- Assure the quality of all Contractor deliverables
- Manage risk, issues, change, and acceptance
- Assist the State in maximizing return on investment in this solution

5.3.3 CONTRACTOR ENGAGEMENT MANAGER

The Contractor must also name an Engagement Manager, who will be the sole point of contact for the State for contract matters and other large issues. This individual must have sufficient authority to resolve contract issues on behalf of the Contractor's organization and becomes the next step in the escalation process. The Engagement Manager may also serve the role of Contractor Project Manager.

5.3.4 ANTICIPATED STAFFING ROLES

The State expects that the Contractor will propose sufficient staff to implement the Solution as defined in the RFP and will supply resumes in advance of adding or replacing staff. Upon replacement, the State reserves the right to interview candidates for key positions within the project team and reject proposed staff from the team. The Contractor shall also clearly describe the retention time of key staff throughout the Contract. Employers are required by Federal Law to ensure that all employees are legally entitled to work in the United States; accordingly the State reserves the right to request legally mandated documentation. In addition to the Project Managers listed above, the State expects the Contractor to respond with a proposed staffing complement, including, but not limited to the following roles (though it is possible that multiple roles may be filled by a single person):

- Senior Product Lead
- Senior Data Lead
- Business/System Analyst(s)
- Product Configuration Manager
- Product Developer(s)
- Quality Assurance and User Experience Tester(s)
- Trainer(s)
- Technical Architect
- System Integrator

5.3.5 STAFF MANAGEMENT

The Contractor Project Manager will be responsible for managing Contractor staff assigned to this Project. In advance of adding or replacing staff, resumes must be provided to the State Project Manager for review and acceptance. The State reserves the right to interview candidates for key positions within the project team and reject proposed staff from the team.

The State requires the Contractor to perform some of its system configuration activities on-site at the State facilities and/or support meaningful interactions remotely. The key consideration for the State is the continuous exposure to and active participation of its designated staff in the architecture, design, customization, and implementation of the solution.

5.4 PROJECT PLAN MANAGEMENT

The Contractor will be required to create and maintain a detailed project plan, including but not limited to the following:

- Kick-off
- Planning
- Solution Design
- Solution Configuration
- Solution Validation and Testing
- Schedule/Time Management
- Cost Tracking

5.5 COMMUNICATIONS MANAGEMENT

The Contractor Project Manager will ensure the lines of communication between the State and the Contractor's project management team. The Contractor Project Manager will be responsible for the following:

- Status Reporting - The Contractor Project Manager will publish a weekly status report to communicate progress, issues, risks, and plans. The status report will be sent to the State Project Manager to ensure they share a common view of the contributions, commitments, and challenges of the effort. The Contractor Project Manager will also post the weekly status report to the electronic media specified by the State Project Manager and ensure that it is accessible by all key stakeholders.
- Status Meetings - At the request of the State, the Contractor Project Manager will meet with the State Project Manager and/or with the entire MarketPlace Catalog and eInvoicing Committee to review progress, adjust priorities, resolve issues, review staffing plans, assess risks, and identify improvements. All meeting results will be described in a follow-up report generated by the Contractor Project Manager.
- Ad Hoc Meetings -The Vender Project Manager will coordinate with the State Project Manager on the scheduling and facilitation of ad hoc project meetings, in particular for those meetings covering topics related to the overall timeliness, cost, and success.
- Executive Meetings – On occasion, meetings will be scheduled to ensure all executive stakeholders and representatives of key users share a common view of the direction of the project. When requested, the Contractor Project Manager will be required to participate in these meetings, anticipated to be held on an as needed basis.
- Phase/Annual Meetings - Executive presentations to Senior Leadership will be conducted at the conclusion of each Phase.

5.6 ISSUE MANAGEMENT

The Project Managers from each organization bear the primary responsibility for ensuring timely issue resolution. The Contractor Project Manager will be required to identify, report, and drive/ resolve project issues. An issue is defined as any item that adversely affects the execution of the project; such as events that impact the implementation timeframe and quality of the deliverable and/or level of service.

The Contractor Project Manager will implement and document – for State's approval – issue management procedures to ensure adequate and timely management of issues. These procedures will include processes to identify, communicate, track, and escalate issues. Issues will be managed through the use of an issue log, maintained by the Contractor Project Manager with open access to the State Project Manager.

The State expects the issues management process to include, but not be limited to the following elements:

- Any team member may raise an issue, with the approval of either the State Project Manager or the Contractor Project Manager
- Issues are retained for the life of the contract regardless of status
- Every issue has a target date for resolution after which the project is expected to be impacted and this impact may result in a change request
- Issues are closed when the initiator and the Project Managers have approved the resolution in writing
- Managers mutually agree that they are unable to resolve an issue, the State Project Manager will present the issue to Senior Leadership and the Contractor Project Manager will present the issue to its organizational leadership.

5.7 RISK MANAGEMENT

The Contractor will be responsible for managing risks. Risks will be identified, assessed, mitigated and tracked throughout the contract. The Contractor Project Manager will review risks with the State Project Manager

The State expects the Contractor to maintain a Risk Management Plan, to include but not be limited to the following:

- Identify, document and report potential project risks
- Prioritize, both in terms of probability and potential impact to the project timeline, costs, quality and/or scope
- Coordinate actions to be taken to mitigate the negative consequences or maximize positive benefits

5.8 CHANGE MANAGEMENT PROCESS

The Contractor will be responsible to manage project change. The Contractor Project Manager with oversight by the State Project Manager will be responsible for managing the change requests. Any change request outside the

scope of the requirements of this RFP will require the preapproval of the State MarketPlace and eInvoicing Committee and shall be carried forward to future version at no cost to the State.

The State expects the Contractor to maintain a Change Management Plan, to include but not be limited to, the following:

- All requests must be sent in writing to the State Project Manager prior to implementing. Requests will be vetted in status meetings.
- The Contractor Project Manager will present each change request to the State Project Manager for review, discussion, and disposition.
- The change request must be disposed (approved or rejected) by the State Project Manager within seven (7) business days after submittal. This approval/rejection must be in writing (no verbal or default approvals).
- If the State Project Manager does not respond to the change within the timeframe, the change request will be added as an item on the Issues Log and fall under the issues management process and reported weekly. Also, it must be understood that the change request may need adjustment after that date due to changes over time.
- The State Project Manager will maintain the original Change Control documents, along with the Change Request Log. These include updating the scope, budget, schedule, and quality requirements as needed, as well as the coordination of all approved changes across the entire project.
- No work associated with the change request will begin until a formal approval is received by the State Project Manager.
- Any proposed enhancement must include a fixed price, a detailed breakout of price, analysis of work to be performed, and impact to overall project.

6 SAAS TERMS AND CONDITIONS

6.1 SAAS PRODUCTS ACCESS

Use. Subject to payment of the applicable fees and the State's or Authorized User's (as applicable) compliance with the terms of this Agreement, Contractor hereby grants the Authorized User a non-exclusive, non-transferable, limited right to access and utilize the SaaS Products, subject to the following restrictions: (i) the Authorized User may use the SaaS Products solely for the Authorized User's own internal business, governmental or other authorized purposes; and (ii) the Authorized User shall not (A) make any copies of all of any portion of the SaaS Products, (B) sell, sublicense, distribute, rent, lease or assign the SaaS Products to any other person or entity, (C) modify, reverse engineer, decompile, disassemble, translate, alter or create derivative works based on the SaaS Products, (D) permit any person, who is not authorized by the State or by an Authorized User, or permit any other third party to use the SaaS Products, or (E) access it in order to (1) build a competitive product or service, (2) build a product or service using similar ideas, features, functions or graphics, or (3) copy any ideas, features, functions or graphics.

User IDs and Passwords. Contractor shall provide the Authorized User with user IDs and passcodes or other secured means to access the SaaS Products, as applicable. The Authorized User is responsible for maintaining the confidentiality of its user IDs and passcodes and will be solely liable for all activities that occur under the Authorized User's user IDs. The Authorized User shall immediately notify Contractor of any unauthorized use of its user IDs and change any affected passcodes. The Authorized User agrees to access the SaaS Products in a secure manner in compliance with Contractor's reasonable standards established from time to time which currently require, to the extent applicable, the use of web browsers utilizing 128 bit SSL encryption.

Cookies. As part of this Agreement, the Authorized User hereby expressly "opts-in" and consents to the use by Contractor of any cookies necessary for the Contractor SaaS Products to function properly. The Authorized User may "opt-out" or revoke consent of the use of cookies by the Contractor Supplier Products at any time, upon reasonable notice to Contractor. If the Authorized User "opts-out" or revokes consent of the use of any necessary cookies by the Contractor SaaS Products, Contractor may, upon reasonable notice to the Authorized User, discontinue providing the Contractor SaaS Products to the Authorized User without breaching this Agreement.

6.2 SCOPE, AVAILABILITY AND MODIFICATIONS

Scope of SaaS Products. The SaaS Products are intended to enable transactions between the Authorized User and Suppliers. Contractor is not a party to, third party beneficiary of, or a guarantor of performance with respect to any subsequent agreement between the Authorized User and any third party. Specifically, (i) Contractor does not control the quality, safety, legality or availability of products accessed through the SaaS Products, the terms and

conditions on which those products are offered or purchased, or the third party's compliance with an agreement that it may execute with the Authorized User; (ii) Contractor undertakes no duties to distribute or ship the products of a Supplier; and (iii) under no circumstances shall Contractor take title to, or in any manner obtain an interest in, or otherwise be deemed to be within the chain of title of, any products of a Supplier. The Authorized User acknowledges that Contractor takes no responsibility for the terms and conditions governing the purchase, sale and delivery of Supplier products. Contractor shall provide such additional services as may be agreed to between the parties and set forth in a properly executed Statement of Work.

Availability of SaaS Products. Notwithstanding anything to the contrary stated herein, the Authorized User acknowledges and agrees that the availability of the SaaS Products is subject to the availability of connection services to and within the Internet and to other network functions within and around the Internet and that the Internet, by its nature, is not fault-tolerant and Contractor shall not have any liability for any breach of any representation, warranty or covenant of this Agreement that arises out of the unavailability of such connection services and other network functions.

Supplier Compliance. To the extent that Contractor is required to transmit credit card information (i.e. credit card data) to Suppliers under the Contract, the Parties agree that Contractor's delivery of such credit card information to Suppliers may only apply with respect to Suppliers who have (i) agreed to Contractor's reasonable requirements, which are designed to ensure compliance with applicable PCI standards, and (ii) who actually meet those requirements.

6.3 PROPRIETARY RIGHTS

Title to Technology. All Intellectual Property Rights pertaining to Contractor and the SaaS Products, in whole or in part, shall be, vest with and remain the exclusive property of Contractor and its third party licensors. Software source code is proprietary.

Title to Transaction Information. As between the Parties, all Intellectual Property Rights in Transaction Information supplied by the State or Authorized User and/or its Suppliers in connection with the SaaS Products are and shall remain the exclusive property of the State or Authorized User. Contractor makes no claims, warranties or representations with regard to the ownership of Transaction Information. Notwithstanding the foregoing, all Intellectual Property Rights in Market Statistics are and shall remain the exclusive property of Contractor, but shall remain available for use by the Authorized User during Contract term.

Title to Content. All title, right and interest in and to Content submitted to Contractor in the course of performing the Services under the Contract shall remain the property of the applicable Supplier or other third party owners. All title, right and interest in and to Content licensed by Contractor from third party licensors and utilized in the process of providing the SaaS Products, if any, shall remain the exclusive property of Contractor or its third party licensors. If all or part of any Content becomes the subject of an actual or threatened lawsuit or if Contractor believes such Content may violate a third party's copyrights, trademarks, contract rights, or applicable law, Contractor will immediately be entitled to remove such Content and provide notification to the State in accordance with Appendix B Section 62.

Suggestions. Contractor shall have a royalty-free, worldwide, perpetual license to use or incorporate into the SaaS Products any suggestions, ideas, feedback, recommendations or other information provided by an Authorized User relating to the SaaS Products.

6.4 TERMINATION/SUSPENSION

State Agencies
In the event the State is in default in making any payment to Contractor when due, Contractor may, in accordance with Appendix B, section 50, suspend the State's access to, and the Contractor's performance of, the SaaS Products or Services until the State has cured such default and made the required payments, and arrangements have been made reasonably satisfactory to Contractor that ensure the payment of future invoices. Contractor shall have all remedies available to it at law or in equity.

Non-State Agencies
Contractor may, by written notice to the State and Authorized User in accordance with Appendix B, Section 50, suspend access to and performance of the SaaS Products or Services to a Non-State Agency Authorized User for any of the following events: (i) the Authorized User fails to pay any amount due under Lot II to Contractor within the time period specified for payment in Appendix B, Section 50; (ii) the Authorized User is in breach of any material, non-monetary term, condition or provision of this Agreement, which breach, if capable of being cured, is not cured

within thirty (30) days after the Contractor gives written notice of such breach in accordance with Appendix B, Section 50; or (iii) the Authorized User becomes subject to any bankruptcy or insolvency proceeding under federal or state statutes which is not rescinded within sixty (60) days.

6.5 RETURN OF MATERIAL

Within a reasonable period of time prior to the expiration date or termination date of this Contract, Contractor shall offer reasonable assistance to the State in extracting or transitioning all State data in a mutually agreeable format. Upon termination of this Agreement consistent with the terms herein, Contractor may immediately discontinue the State's access and use of the SaaS Products. The State shall promptly discontinue use of any SaaS Products or Services or Confidential Information that the State has received from Contractor.

Contractor shall permanently destroy or render inaccessible any portion of the State data in the Contractor's possession or control following the expiration or termination of the Contract.

6.6 SERVICE LEVEL AGREEMENT AND PENALTIES

Contractor will use commercially reasonable efforts to provide a Managed Environment in accordance with the availability service levels indicated in Appendix D - Service Level Agreement. In the event that Contractor fails to meet any of such service levels, Contractor will credit the State with the applicable amount as set forth in Appendix D, in accordance with the terms contained therein.

6.7 STATEMENTS OF WORK (LOT II)

An Authorized User seeking to use any of the "end to end" procurement solution services available under Lot II shall be required to obtain a quote from the Contractor based on the full pricing list and/or the hourly rates contained in Appendix C - Pricing Schedule. The Contractor and Authorized User shall be required to develop a Statement of Work (SOW) detailing any implementation services required for the Authorized User's particular needs. Approval of the Marketplace Catalog and eInvoicing Committee shall be required prior to a New York State Agency implementing services under Lot II.

6.8 NO IMPLIED WARRANTIES

TO THE EXTENT PERMITTED BY LAW, ALL WARRANTIES CONTAINED HEREIN ARE EXCLUSIVE AND THERE ARE NO OTHER EXPRESS OR IMPLIED WARRANTIES OR CONDITIONS, INCLUDING WARRANTIES OR CONDITIONS OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. CONTRACTOR DOES NOT WARRANT OR GUARANTEE THAT THE SAAS PRODUCTS OR SERVICES WILL BE ERROR FREE OR OPERATE WITHOUT INTERRUPTION.

No employee, agent, representative or affiliate of Contractor has authority to bind Contractor to any oral representations or warranty concerning the SaaS Products or Services.

6.9 IP INDEMNIFICATION

Contractor's indemnification obligations under Appendix B, Section 62 do not apply with respect to SaaS Products or Services or portions or components thereof which are: (i) not supplied by Contractor, (ii) made in whole or in part strictly in accordance with State requirements as instructed by the State, where Contractor does not have an opportunity to determine the means of satisfying the State's requirements, (iii) that are modified by the Authorized User after delivery by Contractor without the Contractor's approval, or (iv) where the State's use of the SaaS Products or Services is in violation of this Agreement.

6.10 SOURCE CODE ESCROW

Source Code Escrow is not typically offered by Contractor to other commercial customers for the SaaS Products and Services provided under this Contract. In the event that Contractor's business model changes during the term of this Contract and Source Code Escrow is included as a standard offering to other commercial customers for the SaaS Products and Services provided hereunder, Source Code Escrow will be made available to the State in accordance with Appendix B, Section 73.

6.11 SAAS AND DATA SECURITY

In addition to the Security Requirements set forth herein in Section 2.22, an Authorized User under Lot II may establish additional Security measures or require compliance with additional statutes, standards or certifications, based on the Authorized User's unique needs or the particular data involved. Any such additional requirements will be developed between the Authorized User and Contractor as part of the Statement of Work under Lot II.

7 GENERAL PROVISIONS

7.1 NOTICES

All notices, demands, designations, certificates, requests, offers, consents, approvals and other instruments given pursuant to this Agreement shall be in writing and shall be validly given when mailed by registered or certified mail, or hand delivered, (i) if to the State, addressed to the State at its address set forth below, and (ii) if to Contractor, addressed to Contract Administrator at the address set forth below.

The parties may from time to time, specify any address in the United States as its address for purpose of notices under this Agreement by giving fifteen (15) days written notice to the other party. The Parties agree to mutually designate individuals as their respective representatives for purposes of this Agreement. Contact information for the designated individuals will be set forth on the Contract Award Notification (CAN) and on the Contractor Information page for this Contract, which will be posted on the OGS website.

All notices sent shall be effective upon actual receipt by the receiving party. The Contractor will be required to forward a copy of the official notice to an Authorized User that is associated with the subject of the notice.

Written notice of any alleged breach by one party to the other shall provide specific facts, circumstances and grounds upon which the breach is being declared.

7.2 CAPTIONS

The captions contained in this Contract are intended for convenience and reference purposes only and shall in no way be deemed to define or limit any provision thereof.

7.3 SEVERABILITY

If any provision of this Contract is deemed invalid or unenforceable, such determination shall have no effect on the balance of the Contract, which shall be enforced and interpreted as if such provision was never included in the Contract.

7.4 COUNTERPARTS

This Agreement may be executed in one or more counterparts, each of which shall be deemed to be an original, but all of which together shall constitute the same Agreement. Any signature page of any such counterpart may be attached or appended to any counterpart to complete a fully executed counterpart of this Agreement, and shall bind such party.

7.5 ENTIRE AGREEMENT

This Contract and the referenced Appendices and Attachments constitute the entire agreement between the parties thereto and no statement, promise, condition, understanding, inducement or representation, oral or written, expressed or implied, which is not contained herein shall be binding or valid and the Contract shall not be changed, modified or altered in any manner except by an instrument in writing executed by the State and the Contractor, with all necessary approvals.

Authorized Users shall not have the authority to modify the terms of the Contract, except as to better terms and pricing for a particular procurement than those set forth herein. In accordance with the terms set forth in Appendix B, §28 *Modification of Contract Terms*, and §32 *Purchase Orders*, no preprinted terms or conditions on a Purchase Order issued by an Authorized User which seek to vary the terms of this Contract or impose new duties or obligations on the Contractor shall have any force and effect.

CONTRACTOR SIGNATURE PAGE

IN WITNESS WHEREOF, the parties therefore hereby execute their mutual agreement to the terms of this Contract. This agreement shall be executed and shall be a binding Contract between the parties as set forth in Appendix B, §26 *Contract Creation/Execution*. The State further warrants that, where Contractor is asked to execute multiple original copies of this signature page along with a complete original copy of the Contract, the approved signature page(s) will be affixed by the State, upon receipt of all necessary approvals, to additional copies of this Contract which conform exactly to the complete original copy as submitted by Contractor and executed simultaneously therewith.

CONTRACTOR

Signature: _____

Printed Name: Charles Shannon

Title: COO

Company Name: PerfectCommerce, LLC

Federal ID: 26-0557687

NYS Vendor ID: 1100114416

THE PEOPLE OF THE STATE OF NEW YORK

Signature: _____

Printed Name: Sergio Panzone

Title: Chief Procurement Officer

The acknowledgment must be fully and properly executed by an authorized person. By signing you certify your express authority to sign on behalf of yourself, your company, or other entity and full knowledge and acceptance of this agreement, Appendix A (Standard Clauses For New York State Contracts), Appendix B (OGS General Specifications), and State Finance Law §139-j and §139-k (Procurement Lobbying), and that all information provided is complete, true and accurate. By signing, bidder affirms that it understands and agrees to comply with the OGS procedures relative to permissible contacts as required by State Finance Law §139-j (3) and §139-j (6) (b).

INDIVIDUAL, CORPORATION, PARTNERSHIP, OR LLC ACKNOWLEDGMENT

STATE OF }

: **Sworn Statement:**

COUNTY OF }

On the 17 day of October in the year 2014, before me personally appeared Charles Shannon, known to me to be the person who executed the foregoing instrument, who, being duly sworn by me did depose and say that _he maintains an office at

Town of Newport News

County of _____, State of VA; and further that:

[Check One]

(☐ **If an individual):** _he executed the foregoing instrument in his/her name and on his/her own behalf.

(☐ **If a corporation):** _he is the _____ of _____, the corporation described in said instrument; that, by authority of the Board of Directors of said corporation, _he is authorized to execute the foregoing instrument on behalf of the corporation for purposes set forth therein; and that, pursuant to that authority, _he executed the foregoing instrument in the name of and on behalf of said corporation as the act and deed of said corporation.

(☐ **If a partnership):** _he is the _____ of _____, the partnership described in said instrument; that, by the terms of said partnership, _he is authorized to execute the foregoing instrument on behalf of the partnership for purposes set forth therein; and that, pursuant to that authority, _he executed the foregoing instrument in the name of and on behalf of said partnership as the act and deed of said partnership.

(☒ **If a limited liability company):** _he is a duly authorized member of Perfect Commerce, LLC _____, LLC, the limited liability company described in said instrument; that, _he is authorized to execute the foregoing instrument on behalf of the limited liability company for purposes set forth therein; and that, pursuant to that authority, _he executed the foregoing instrument in the name of and on behalf of said limited liability company as the act and deed of said limited liability company.

Stacy Leithead

Signature of Notary Public

STACY L LEITHEAD
NOTARY PUBLIC
REG. #7541499
COMMONWEALTH OF VIRGINIA
MY COMMISSION EXPIRES MARCH 31, 2017

APPENDIX A

STANDARD CLAUSES FOR NEW YORK STATE CONTRACTS

PLEASE RETAIN THIS DOCUMENT
FOR FUTURE REFERENCE.

January 2014

TABLE OF CONTENTS

		Page
1.	Executory Clause	3
2.	Non-Assignment Clause	3
3.	Comptroller's Approval	3
4.	Workers' Compensation Benefits	3
5.	Non-Discrimination Requirements	3
6.	Wage and Hours Provisions	3
7.	Non-Collusive Bidding Certification	4
8.	International Boycott Prohibition	4
9.	Set-Off Rights	4
10.	Records	4
11.	Identifying Information and Privacy Notification	4
12.	Equal Employment Opportunities For Minorities and Women	4-5
13.	Conflicting Terms	5
14.	Governing Law	5
15.	Late Payment	5
16.	No Arbitration	5
17.	Service of Process	5
18.	Prohibition on Purchase of Tropical Hardwoods	5-6
19.	MacBride Fair Employment Principles	6
20.	Omnibus Procurement Act of 1992	6
21.	Reciprocity and Sanctions Provisions	6
22.	Compliance with New York State Information Security Breach and Notification Act	6
23.	Compliance with Consultant Disclosure Law	6
24.	Procurement Lobbying	7
25.	Certification of Registration to Collect Sales and Compensating Use Tax by Certain State Contractors, Affiliates and Subcontractors	7
26.	Iran Divestment Act	7

STANDARD CLAUSES FOR NYS CONTRACTS

The parties to the attached contract, license, lease, amendment or other agreement of any kind (hereinafter, "the contract" or "this contract") agree to be bound by the following clauses which are hereby made a part of the contract (the word "Contractor" herein refers to any party other than the State, whether a contractor, licenser, licensee, lessor, lessee or any other party):

1. EXECUTORY CLAUSE. In accordance with Section 41 of the State Finance Law, the State shall have no liability under this contract to the Contractor or to anyone else beyond funds appropriated and available for this contract.

2. NON-ASSIGNMENT CLAUSE. In accordance with Section 138 of the State Finance Law, this contract may not be assigned by the Contractor or its right, title or interest therein assigned, transferred, conveyed, sublet or otherwise disposed of without the State's previous written consent, and attempts to do so are null and void. Notwithstanding the foregoing, such prior written consent of an assignment of a contract let pursuant to Article XI of the State Finance Law may be waived at the discretion of the contracting agency and with the concurrence of the State Comptroller where the original contract was subject to the State Comptroller's approval, where the assignment is due to a reorganization, merger or consolidation of the Contractor's business entity or enterprise. The State retains its right to approve an assignment and to require that any Contractor demonstrate its responsibility to do business with the State. The Contractor may, however, assign its right to receive payments without the State's prior written consent unless this contract concerns Certificates of Participation pursuant to Article 5-A of the State Finance Law.

3. COMPTROLLER'S APPROVAL. In accordance with Section 112 of the State Finance Law (or, if this contract is with the State University or City University of New York, Section 355 or Section 6218 of the Education Law), if this contract exceeds $50,000 (or the minimum thresholds agreed to by the Office of the State Comptroller for certain S.U.N.Y. and C.U.N.Y. contracts), or if this is an amendment for any amount to a contract which, as so amended, exceeds said statutory amount, or if, by this contract, the State agrees to give something other than money when the value or reasonably estimated value of such consideration exceeds $10,000, it shall not be valid, effective or binding upon the State until it has been approved by the State Comptroller and filed in his office. Comptroller's approval of contracts let by the Office of General Services is required when such contracts exceed $85,000 (State Finance Law Section 163.6-a). However, such pre-approval shall not be required for any contract established as a centralized contract through the Office of General Services or for a purchase order or other transaction issued under such centralized contract.

4. WORKERS' COMPENSATION BENEFITS. In accordance with Section 142 of the State Finance Law, this contract shall be void and of no force and effect unless the Contractor shall provide and maintain coverage during the life of this contract for the benefit of such employees as are required to be covered by the provisions of the Workers' Compensation Law.

5. NON-DISCRIMINATION REQUIREMENTS. To the extent required by Article 15 of the Executive Law (also known as the Human Rights Law) and all other State and Federal statutory and constitutional non-discrimination provisions, the Contractor will not discriminate against any employee or applicant for employment because of race, creed, color, sex (including gender identity or expression), national origin, sexual orientation, military status, age, disability, predisposing genetic characteristics, marital status or domestic violence victim status. Furthermore, in accordance with Section 220-e of the Labor Law, if this is a contract for the construction, alteration or repair of any public building or public work or for the manufacture, sale or distribution of materials, equipment or supplies, and to the extent that this contract shall be performed within the State of New York, Contractor agrees that neither it nor its subcontractors shall,-by reason of race, creed, color, disability, sex, or national origin: (a) discriminate in hiring against any New York State citizen who is qualified and available to perform the work; or (b) discriminate against or intimidate any employee hired for the performance of work under this contract. If this is a building service contract as defined in Section 230 of the Labor Law, then, in accordance with Section 239 thereof, Contractor agrees that neither it nor its subcontractors shall by reason of race, creed, color, national origin, age, sex or disability: (a) discriminate in hiring against any New York State citizen who is qualified and available to perform the work; or (b) discriminate against or intimidate any employee hired for the performance of work under this contract. Contractor is subject to fines of $50.00 per person per day for any violation of Section 220-e or Section 239 as well as possible termination of this contract and forfeiture of all moneys due hereunder for a second or subsequent violation.

6. WAGE AND HOURS PROVISIONS. If this is a public work contract covered by Article 8 of the Labor Law or a building service contract covered by Article 9 thereof, neither Contractor's employees nor the employees of its subcontractors may be required or permitted to work more than the number of hours or days stated in said statutes, except as otherwise provided in the Labor Law and as set forth in prevailing wage and supplement schedules issued by the State Labor Department. Furthermore, Contractor and its subcontractors must pay at least the prevailing wage rate and pay or provide the prevailing supplements, including the premium rates for overtime pay, as determined by the State Labor Department in accordance with the Labor Law. Additionally, effective April 28, 2008, if this is a public work contract covered by Article 8 of the Labor Law, the Contractor

understands and agrees that the filing of payrolls in a manner consistent with Subdivision 3-a of Section 220 of the Labor Law shall be a condition precedent to payment by the State of any State approved sums due and owing for work done upon the project.

7. **NON-COLLUSIVE BIDDING CERTIFICATION.** In accordance with Section 139-d of the State Finance Law, if this contract was awarded based upon the submission of bids, Contractor affirms, under penalty of perjury, that its bid was arrived at independently and without collusion aimed at restricting competition. Contractor further affirms that, at the time Contractor submitted its bid, an authorized and responsible person executed and delivered to the State a non-collusive bidding certification on Contractor's behalf.

8. **INTERNATIONAL BOYCOTT PROHIBITION.** In accordance with Section 220-f of the Labor Law and Section 139-h of the State Finance Law, if this contract exceeds $5,000, the Contractor agrees, as a material condition of the contract, that neither the Contractor nor any substantially owned or affiliated person, firm, partnership or corporation has participated, is participating, or shall participate in an international boycott in violation of the federal Export Administration Act of 1979 (50 USC App. Sections 2401 et seq.) or regulations thereunder. If such Contractor, or any of the aforesaid affiliates of Contractor, is convicted or is otherwise found to have violated said laws or regulations upon the final determination of the United States Commerce Department or any other appropriate agency of the United States subsequent to the contract's execution, such contract, amendment or modification thereto shall be rendered forfeit and void. The Contractor shall so notify the State Comptroller within five (5) business days of such conviction, determination or disposition of appeal (2NYCRR 105.4).

9. **SET-OFF RIGHTS.** The State shall have all of its common law, equitable and statutory rights of set-off. These rights shall include, but not be limited to, the State's option to withhold for the purposes of set-off any moneys due to the Contractor under this contract up to any amounts due and owing to the State with regard to this contract, any other contract with any State department or agency, including any contract for a term commencing prior to the term of this contract, plus any amounts due and owing to the State for any other reason including, without limitation, tax delinquencies, fee delinquencies or monetary penalties relative thereto. The State shall exercise its set-off rights in accordance with normal State practices including, in cases of set-off pursuant to an audit, the finalization of such audit by the State agency, its representatives, or the State Comptroller.

10. **RECORDS.** The Contractor shall establish and maintain complete and accurate books, records, documents, accounts and other evidence directly pertinent to performance under this contract (hereinafter, collectively, "the Records"). The Records must be kept for the balance of the calendar year in which they were made and for six (6) additional years thereafter. The State Comptroller, the Attorney General and any other person or entity authorized to conduct an examination, as well as the agency or agencies involved in this contract, shall have access to the Records during normal business hours at an office of the Contractor within the State of New York or, if no such office is available, at a mutually agreeable and reasonable venue within the State, for the term specified above for the purposes of inspection, auditing and copying. The State shall take reasonable steps to protect from public disclosure any of the Records which are exempt from disclosure under Section 87 of the Public Officers Law (the "Statute") provided that: (i) the Contractor shall timely inform an appropriate State official, in writing, that said records should not be disclosed; and (ii) said records shall be sufficiently identified; and (iii) designation of said records as exempt under the Statute is reasonable. Nothing contained herein shall diminish, or in any way adversely affect, the State's right to discovery in any pending or future litigation.

11. **IDENTIFYING INFORMATION AND PRIVACY NOTIFICATION.** (a) Identification Number(s). Every invoice or New York State Claim for Payment submitted to a New York State agency by a payee, for payment for the sale of goods or services or for transactions (e.g., leases, easements, licenses, etc.) related to real or personal property must include the payee's identification number. The number is any or all of the following: (i) the payee's Federal employer identification number, (ii) the payee's Federal social security number, and/or (iii) the payee's Vendor Identification Number assigned by the Statewide Financial System. Failure to include such number or numbers may delay payment. Where the payee does not have such number or numbers, the payee, on its invoice or Claim for Payment, must give the reason or reasons why the payee does not have such number or numbers.

(b) Privacy Notification. (1) The authority to request the above personal information from a seller of goods or services or a lessor of real or personal property, and the authority to maintain such information, is found in Section 5 of the State Tax Law. Disclosure of this information by the seller or lessor to the State is mandatory. The principal purpose for which the information is collected is to enable the State to identify individuals, businesses and others who have been delinquent in filing tax returns or may have understated their tax liabilities and to generally identify persons affected by the taxes administered by the Commissioner of Taxation and Finance. The information will be used for tax administration purposes and for any other purpose authorized by law. (2) The personal information is requested by the purchasing unit of the agency contracting to purchase the goods or services or lease the real or personal property covered by this contract or lease. The information is maintained in the Statewide Financial System by the Vendor Management Unit within the Bureau of State Expenditures, Office of the State Comptroller, 110 State Street, Albany, New York 12236.

12. **EQUAL EMPLOYMENT OPPORTUNITIES FOR MINORITIES AND WOMEN.** In accordance with Section

312 of the Executive Law and 5 NYCRR 143, if this contract is: (i) a written agreement or purchase order instrument, providing for a total expenditure in excess of $25,000.00, whereby a contracting agency is committed to expend or does expend funds in return for labor, services, supplies, equipment, materials or any combination of the foregoing, to be performed for, or rendered or furnished to the contracting agency; or (ii) a written agreement in excess of $100,000.00 whereby a contracting agency is committed to expend or does expend funds for the acquisition, construction, demolition, replacement, major repair or renovation of real property and improvements thereon; or (iii) a written agreement in excess of $100,000.00 whereby the owner of a State assisted housing project is committed to expend or does expend funds for the acquisition, construction, demolition, replacement, major repair or renovation of real property and improvements thereon for such project, then the following shall apply and by signing this agreement the Contractor certifies and affirms that it is Contractor's equal employment opportunity policy that:

(a) The Contractor will not discriminate against employees or applicants for employment because of race, creed, color, national origin, sex, age, disability or marital status, shall make and document its conscientious and active efforts to employ and utilize minority group members and women in its work force on State contracts and will undertake or continue existing programs of affirmative action to ensure that minority group members and women are afforded equal employment opportunities without discrimination. Affirmative action shall mean recruitment, employment, job assignment, promotion, upgradings, demotion, transfer, layoff, or termination and rates of pay or other forms of compensation;

(b) at the request of the contracting agency, the Contractor shall request each employment agency, labor union, or authorized representative of workers with which it has a collective bargaining or other agreement or understanding, to furnish a written statement that such employment agency, labor union or representative will not discriminate on the basis of race, creed, color, national origin, sex, age, disability or marital status and that such union or representative will affirmatively cooperate in the implementation of the Contractor's obligations herein; and

(c) the Contractor shall state, in all solicitations or advertisements for employees, that, in the performance of the State contract, all qualified applicants will be afforded equal employment opportunities without discrimination because of race, creed, color, national origin, sex, age, disability or marital status.

Contractor will include the provisions of "a", "b", and "c" above, in every subcontract over $25,000.00 for the construction, demolition, replacement, major repair, renovation, planning or design of real property and improvements thereon (the "Work") except where the Work is for the beneficial use of the Contractor. Section 312 does not apply to: (i) work, goods or services unrelated to this contract; or (ii) employment outside New York State. The State shall consider compliance by a contractor or subcontractor with the requirements of any federal law concerning equal employment opportunity which effectuates the purpose of this section. The contracting agency shall determine whether the imposition of the requirements of the provisions hereof duplicate or conflict with any such federal law and if such duplication or conflict exists, the contracting agency shall waive the applicability of Section 312 to the extent of such duplication or conflict. Contractor will comply with all duly promulgated and lawful rules and regulations of the Department of Economic Development's Division of Minority and Women's Business Development pertaining hereto.

13. CONFLICTING TERMS. In the event of a conflict between the terms of the contract (including any and all attachments thereto and amendments thereof) and the terms of this Appendix A, the terms of this Appendix A shall control.

14. GOVERNING LAW. This contract shall be governed by the laws of the State of New York except where the Federal supremacy clause requires otherwise.

15. LATE PAYMENT. Timeliness of payment and any interest to be paid to Contractor for late payment shall be governed by Article 11-A of the State Finance Law to the extent required by law.

16. NO ARBITRATION. Disputes involving this contract, including the breach or alleged breach thereof, may not be submitted to binding arbitration (except where statutorily authorized), but must, instead, be heard in a court of competent jurisdiction of the State of New York.

17. SERVICE OF PROCESS. In addition to the methods of service allowed by the State Civil Practice Law & Rules ("CPLR"), Contractor hereby consents to service of process upon it by registered or certified mail, return receipt requested. Service hereunder shall be complete upon Contractor's actual receipt of process or upon the State's receipt of the return thereof by the United States Postal Service as refused or undeliverable. Contractor must promptly notify the State, in writing, of each and every change of address to which service of process can be made. Service by the State to the last known address shall be sufficient. Contractor will have thirty (30) calendar days after service hereunder is complete in which to respond.

18. PROHIBITION ON PURCHASE OF TROPICAL HARDWOODS. The Contractor certifies and warrants that all wood products to be used under this contract award will be in accordance with, but not limited to, the specifications and provisions of Section 165 of the State Finance Law, (Use of Tropical Hardwoods) which prohibits purchase and use of tropical hardwoods, unless specifically exempted, by the State or any governmental agency or political subdivision or public benefit corporation. Qualification for an exemption under this

law will be the responsibility of the contractor to establish to meet with the approval of the State.

In addition, when any portion of this contract involving the use of woods, whether supply or installation, is to be performed by any subcontractor, the prime Contractor will indicate and certify in the submitted bid proposal that the subcontractor has been informed and is in compliance with specifications and provisions regarding use of tropical hardwoods as detailed in §165 State Finance Law. Any such use must meet with the approval of the State; otherwise, the bid may not be considered responsive. Under bidder certifications, proof of qualification for exemption will be the responsibility of the Contractor to meet with the approval of the State.

19. MACBRIDE FAIR EMPLOYMENT PRINCIPLES. In accordance with the MacBride Fair Employment Principles (Chapter 807 of the Laws of 1992), the Contractor hereby stipulates that the Contractor either (a) has no business operations in Northern Ireland, or (b) shall take lawful steps in good faith to conduct any business operations in Northern Ireland in accordance with the MacBride Fair Employment Principles (as described in Section 165 of the New York State Finance Law), and shall permit independent monitoring of compliance with such principles.

20. OMNIBUS PROCUREMENT ACT OF 1992. It is the policy of New York State to maximize opportunities for the participation of New York State business enterprises, including minority and women-owned business enterprises as bidders, subcontractors and suppliers on its procurement contracts.

Information on the availability of New York State subcontractors and suppliers is available from:

NYS Department of Economic Development
Division for Small Business
Albany, New York 12245
Telephone: 518-292-5100
Fax: 518-292-5884
email: opa@esd.ny.gov

A directory of certified minority and women-owned business enterprises is available from:

NYS Department of Economic Development
Division of Minority and Women's Business Development
633 Third Avenue
New York, NY 10017
212-803-2414
email: mwbecertification@esd.ny.gov
https://ny.newnycontracts.com/FrontEnd/VendorSearchPublic.asp

The Omnibus Procurement Act of 1992 requires that by signing this bid proposal or contract, as applicable, Contractors certify that whenever the total bid amount is greater than $1 million:

(a) The Contractor has made reasonable efforts to encourage the participation of New York State Business Enterprises as suppliers and subcontractors, including certified minority and women-owned business enterprises, on this project, and has retained the documentation of these efforts to be provided upon request to the State;

(b) The Contractor has complied with the Federal Equal Opportunity Act of 1972 (P.L. 92-261), as amended;

(c) The Contractor agrees to make reasonable efforts to provide notification to New York State residents of employment opportunities on this project through listing any such positions with the Job Service Division of the New York State Department of Labor, or providing such notification in such manner as is consistent with existing collective bargaining contracts or agreements. The Contractor agrees to document these efforts and to provide said documentation to the State upon request; and

(d) The Contractor acknowledges notice that the State may seek to obtain offset credits from foreign countries as a result of this contract and agrees to cooperate with the State in these efforts.

21. RECIPROCITY AND SANCTIONS PROVISIONS. Bidders are hereby notified that if their principal place of business is located in a country, nation, province, state or political subdivision that penalizes New York State vendors, and if the goods or services they offer will be substantially produced or performed outside New York State, the Omnibus Procurement Act 1994 and 2000 amendments (Chapter 684 and Chapter 383, respectively) require that they be denied contracts which they would otherwise obtain. NOTE: As of May 15, 2002, the list of discriminatory jurisdictions subject to this provision includes the states of South Carolina, Alaska, West Virginia, Wyoming, Louisiana and Hawaii. Contact NYS Department of Economic Development for a current list of jurisdictions subject to this provision.

22. COMPLIANCE WITH NEW YORK STATE INFORMATION SECURITY BREACH AND NOTIFICATION ACT. Contractor shall comply with the provisions of the New York State Information Security Breach and Notification Act (General Business Law Section 899-aa; State Technology Law Section 208).

23. COMPLIANCE WITH CONSULTANT DISCLOSURE LAW. If this is a contract for consulting services, defined for purposes of this requirement to include analysis, evaluation, research, training, data processing, computer programming, engineering, environmental, health, and mental health services, accounting, auditing, paralegal, legal or similar services, then, in accordance with Section 163 (4-g) of the State Finance Law (as amended by Chapter 10 of

the Laws of 2006), the Contractor shall timely, accurately and properly comply with the requirement to submit an annual employment report for the contract to the agency that awarded the contract, the Department of Civil Service and the State Comptroller.

24. PROCUREMENT LOBBYING. To the extent this agreement is a "procurement contract" as defined by State Finance Law Sections 139-j and 139-k, by signing this agreement the contractor certifies and affirms that all disclosures made in accordance with State Finance Law Sections 139-j and 139-k are complete, true and accurate. In the event such certification is found to be intentionally false or intentionally incomplete, the State may terminate the agreement by providing written notification to the Contractor in accordance with the terms of the agreement.

25. CERTIFICATION OF REGISTRATION TO COLLECT SALES AND COMPENSATING USE TAX BY CERTAIN STATE CONTRACTORS, AFFILIATES AND SUBCONTRACTORS.
To the extent this agreement is a contract as defined by Tax Law Section 5-a, if the contractor fails to make the certification required by Tax Law Section 5-a or if during the term of the contract, the Department of Taxation and Finance or the covered agency, as defined by Tax Law 5-a, discovers that the certification, made under penalty of perjury, is false, then such failure to file or false certification shall be a material breach of this contract and this contract may be terminated, by providing written notification to the Contractor in accordance with the terms of the agreement, if the covered agency determines that such action is in the best interest of the State.

26. **IRAN DIVESTMENT ACT**. By entering into this Agreement, Contractor certifies in accordance with State Finance Law §165-a that it is not on the "Entities Determined to be Non-Responsive Bidders/Offerers pursuant to the New York State Iran Divestment Act of 2012" ("Prohibited Entities List") posted at:
http://www.ogs.ny.gov/about/regs/docs/ListofEntities.pdf

Contractor further certifies that it will not utilize on this Contract any subcontractor that is identified on the Prohibited Entities List. Contractor agrees that should it seek to renew or extend this Contract, it must provide the same certification at the time the Contract is renewed or extended. Contractor also agrees that any proposed Assignee of this Contract will be required to certify that it is not on the Prohibited Entities List before the contract assignment will be approved by the State.

During the term of the Contract, should the state agency receive information that a person (as defined in State Finance Law §165-a) is in violation of the above-referenced certifications, the state agency will review such information and offer the person an opportunity to respond. If the person fails to demonstrate that it has ceased its engagement in the investment activity which is in violation of the Act within 90 days after the determination of such violation, then the state agency shall take such action as may be appropriate and provided for by law, rule, or contract, including, but not limited to, imposing sanctions, seeking compliance, recovering damages, or declaring the Contractor in default.

The state agency reserves the right to reject any bid, request for assignment, renewal or extension for an entity that appears on the Prohibited Entities List prior to the award, assignment, renewal or extension of a contract, and to pursue a responsibility review with respect to any entity that is awarded a contract and appears on the Prohibited Entities list after contract award.

APPENDIX B

GENERAL SPECIFICATIONS

TABLE OF CONTENTS

GENERAL — **PAGE**

1. Ethics Compliance 1
2. Definitions 1

BID SUBMISSION

3. International Bidding 2
4. Bid Opening 2
5. Bid Submission 2
6. Late Bids Rejected 3
7. Bid Contents 3
8. Extraneous Terms 3
9. Confidential/Trade Secret Materials 3
10. Prevailing Wage Rates - Public Works and Building Services Contracts 3
11. Taxes 4
12. Expenses Prior to Contract Execution 4
13. Advertising Results 4
14. Product References 4
15. Remanufactured, Recycled, Recyclable Or Recovered Materials 5
16. Products Manufactured in Public Institutions 5
17. Pricing 5
18. Drawings 5
19. Site Inspection 6
20. Procurement Card 6
21. Samples 6

BID EVALUATION

22. Bid Evaluation 6
23. Tie Bids 6
24. Quantity Changes Prior To Award 6
25. Timeframe for Offers 7

TERMS & CONDITIONS

26. Contract Creation/Execution 7
27. Participation in Centralized Contracts 7
28. Modification of Contract Terms 7
29. Scope Changes 7
30. Estimated/Specific Quantity Contracts 7
31. Emergency Contracts 7
32. Purchase Orders 8
33. Product Delivery 8
34. Weekend and Holiday Deliveries 8
35. Shipping/Receipt of Product 8

TERMS & CONDITIONS (CONT.) — **PAGE**

36. Title and Risk of Loss 8
37. Re-Weighing Product 8
38. Product Substitution 8
39. Rejected Product 9
40. Installation 9
41. Repaired or Replaced Product/ Components 9
42. Employees/Subcontractors/Agents 9
43. Assignment 9
44. Subcontractors and Suppliers 9
45. Performance/Bid Bond 9
46. Suspension of Work 9
47. Termination 10
48. Savings/Force Majeure 10
49. Contract Invoicing 11
50. Default - Authorized User 11
51. Prompt Payments 11
52. Remedies for Breach 11
53. Assignment of Claim 12
54. Toxic Substances 12
55. Independent Contractor 12
56. Security 12
57. Cooperation with Third Parties 12
58. Contract Term - Renewal 12
59. Warranties 12
60. Legal Compliance 13
61. Indemnification 13
62. Indemnification Relating to Third Party Rights 14
63. Limitation of Liability 14
64. Disputes 14

THE FOLLOWING CLAUSES PERTAIN TO TECHNOLOGY & NEGOTIATED CONTRACTS

65. Software License Grant 16
66. Product Acceptance 17
67. Audit of Licensed Product Usage 17
68. Ownership/Title to Project Deliverables 17
69. Proof of License 18
70. Product Version 18
71. Changes to Product or Service Offerings 19
72. No Hardstop/Passive License Monitoring 19
73. Source Code Escrow for Licensed Product 19

GENERAL

1. ETHICS COMPLIANCE All Bidders/Contractors and their employees must comply with the requirements of Sections 73 and 74 of the Public Officers Law, other State codes, rules, regulations and executive orders establishing ethical standards for the conduct of business with New York State. In signing the Bid, Bidder certifies full compliance with those provisions for any present or future dealings, transactions, sales, contracts, services, offers, relationships, etc., involving New York State and/or its employees. Failure to comply with those provisions may result in disqualification from the Bidding process, termination of contract, and/or other civil or criminal proceedings as required by law.

2. DEFINITIONS Terms used herein shall have the following meanings:

a. AGENCY OR AGENCIES The State of New York, acting by or through one or more departments, boards, commissions, offices or institutions of the State of New York.

b. AUTHORIZED USER(S) Authorized User shall have the meaning set forth in New York State Finance Law section 163(1)(k) and includes, but is not limited to, New York State agencies, political subdivisions, local governments, public authorities, public school and fire districts, public and nonprofit libraries, and certain other nonpublic/nonprofit organizations.

c. COMMISSIONER Commissioner of OGS, or in the case of Bid Specifications issued by an Authorized User, the head of such Authorized User or his or her authorized representative.

d. CONTRACT The writing(s) which contain the agreement of the Commissioner and the bidder/Contractor setting forth the total legal obligation between the parties as determined by applicable rules of law, and which most typically include the following classifications of public procurements:

1. **Agency Specific Contracts** Contracts where the specifications for a Product or a particular scope of work are described and defined to meet the needs of one or more Authorized User(s).

2. **Centralized Contracts** Single or multiple award Contracts where the specifications for a Product or general scope of work are described and defined by the Office of General Services to meet the needs of Authorized Users. Centralized Contracts may be awarded through multiple awards or through adoption of another jurisdiction's contract or on a sole source, single source, emergency or competitive basis. Once established, procurements may be made from the selected Contractor(s) without further competition or Mini-Bid unless otherwise required by the Bid Specifications or Contract Award Notification.

3. **Back-Drop Contracts** Multiple award Centralized Contracts where the Office of General Services defines the specifications for a Product or general scope of work to meet the needs of Authorized Users. Bids may be submitted either at a date and time certain or may be accepted on a continuous or periodic recruitment basis, as set forth in the Bid Specifications. Selection of a Contractor(s) from among Back-Drop contract holders for an actual Product, project or particular scope of work may subsequently be made on a single or sole source basis, or on the basis of a Mini-Bid among qualified Back-Drop contract holders, or such other method as set forth in the Bid Document.

4. **Piggyback Contract** A Contract let by any department, agency or instrumentality of the United States government, or any department, agency, office, political subdivision or instrumentality of any state or state(s) which is adopted and extended for use by the OGS Commissioner in accordance with the requirements of the State Finance Law.

5. **Contract Letter** A letter to the successful Bidder(s) indicating acceptance of its Bid in response to a solicitation. Unless otherwise specified, the issuance of a Letter of Acceptance forms a Contract but is not an order for Product, and Contractor should not take any action with respect to actual Contract deliveries except on the basis of Purchase Orders sent from Authorized User(s).

e CONTRACT AWARD NOTIFICATION An announcement to Authorized Users that a Contract has been established.

f. CONTRACTOR Any successful Bidder(s) to whom a Contract has been awarded by the Commissioner.

g. DOCUMENTATION The complete set of manuals (e.g., user, installation, instruction or diagnostic manuals) in either hard or electronic copy, which are necessary to enable an Authorized User to properly test, install, operate and enjoy full use of the Product.

h. EMERGENCY An urgent and unexpected requirement where health and public safety or the conservation of public resources is at risk.

i. ENTERPRISE The total business operations in the United States of Authorized User(s) without regard to geographic location where such operations are performed or the entity actually performing such operations on behalf of Authorized User(s).

j. ENTERPRISE LICENSE A license grant of unlimited rights to deploy, access, use and execute Product anywhere within the Enterprise up to the maximum capacity stated on the Purchase Order or in the Contract.

k. ERROR CORRECTIONS Machine executable software code furnished by Contractor which corrects the Product so as to conform to the applicable warranties, performance standards and/or obligations of the Contractor.

l. GROUP A classification of Product, services or technology which is designated by OGS.

m. INVITATION FOR BIDS (IFB) A type of Bid Document which is most typically used for procurements where requirements can be stated and award will be made based on lowest price to the responsive and responsible Bidder(s).

n. LICENSED SOFTWARE Software transferred upon the terms and conditions set forth in the Contract. "Licensed Software" includes error corrections, upgrades, enhancements or new releases, and any deliverables due under a maintenance or service contract (e.g., patches, fixes, PTFs, programs, code or data conversion, or custom programming).

o. LICENSEE(S) One or more Authorized Users who acquire Product from Contractor by issuing a Purchase Order in accordance with the terms and conditions of the Contract; provided that, for

purposes of compliance with an individual license, the term "Licensee(s)" shall be deemed to refer separately to the individual Authorized User(s) who took receipt of and who is executing the Product, and who shall be solely responsible for performance and liabilities incurred. In the case of acquisitions by State Agencies, the Licensee shall be the State of New York.

p. LICENSE EFFECTIVE DATE The date Product is delivered to an Authorized User. Where a License involves Licensee's right to copy a previously licensed and delivered Master Copy of a Program, the license effective date for additional copies shall be deemed to be the date on which the Purchase Order is executed.

q. LICENSOR A Contractor who transfers rights in proprietary Product to Authorized Users in accordance with the rights and obligations specified in the Contract.

r. NEW PRODUCT RELEASES (Product Revisions) Any commercially released revisions to the licensed version of a Product as may be generally offered and available to Authorized Users. New releases involve a substantial revision of functionality from a previously released version of the Product.

s. OGS The New York State Office of General Services.

t. PRODUCT A deliverable under any Bid or Contract which may include commodities, services and/or technology. The term "Product" includes Licensed Software.

u. PROPRIETARY Protected by secrecy, patent, copyright or trademark against commercial competition.

v. PURCHASE ORDER The Authorized User's fiscal form or format that is used when making a purchase (e.g., formal written Purchase Order, Procurement Card, electronic Purchase Order, or other authorized instrument).

w. REQUEST FOR PROPOSALS (RFP) A type of Bid Document that is used for procurements where factors in addition to cost are considered and weighted in awarding the contract and where the award will be made based on "best value," as defined by the State Finance Law, to the responsive and responsible Bidder(s).

x. REQUEST FOR QUOTATION (RFQ) A type of Bid Document that can be used when a formal Bid opening is not required (e.g., discretionary, sole source, single source or emergency purchases).

y. RESPONSIBLE BIDDER A Bidder that is determined to have financial and organizational capacity, legal authority, satisfactory previous performance, skill, judgment and integrity, and that is found to be competent, reliable and experienced, as determined by the Commissioner. For purposes of being deemed responsible, a Bidder must also be determined to be in compliance with Sections 139-j and 139-k of the State Finance Law relative to restrictions on contacts during the procurement process and disclosure of contacts and prior findings of non-responsibility under these statutes.

z. RESPONSIVE BIDDER A Bidder meeting the specifications or requirements prescribed in the Bid Document or solicitation, as determined by the OGS Commissioner.

aa. SINGLE SOURCE A procurement where two or more Bidders can supply the required Product, and the Commissioner may award the contract to one Bidder over the other.

bb. SITE The location (street address) where Product will be executed or services delivered.

cc. SOLE SOURCE A procurement where only one Bidder is capable of supplying the required Product.

dd. SOURCE CODE The programming statements or instructions written and expressed in any language understandable by a human being skilled in the art which are translated by a language compiler to produce executable machine Object Code.

ee. STATE State of New York.

ff. SUBCONTRACTOR Any individual or other legal entity (including but not limited to sole proprietor, partnership, limited liability company, firm or corporation) who has entered into a contract, express or implied, for the performance of a portion of a Contract with a Contractor.

gg. TERMS OF LICENSE The terms and conditions set forth in the Contract that are in effect and applicable to a Purchase Order at the time of order placement.

hh. VIRUS Any computer code, whether or not written or conceived by Contractor, that disrupts, disables, harms, or otherwise impedes in any manner the operation of the Product, or any other associated software, firmware, hardware, or computer system (such as local area or wide-area networks), including aesthetic disruptions or distortions, but does not include security keys or other such devices installed by Product manufacturer.

BID SUBMISSION

3. INTERNATIONAL BIDDING All offers (tenders), and all information and Product required by the solicitation or provided as explanation thereof, shall be submitted in English. All prices shall be expressed, and all payments shall be made, in United States Dollars ($US). Any offers (tenders) submitted which do not meet the above criteria will be rejected.

4. BID OPENING Bids may, as applicable, be opened publicly. The Commissioner reserves the right at any time to postpone or cancel a scheduled Bid opening.

5. BID SUBMISSION All Bids are to be packaged, sealed and submitted to the location stated in the Bid Specifications. Bidders are solely responsible for timely delivery of their Bids to the location set forth in the Bid Specifications prior to the stated Bid opening date/time.

A Bid return envelope, if provided with the Bid Specifications, should be used with the Bid sealed inside. If the Bid response does not fit into the envelope, the Bid envelope should be attached to the outside of the sealed box or package with the Bid inside. If using a commercial delivery company that requires use of their shipping package or envelope, Bidder's sealed Bid, labeled as detailed below, should be placed within the shipper's sealed envelope to ensure that the Bid is not prematurely opened.

All Bids must have a label on the outside of the package or shipping container outlining the following information:

"**BID ENCLOSED** (bold print, all capitals)

- Group Number

- IFB or RFP Number
- Bid Submission date and time"

In the event that a Bidder fails to provide such information on the return Bid envelope or shipping material, the receiving entity reserves the right to open the shipping package or envelope to determine the proper Bid number or Group Number, and the date and time of Bid opening. Bidder shall have no claim against the receiving entity arising from such opening and such opening shall not affect the validity of the Bid or the procurement.

Bidder assumes all risk of late delivery associated with the Bid not being identified, packaged or labeled in accordance with the foregoing requirements.

All Bids must be signed by a person authorized to commit the Bidder to the terms of the Bid Documents and the content of the Bid (offer).

6. LATE BIDS REJECTED For purposes of Bid openings held and conducted by OGS, a Bid must be received in such place as may be designated in the Bid Documents or, if no place is specified, in the OGS Mailroom located in the Empire State Plaza, Albany, New York 12242, at or before the date and time established in the Bid Specifications for the Bid opening. For purposes of Bid openings held and conducted by Authorized Users other than OGS, the term late Bid is defined as a Bid not received in the location established in the Bid Specifications at or before the date and time specified for the Bid opening.

Any Bid received at the specified location after the time specified will be considered a late Bid. A late Bid shall not be considered for award unless: (i) no timely Bids meeting the requirements of the Bid Documents are received or, (ii) in the case of a multiple award, an insufficient number of timely Bids were received to satisfy the multiple award; and acceptance of the late Bid is in the best interests of the Authorized Users. Bids submitted for continuous or periodic recruitment contract awards must meet the submission requirements associated with their specifications. Delays in United States mail deliveries or any other means of transmittal, including couriers or agents of the Authorized User, shall not excuse late Bid submissions. Similar types of delays, including but not limited to, bad weather, or security procedures for parking and building admittance, shall not excuse late Bid submissions. Determinations relative to Bid timeliness shall be at the sole discretion of the Commissioner.

7. BID CONTENTS Bids must be complete and legible. All Bids must be signed. All information required by the Bid Specifications must be supplied by the Bidder on the forms or in the format specified. No alteration, erasure or addition is to be made to the Bid Documents. Changes may be ignored by the Commissioner or may be grounds for rejection of the Bid. Changes, corrections and/or use of white-out in the Bid or Bidder's response portion of the Bid Document must be initialed by an authorized representative of the Bidder. Bidders are cautioned to verify their Bids before submission, as amendments to Bids or requests for withdrawal of Bids received by the Commissioner after the time specified for the Bid opening may not be considered.

8. EXTRANEOUS TERMS Bids must conform to the terms set forth in the Bid Documents, as extraneous terms or material deviations (including additional, inconsistent, conflicting or alternative terms) may render the Bid non-responsive and may result in rejection of the Bid.

Extraneous term(s) submitted on standard, pre-printed forms (including but not limited to: product literature, order forms, license agreements, contracts or other documents) that are attached or referenced with submissions shall not be considered part of the Bid or resulting Contract, but shall be deemed included for informational or promotional purposes only.

Only those extraneous terms that meet all the following requirements may be considered as having been submitted as part of the Bid:

a. Each proposed extraneous term (addition, deletion, counter-offer, deviation, or modification) must be specifically enumerated in a writing which is not part of a pre-printed form; and

b. The writing must identify the particular specification requirement (if any) that Bidder rejects or proposes to modify by inclusion of the extraneous term; and

c. The Bidder shall enumerate the proposed addition, deletion, counter-offer, deviation, or modification from the Bid Document, and the reasons therefore.

No extraneous term(s), whether or not deemed "material," shall be incorporated into a Contract or Purchase Order unless submitted in accordance with the above and the Commissioner or Authorized User expressly accepts each such term(s) in writing. Acceptance and/or processing of the Bid shall not constitute such written acceptance of Extraneous Term(s).

9. CONFIDENTIAL/TRADE SECRET MATERIALS

a. CONTRACTOR Confidential, trade secret or proprietary materials as defined by the laws of the State of New York must be clearly marked and identified as such upon submission by the Bidder. Marking the Bid as "confidential" or "proprietary" on its face or in the document header or footer shall not be considered by the Commissioner or Authorized User to be sufficient without specific justification as to why disclosure of particular information in the Bid would cause substantial injury to the competitive position of the Bidder. Bidders/Contractors intending to seek an exemption from disclosure of these materials under the Freedom of Information Law must request the exemption in writing, setting forth the reasons for the claimed exemption. The State's receipt/acceptance of the claimed materials does not constitute a determination on the exemption request, which determination will be made in accordance with statutory procedures. Properly identified information that has been designated confidential, trade secret, or proprietary by the Bidder will not be disclosed except as may be required by the Freedom of Information Law or other applicable State and federal laws.

b. COMMISSIONER OR AUTHORIZED USER Contractor warrants, covenants and represents that any confidential information obtained by Contractor, its agents, Subcontractors, officers, distributors, resellers or employees in the course of performing its obligations, including without limitation, security procedures, business operations information, or commercial proprietary information in the possession of the State or any Authorized User hereunder or received from another third party, will not be divulged to any third parties without the written consent of the Commissioner or Authorized User. Contractor shall not be required to keep confidential any such material that is publicly available through no fault of Contractor, independently developed by Contractor without reliance on confidential information of the Authorized User, or otherwise obtained under the Freedom of Information Law or other applicable New York State laws and regulations. This warranty shall survive termination of this Contract. Contractor further agrees to take commercially reasonable steps as to its agents, Subcontractors, officers, distributors, resellers or employees regarding the obligations arising under this clause to insure such confidentiality.

10. PREVAILING WAGE RATES - PUBLIC WORKS AND BUILDING SERVICES CONTRACTS If any portion of work being Bid is subject to the prevailing wage rate provisions of the Labor Law, the following shall apply:

a. PREVAILING WAGE RATE APPLICABLE TO BID SUBMISSIONS A copy of the applicable prevailing wage rates to be paid or provided are annexed to the Bid Documents. Bidders must submit Bids which are based upon the prevailing hourly wages, and supplements in cash or equivalent benefits (i.e., fringe benefits and any cash or non-cash compensation which are not wages, as defined by law) that equal or exceed the applicable prevailing wage rate(s) for the location where the work is to be performed. Bidders may not submit Bids based upon hourly wage rates and supplements below the applicable prevailing wage rates as established by the New York State Department of Labor. Bids that fail to comply with this requirement will be disqualified.

b. WAGE RATE PAYMENTS/CHANGES DURING CONTRACT TERM The wages to be paid under any resulting Contract shall not be less than the prevailing rate of wages and supplements as set forth by law. It is required that the Contractor keep informed of all changes in the prevailing wage rates during the Contract term that apply to the classes of individuals supplied by the Contractor on any projects resulting from this Contract, subject to the provisions of the Labor Law. Contractor is solely liable for and must pay such required prevailing wage adjustments during the Contract term as required by law.

c. ARTICLE 8 CONSTRUCTION/PUBLIC WORKS CONTRACTS In compliance with Article 8, Section 220 of the New York State Labor Law:

i. Posting The Contractor must publicly post on the work site, in a prominent and accessible place, a legible schedule of the prevailing wage rates and supplements.

ii. Payroll Records Contractors and Subcontractors must keep original payrolls or transcripts subscribed and affirmed as true under the penalties of perjury as required by law. For public works contracts over $25,000 where the Contractor maintains no regular place of business in New York State, such records must be kept at the work site. For building services contracts, such records must be kept at the work site while work is being performed.

iii. Submission of Certified Payroll Transcripts for Public Works Contracts Only Contractors and Subcontractors on public works projects must submit monthly payroll transcripts to the Authorized User that has prepared or directs the preparation of the plans and specifications for a public works project, as set forth in the Bid Specifications. For Mini-Bid solicitations, the payroll records must be submitted to the entity preparing the agency Mini-Bid project specification. For "agency specific" Bids, the payroll records should be submitted to the entity issuing the purchase order. For all other OGS Centralized Contracts, such records should be submitted to the individual agency issuing the purchase order(s) for the work. Upon mutual agreement of the Contractor and the Authorized User, the form of submission may be submitted in a specified disk format acceptable to the Department of Labor provided: 1) the Contractor/Subcontractor retains the original records; and, (2) an original signed letter by a duly authorized individual of the Contractor or Subcontractor attesting to the truth and accuracy of the records accompanies the disk. This provision does not apply to Article 9 of the Labor Law building services contracts.

iv. Day's Labor No laborers, workmen or mechanics in the employ of the Contractor, Subcontractor or other person doing or contracting to do all or part of the work contemplated by the Contract shall be permitted or required to work more than eight hours in any one calendar day or more than five calendar days in any one week except in cases of extraordinary emergency including fire, flood or danger to life or property. "Extraordinary emergency" shall be deemed to include situations in which sufficient laborers, workers and mechanics cannot be employed to carry on public work expeditiously as a result of such restrictions upon the number of hours and days of labor and the immediate commencement or prosecution or completion without undue delay of the public work is necessary in the judgment of the NYS Commissioner of Labor for the preservation of the Contract site or for the protection of the life and limb of the persons using the Contract site.

d. ARTICLE 9 BUILDING SERVICES CONTRACTS
In compliance with Article 9, Section 230 of the New York State Labor Law:

i. Payroll Records Contractors and Subcontractors must keep original payrolls or transcripts subscribed and affirmed as true under the penalties of perjury as required by law. Where the Contractor or Subcontractor maintains no regular place of business in New York State, such records must be kept at the work site while work is being performed.

ii. Overtime Employees of Contractors and Subcontractors who work in excess of eight hours in a day or forty hours in a week shall be paid at the overtime rate identified by the New York State Department of Labor.

11. TAXES
a. Unless otherwise specified in the Bid Specifications or Contract, the quoted Bid price includes all taxes applicable to the transaction.

b. Purchases made by the State of New York and certain non-State Authorized Users are exempt from New York State and local sales taxes and, with certain exceptions, federal excise taxes. To satisfy the requirements of the New York State Sales tax exemption, either the Purchase Order issued by a State Agency or the invoice forwarded to authorize payment for such purchases will be sufficient evidence that the sale by the Contractor was made to the State, an exempt organization under Section 1116 (a) (1) of the Tax Law. Non-State Authorized Users must offer their own proof of exemption upon request. No person, firm or corporation is, however, exempt from paying the State Truck Mileage and Unemployment Insurance or Federal Social Security taxes, which remain the sole responsibility of the Bidder/Contractor.

c. Purchases by Authorized Users other than the State of New York may be subject to certain taxes which were not included in the Bid price, and in those instances the tax should be computed based on the Contract price and added to the invoice submitted to such entity for payment.

12. EXPENSES PRIOR TO CONTRACT EXECUTION The Commissioner and any Authorized User(s) are not liable for any costs incurred by a Vendor, Bidder or Contractor in the preparation and production of a Bid, Mini-Bid, cost proposal revision, or for any work performed prior to Contract execution.

13. ADVERTISING RESULTS The prior written approval of the Commissioner is required in order for results of the Bid to be used by the Contractor as part of any commercial advertising. The Contractor

shall also obtain the prior written approval of the Commissioner relative to the Bid or Contract for press or other media releases.

14. PRODUCT REFERENCES

a. "Or Equal" In all Bid Specifications the words "or equal" are understood to apply where a copyrighted, brand name, trade name, catalog reference, or patented Product is referenced. References to such specific Product are intended as descriptive, not restrictive, unless otherwise stated. Comparable Product will be considered if proof of compatibility is provided, including appropriate catalog excerpts, descriptive literature, specifications and test data, etc. The Commissioner's decision as to acceptance of the Product as equal shall be final.

b. Discrepancies in References In the event of a discrepancy between the model number referenced in the Bid Specifications and the written description of the Products which cannot be reconciled, with respect to such discrepancy, then the written description shall prevail.

15. REMANUFACTURED, RECYCLED, RECYCLABLE OR RECOVERED MATERIALS Upon the conditions specified in the Bid Specifications and in accordance with the laws of the State of New York, Contractors are encouraged to use recycled, recyclable or recovered materials in the manufacture of Products and packaging to the maximum extent practicable without jeopardizing the performance or intended end use of the Product or packaging unless such use is precluded due to health, welfare, safety requirements or in the Bid Specifications. Contractors are further encouraged to offer remanufactured Products to the maximum extent practicable without jeopardizing the performance or intended end use of the Product and unless such use is precluded due to health, welfare, safety requirements or by the Bid Specifications. Where such use is not practical, suitable, or permitted by the Bid Specifications, Contractor shall deliver new materials in accordance with the "Warranties" set forth below.

Items with recycled, recyclable, recovered, refurbished or remanufactured content must be identified in the Bid or Bidder will be deemed to be offering new Product.

16. PRODUCTS MANUFACTURED IN PUBLIC INSTITUTIONS Bids offering Products that are manufactured or produced in public institutions will be rejected.

17. PRICING

a. Unit Pricing If required by the Bid Specifications, the Bidder should insert the price per unit specified and the price extensions in decimals, not to exceed four places for each item unless otherwise specified, in the Bid. In the event of a discrepancy between the unit price and the extension, the unit price shall govern unless, in the sole judgment of the Commissioner, such unit pricing is obviously erroneous.

b. Net Pricing Unless otherwise required by the Bid Specifications, prices shall be net, including transportation, customs, tariff, delivery and other charges fully prepaid by the Contractor to the destination(s) indicated in the Bid Specifications, subject to the cash discount.

c. "No Charge" Bid When Bids are requested on a number of Products as a Group or Lot, a Bidder desiring to Bid "no charge" on a Product in the Group or Lot must clearly indicate such. Otherwise, such Bid may be considered incomplete and be rejected, in whole or in part, at the discretion of the Commissioner.

d. Educational Pricing All Products to be supplied for educational purposes that are subject to educational discounts shall be identified in the Bid and such discounts shall be made available to qualifying institutions.

e. Third Party Financing If Product acquisitions are financed through any third party financing, Contractor may be required as a condition of Contract Award to agree to the terms and conditions of a "Consent & Acknowledgment Agreement" in a form acceptable to the Commissioner.

f. Best Pricing Offer During the Contract term, if substantially the same or a smaller quantity of a Product is sold by the Contractor outside of this Contract upon the same or similar terms and conditions as that of this Contract at a lower price to a federal, state or local governmental entity, the price under this Contract, at the discretion of the Commissioner, shall be immediately reduced to the lower price.

g. Specific price decreases:

(i) GSA Changes: Where NYS Net Prices are based on an approved GSA Schedule, price decreases shall take effect automatically during the Contract term and apply to Purchase Orders submitted on or after the date the approved GSA Schedule pricing decreases during the Contract term; or

(ii) Commercial Price List Reductions: Where NYS Net Prices are based on a discount from Contractor's list prices, price decreases shall take effect automatically during the Contract term and apply to Purchase Orders submitted on or after the date Contractor lowers its pricing to its customers generally or to similarly situated government customers during the Contract term; or

(iii) Special Offers/Promotions Generally: Where Contractor generally offers more advantageous special price promotions or special discount pricing to other customers during the Contract term for a similar quantity, and the maximum price or discount associated with such offer or promotion is better than the discount or Net Price otherwise available under this Contract, such better price or discount shall apply for similar quantity transactions under this Contract for the life of such general offer or promotion; and

(iv) Special Offers/Promotions to Authorized Users: Contractor may offer Authorized Users, under either this Contract or any other Contracting vehicle, competitive pricing which is lower than the NYS Net Price set forth herein at any time during the Contract term and such lower pricing shall not be applied as a global price reduction under the Contract pursuant to the foregoing paragraph (iii).

Unless otherwise specified in the Bid Specifications, Contractor may offer lower prices or better terms (see Modification of Contract Terms) on any specific Purchase Order(s) from any Authorized User without being in conflict with, or having any obligation to comply on a global basis with, the terms of this clause.

h. Cost Proposal Revisions A Contractor may be solicited prior to contract award to propose the best possible offer for the Product or service being bid on, in accordance with State Finance Law § 163(9)(c). A cost proposal revision must be a lower price than the initial price.

18. DRAWINGS

a. Drawings Submitted With Bid When the Bid Specifications require the Bidder to furnish drawings and/or plans, such drawings

and/or plans shall conform to the mandates of the Bid Documents and shall, when approved by the Commissioner, be considered a part of the Bid and of any resulting Contract. All symbols and other representations appearing on the drawings shall be considered a part of the drawing.

b. Drawings Submitted During the Contract Term Where required to develop, maintain and deliver diagrams or other technical schematics regarding the scope of work, Contractor shall do so on an ongoing basis at no additional charge, and must, as a condition of payment, update drawings and plans during the Contract term to reflect additions, alterations, and deletions. Such drawings and diagrams shall be delivered to the Authorized User's representative.

c. Accuracy of Drawings Submitted All drawings shall be neat and professional in manner and shall be clearly labeled as to locations and type of Product, connections and components. Drawings and diagrams are to be in compliance with accepted drafting standards. Acceptance or approval of such plans shall not relieve the Contractor from responsibility for design or other errors of any sort in the drawings or plans, or from its responsibility for performing as required, furnishing Product, services or installation, or carrying out any other requirements of the intended scope of work.

19. SITE INSPECTION Where a site inspection is required by the Bid Specifications or Project Definition, Bidder shall be required to inspect the site, including environmental or other conditions for pre-existing deficiencies that may affect the installed Product, equipment, or environment or services to be provided and, which may affect Bidder's ability to properly deliver, install or otherwise provide the required Product. All inquiries regarding such conditions shall be made in writing. Bidder shall be deemed to have knowledge of any deficiencies or conditions which such inspection or inquiry might have disclosed. Bidder must provide a detailed explanation with its Bid if additional work is required under this clause in order to properly complete the delivery and installation of the required Product or provide the requested service.

20. PROCUREMENT CARD The State has entered into an agreement for purchasing card services. The Purchasing Card enables Authorized Users to make authorized purchases directly from a Contractor without processing Purchase Orders or Purchase Authorizations. Purchasing Cards are issued to selected employees authorized to purchase for the Authorized User and having direct contact with Contractors. Cardholders can make purchases directly from any Contractor that accepts the Purchasing Card.

The Contractor shall not process a transaction for payment through the credit card clearinghouse until the purchased Products have been shipped or services performed. Unless the cardholder requests correction or replacement of a defective or faulty Product in accordance with other Contract requirements, the Contractor shall immediately credit a cardholder's account for Products returned as defective or faulty.

21. SAMPLES

a. Standard Samples Bid Specifications may indicate that the Product to be purchased must be equal to a standard sample on display in a place designated by the Commissioner and such sample will be made available to the Bidder for examination prior to the opening date. Failure by the Bidder to examine such sample shall not entitle the Bidder to any relief from the conditions imposed by the Bid Specifications.

b. Bidder Supplied Samples The Commissioner reserves the right to request from the Bidder/Contractor a representative sample(s) of the Product offered at any time prior to or after award of a contract. Unless otherwise instructed, samples shall be furnished within the time specified in the request. Untimely submission of a sample may constitute grounds for rejection of the Bid or cancellation of the Contract. Samples must be submitted free of charge and be accompanied by the Bidder's name and address, any descriptive literature relating to the Product and a statement indicating how and where the sample is to be returned. Where applicable, samples must be properly labeled with the appropriate Bid or Contract reference.

A sample may be held by the Commissioner during the entire term of the Contract and for a reasonable period thereafter for comparison with deliveries. At the conclusion of the holding period, the sample, where feasible, will be returned as instructed by the Bidder, at the Bidder's expense and risk. Where the Bidder has failed to fully instruct the Commissioner as to the return of the sample (i.e., mode and place of return, etc.) or refuses to bear the cost of its return, the sample shall become the sole property of the receiving entity at the conclusion of the holding period.

c. Enhanced Samples When an approved sample exceeds the minimum specifications, all Product delivered must be of the same enhanced quality and identity as the sample. Thereafter, in the event of a Contractor's default, the Commissioner may procure a Product substantially equal to the enhanced sample from other sources, charging the Contractor for any additional costs incurred.

d. Conformance with Samples Submission of a sample (whether or not such sample is tested by, or for, the Commissioner) and approval thereof shall not relieve the Contractor from full compliance with all terms and conditions, performance related and otherwise, specified in the Bid Specifications. If in the judgment of the Commissioner the sample or Product submitted is not in accordance with the specifications or testing requirements prescribed in the Bid Specifications, the Commissioner may reject the Bid. If an award has been made, the Commissioner may cancel the Contract at the expense of the Contractor.

e. Testing All samples are subject to tests in the manner and place designated by the Commissioner, either prior to or after Contract award. Unless otherwise stated in the Bid Specifications, Bidder samples consumed or rendered useless by testing will not be returned to the Bidder. Testing costs for samples that fail to meet Contract requirements may be at the expense of the Contractor.

f. Requests For Samples By Authorized Users Requests for samples by Authorized Users require the consent of the Contractor. Where Contractor refuses to furnish a sample, Authorized User may, in its sole discretion, make a determination on the performance capability of the Product or on the issue in question.

BID EVALUATION

22. BID EVALUATION The Commissioner reserves the right to accept or reject any and all Bids, or separable portions of Bids, and waive technicalities, irregularities, and omissions if the Commissioner determines the best interests of the State will be served. The Commissioner, in his/her sole discretion, may accept or reject illegible, incomplete or vague Bids and his/her decision shall be final. A conditional or revocable Bid which clearly communicates the terms or limitations of acceptance may be considered, and Contract award may be made in compliance with the Bidder's conditional or revocable terms in the Bid.

23. TIE BIDS In the event two Bids are found to be substantially equivalent, price shall be the basis for determining the award recipient. While prompt payment discounts will not be considered in determining the low Bid, the Commissioner may consider any prompt payment discount in resolving Bids which are otherwise tied. If two or more Bidders submit substantially equivalent Bids as to pricing or other factors, the decision of the Commissioner to award a Contract to one or more of such Bidders shall be final.

24. QUANTITY CHANGES PRIOR TO AWARD The Commissioner reserves the right, at any time prior to the award of a specific quantity Contract, to alter in good faith the quantities listed in the Bid Specifications. In the event such right is exercised, the lowest responsible Bidder meeting Bid Specifications will be advised of the revised quantities and afforded an opportunity to extend or reduce its Bid price in relation to the changed quantities. Refusal by the low Bidder to so extend or reduce its Bid price may result in the rejection of its Bid and the award of such Contract to the lowest responsible Bidder who accepts the revised qualifications.

25. TIMEFRAME FOR OFFERS The Commissioner reserves the right to make awards within sixty days after the date of the Bid opening or such other period of time as set forth in the Bid Documents, during which period, Bids must remain firm and cannot be withdrawn. Where an award is not made within the sixty day period or other time specified as set forth in the Bid Documents, the Bids shall remain firm until such later time as either a Contract is awarded or the Bidder delivers to the Commissioner written notice of the withdrawal of its Bid.

TERMS & CONDITIONS

26. CONTRACT CREATION / EXECUTION Except for contracts governed by Article 11-B of the State Finance Law, subject to and upon receipt of all required approvals as set forth in the Bid Specifications, a Contract shall be deemed executed and created with the successful Bidder(s) upon the Commissioner's mailing or electronic communication to the address on the Bid/Contract of: (i) the final Contract Award Notice; (ii) a fully executed Contract; or (iii) a Purchase Order authorized by the Commissioner.

27. PARTICIPATION IN CENTRALIZED CONTRACTS

a. Agencies All State Agencies may utilize and purchase under any Centralized Contract let by the Commissioner, unless the Bid Documents limit purchases to specific State Agencies.

b. Non-State Agency Authorized Users Authorized Users other than State Agencies are permitted to make purchases through Centralized Contracts where permitted by law, the Contract or the Commissioner.

c. Voluntary Extension Purchase Orders issued against a Centralized Contract by any Authorized User not provided for in the Bid Specifications shall be honored by the Contractor at its discretion and only with the approval of the OGS Commissioner and any other approvals required by law. Contractors are encouraged to voluntarily extend service Contracts to those additional entities authorized to utilize commodity Contracts under Section 163(3)(a)(iv) of the State Finance Law.

d. Responsibility for Performance Participation in Centralized Contracts by Authorized Users is permitted upon the following conditions: (i) the responsibility with regard to performance of any contractual obligation, covenant, condition or term thereunder by any Authorized User other than State Agencies shall be borne and is expressly assumed by such Authorized User and not by the State; (ii) a breach of the Contract by any particular Authorized User shall neither constitute nor be deemed a breach of the Contract as a whole which shall remain in full force and effect, and shall not affect the validity of the Contract nor the obligations of the Contractor thereunder respecting non-breaching Authorized Users, whether State or otherwise; (iii) for a breach by an Authorized User other than a State Agency, the State specifically and expressly disclaims any and all liability for such breach; and (iv) each non-State Agency Authorized User and Contractor guarantees to save the State, its officers, agents and employees harmless from any liability that may be or is imposed by the non-State Agency Authorized User's or Contractor's failure to perform in accordance with its obligations under the Contract.

e. Contract Migration Authorized Users holding individual Contracts with a Contractor at the time that Contractor is awarded a Centralized Contract for the same Products or services shall be permitted to migrate to that Centralized Contract effective with its commencement date. Such migration shall not operate to diminish, alter or eliminate any right that the Authorized User otherwise had under the terms and conditions of their individual Contract.

28. MODIFICATION OF CONTRACT TERMS The terms and conditions set forth in the Contract shall govern all transactions by Authorized User(s) under this Contract. The Contract may only be modified or amended upon mutual written agreement of the Commissioner and Contractor.

The Contractor may, however, offer Authorized User(s) more advantageous pricing, payment, or other terms and conditions than those set forth in the Contract. In such event, a copy of such terms shall be furnished to the Authorized User(s) and Commissioner by the Contractor at the time of such offer.

Other than where such terms are more advantageous for the Authorized User(s) than those set forth in the Contract, no alteration or modification of the terms of the Contract, including substitution of Product, shall be valid or binding against Authorized User(s) unless authorized by the Commissioner or specified in the Contract Award Notification. No such alteration or modification shall be made by unilaterally affixing such terms to Product upon delivery (including, but not limited to, attachment or inclusion of standard pre-printed order forms, product literature, "shrink wrap" terms accompanying software upon delivery, or other documents) or by incorporating such terms onto order forms, purchase orders or other documents forwarded by the Contractor for payment, notwithstanding Authorized User's subsequent acceptance of Product, or that Authorized User has subsequently processed such document for approval or payment.

29. SCOPE CHANGES The Commissioner reserves the right to require, by written order, changes to the scope of the Contract, by altering, adding to or deducting from the Bid Specifications, such changes to be within the general scope of the Contract. If any such change causes an increase or decrease in the cost of, or the time required for, performance of any part of the work under the Contract, whether or not changed by the order, the Commissioner shall, upon notice from Contractor as hereafter stated, make an equitable adjustment in the Contract price, the delivery schedule or both and shall modify the Contract. The Contractor must assert its right to an adjustment under this clause within thirty days from the date of receipt of the written order. However, if the Commissioner decides that the facts justify it, the Commissioner may provide an adjustment without receipt of a proposal. Failure to agree to any adjustment shall be a dispute under the Disputes clause, provided, however, that nothing in this clause shall excuse the Contractor from proceeding with the Contract as changed.

30. ESTIMATED / SPECIFIC QUANTITY CONTRACTS
Estimated quantity contracts, also referred to as indefinite delivery / indefinite quantity contracts, are expressly agreed and understood to be made for only the quantities, if any, actually ordered during the Contract term. No guarantee of any quantity is implied or given.

With respect to any specific quantity stated in the contract, the Commissioner reserves the right after award to order up to 20% more or less (rounded to the next highest whole number) than the specific quantities called for in the Contract. Notwithstanding the foregoing, the Commissioner may purchase greater or lesser percentages of Contract quantities should the Commissioner and Contractor so agree. Such agreement may include an equitable price adjustment.

31. EMERGENCY CONTRACTS In the event that a disaster emergency is declared by Executive Order under Section 28 of Article 2-B of the Executive Law, or the Commissioner determines pursuant to his/her authority under Section 163(10)(b) of the State Finance Law that an emergency exists requiring the prompt and immediate delivery of Product, the Commissioner reserves the right to obtain such Product from any source, including but not limited to this Contract(s), as the Commissioner in his/her sole discretion determines will meet the needs of such emergency. Contractor shall not be entitled to any claim or lost profits for Product procured from other sources pursuant to this clause. The reasons underlying the finding that an emergency exists shall be included in the procurement record.

32. PURCHASE ORDERS Unless otherwise authorized in writing by the Commissioner, no Product is to be delivered or furnished by Contractor until transmittal of an official Purchase Order from the Authorized User. Unless terminated or cancelled pursuant to the authority vested in the Commissioner, Purchase Orders shall be effective and binding upon the Contractor when placed in the mail or electronically transmitted prior to the termination of the Contract period, addressed to the Contractor at the address for receipt of orders set forth in the Contract or in the Contract Award Notification.

All Purchase Orders issued pursuant to Contracts let by the Commissioner must bear the appropriate Contract number and, if necessary, required State approvals. As deemed necessary, the Authorized User may confirm pricing and other Product information with the Contractor prior to placement of the Purchase Order. The State reserves the right to require any other information from the Contractor which the State deems necessary in order to complete any Purchase Order placed under the Contract. Unless otherwise specified, all Purchase Orders against Centralized Contracts will be placed by Authorized Users directly with the Contractor and any discrepancy between the terms stated on the Contractor's order form, confirmation or acknowledgment, and the Contract terms shall be resolved in favor of the terms most favorable to the Authorized User. Should an Authorized User add written terms and conditions to the Purchase Order that conflict with the terms and conditions of the Contract, the Contractor has the option of rejecting the Purchase Order within five business days of its receipt but shall first attempt to negotiate the additional written terms and conditions in good faith with the Authorized User, or fulfill the Purchase Order. Notwithstanding the above, the Authorized User reserves the right to dispute any discrepancies arising from the presentation of additional terms and conditions with the Contractor.

If, with respect to an Agency Specific Contract let by the Commissioner, a Purchase Order is not received by the Contractor within two weeks after the issuance of a Contract Award Notification, it is the responsibility of the Contractor to request in writing that the appropriate Authorized User forward a Purchase Order. If, thereafter, a Purchase Order is not received within a reasonable period of time, the Contractor shall promptly notify in writing the appropriate purchasing officer in OGS. Failure to timely notify such officer may, in the discretion of the OGS Commissioner and without cost to the State, result in the cancellation of such requirement by the OGS Commissioner with a corresponding reduction in the Contract quantity and price.

33. PRODUCT DELIVERY Delivery must be made as ordered to the address specified on the Purchase Order and in accordance with the terms of the Contract. Delivery shall be made within thirty calendar days after receipt of a Purchase Order by the Contractor, unless otherwise agreed to by the Authorized User and the Contractor. The decision of the Commissioner as to compliance with delivery terms shall be final. The burden of proof for delay in receipt of a Purchase Order shall rest with the Contractor. In all instances of a potential or actual delay in delivery, the Contractor shall immediately notify the Commissioner and the Authorized User, and confirm in writing the explanation of the delay, and take appropriate action to avoid any subsequent late deliveries. Any extension of time for delivery must be requested in writing by the Contractor and approved in writing by the Authorized User. Failure to meet such delivery time schedule may be grounds for cancellation of the order or, in the Commissioner's discretion, the Contract.

34. WEEKEND AND HOLIDAY DELIVERIES Unless otherwise specified in the Bid Specifications or by an Authorized User, deliveries will be scheduled for ordinary business hours, Monday through Friday (excluding legal holidays observed by the State of New York). Deliveries may be scheduled by mutual agreement for Saturdays, Sundays or legal holidays observed by the State of New York where the Product is for daily consumption, an emergency exists, the delivery is a replacement, delivery is late, or other reasonable circumstance in which event the convenience of the Authorized User shall govern.

35. SHIPPING/RECEIPT OF PRODUCT

a. Packaging Product shall be securely and properly packed for shipment, storage and stocking in appropriate, clearly labeled shipping containers and according to accepted commercial practice, without any extra charges for packing materials, cases or other types of containers. The container shall become and remain the property of the Authorized User unless otherwise specified in the Contract documents.

b. Shipping Charges Unless otherwise stated in the Bid Specifications, all deliveries shall be deemed to be freight on board (F.O.B.) destination tailgate delivery at the dock of the Authorized User. Unless otherwise agreed, items purchased at a price F.O.B. Shipping point plus transportation charges shall not relieve the Contractor from responsibility for safe and proper delivery notwithstanding the Authorized User's payment of transportation charges. Contractor shall be responsible for ensuring that the Bill of Lading states "charges prepaid" for all shipments.

c. Receipt of Product The Contractor shall be solely responsible for assuring that deliveries are made to personnel authorized to accept delivery on behalf of the Authorized User. Any losses resulting from the Contractor's failure to deliver Product to authorized personnel shall be borne exclusively by the Contractor.

36. TITLE AND RISK OF LOSS Notwithstanding the form of shipment, title or other property interest, risk of loss shall not pass from the Contractor to the Authorized User until the Products have been received, inspected and accepted by the receiving entity. Acceptance shall occur within a reasonable time or in accordance with such other defined acceptance period as may be specified in the Bid Specifications or Purchase Order. Mere acknowledgment by

Authorized User personnel of the delivery or receipt of goods (e.g., signed bill of lading) shall not be deemed or construed as acceptance of the Products received. Any delivery of Product that is substandard or does not comply with the Bid Specifications or Contract terms and conditions, may be rejected or accepted on an adjusted price basis, as determined by the Commissioner.

37. RE-WEIGHING PRODUCT Deliveries are subject to re-weighing at the point of destination by the Authorized User. If shrinkage occurs which exceeds that normally allowable in the trade, the Authorized User shall have the option to require delivery of the difference in quantity or to reduce the payment accordingly. Such option shall be exercised in writing by the Authorized User.

38. PRODUCT SUBSTITUTION In the event a specified manufacturer's Product listed in the Contract becomes unavailable or cannot be supplied by the Contractor for any reason (except as provided for in the Savings/Force Majeure Clause), a Product deemed in writing by the Commissioner to be equal to or better than the specified Product must be substituted by the Contractor at no additional cost or expense to the Authorized User. Unless otherwise specified, any substitution of Product prior to the Commissioner's written approval may be cause for termination of Contract.

39. REJECTED PRODUCT When Product is rejected, it must be removed by the Contractor from the premises of the Authorized User within ten calendar days of notification of rejection by the Authorized User. Upon notification of rejection, risk of loss of rejected or non-conforming Product shall remain with Contractor. Rejected items not removed by the Contractor within ten calendar days of notification shall be regarded as abandoned by the Contractor, and the Authorized User shall have the right to dispose of Product as its own property. The Contractor shall promptly reimburse the Authorized User for any and all costs and expenses incurred in storage or effecting removal or disposition after the ten-calendar-day period.

40. INSTALLATION Where installation is required, Contractor shall be responsible for placing and installing the Product in the required locations. All materials used in the installation shall be of good quality and shall be free from any and all defects that would mar the Product or render it unsound. Installation includes the furnishing of any equipment, rigging and materials required to install or place the Product in the proper location. The Contractor shall protect the site from damage for all its work and shall repair damages or injury of any kind caused by the Contractor, its employees, officers or agents. If any alteration, dismantling or excavation, etc. is required to effect installation, the Contractor shall thereafter promptly restore the structure or site. Work shall be performed to cause the least inconvenience to the Authorized User(s) and with proper consideration for the rights of other Contractors or workers. The Contractor shall promptly perform its work and shall coordinate its activities with those of other Contractors. The Contractor shall clean up and remove all debris and rubbish from its work as required or directed. Upon completion of the work, the building and surrounding area of work shall be left clean and in a neat, unobstructed condition, and everything in satisfactory repair and order.

41. REPAIRED OR REPLACED PARTS / COMPONENTS Where the Contractor is required to repair, replace or substitute Product or parts or components of the Product under the Contract, the repaired, replaced or substituted Products shall be subject to all terms and conditions for new parts and components set forth in the Contract including Warranties, as set forth in the Warranties Clause herein. Replaced or repaired Product or parts and components of such Product shall be new and shall, if available, be replaced by the original manufacturer's component or part. Remanufactured parts or components meeting new Product standards may be permitted by the Commissioner or Authorized User. Before installation, all proposed substitutes for the original manufacturers installed parts or components must be approved by the Authorized User. The part or component shall be equal to or of better quality than the original part or component being replaced.

42. EMPLOYEES, SUBCONTRACTORS & AGENTS All employees, Subcontractors or agents performing work under the Contract must be trained staff or technicians who meet or exceed the professional, technical and training qualifications set forth in the Bid Specifications or the Bid Documents, whichever is more restrictive, and must comply with all security and administrative requirements of the Authorized User. The Commissioner reserves the right to conduct a security background check or otherwise approve any employee, Subcontractor or agent furnished by Contractor and to refuse access to or require replacement of any personnel for cause based on professional, technical or training qualifications, quality of work or change in security status or non-compliance with Authorized User's security or other requirements. Such approval shall not relieve the Contractor of the obligation to perform all work in compliance with the Contract terms. The Commissioner reserves the right to reject and/or bar from any facility for cause any employee, Subcontractor, or agents of the Contractor.

43. ASSIGNMENT The Contractor shall not assign, transfer, convey, sublet, or otherwise dispose of the contract or its right, title or interest therein, or its power to execute such contract to any other person, company, firm or corporation in performance of the contract without the prior written consent of the Commissioner or Authorized User (as applicable); provided, however, notwithstanding anything in Section 138 of the State Finance Law to the contrary, any approval required thereunder shall not be unreasonably withheld, conditioned, delayed or denied. Notwithstanding the foregoing, the State shall not hinder, prevent or affect assignment of money by a Contractor for the benefit of its creditors. Prior to a consent to assignment of monies becoming effective, the Contractor shall file a written notice of such monies assignment(s) with the Comptroller. Prior to a consent to assignment of a Contract, or portion thereof, becoming effective, the Contractor shall submit the request for assignment to the Commissioner and seek written agreement from the Commissioner which will be filed with the Comptroller. Commissioner shall use reasonable efforts to promptly respond to any request by Contractor for an assignment, provided that Contractor supplies sufficient information about the party to whom the Contractor proposes to assign the contract.

Upon notice to the Contractor, the Contract may be assigned without the consent of the Contractor to another State Agency or subdivision of the State pursuant to a governmental reorganization or assignment of functions under which the functions are transferred to a successor Agency or to another Agency that assumes OGS responsibilities for the Contract.

44. SUBCONTRACTORS AND SUPPLIERS The Commissioner reserves the right to reject any proposed Subcontractor or supplier for bona fide business reasons, including, but not limited to: the company failed to solicit New York State certified minority- and women-owned business enterprises as required in prior OGS Contracts; the fact that such Subcontractor or supplier is on the New York State Department of Labor's list of companies with which New York State cannot do business; the Commissioner's determination that the company is not qualified or is not responsible; or the fact that the company has previously provided unsatisfactory work or services.

45. PERFORMANCE / BID BOND The Commissioner reserves the right to require a Bidder or Contractor to furnish, without additional cost, a performance, payment or Bid bond, negotiable

irrevocable letter of credit, or other form of security for the faithful performance of the Contract. Where required, such bond or other security shall be in the form prescribed by the Commissioner.

46. SUSPENSION OF WORK The Commissioner, in his/her sole discretion, reserves the right to suspend any or all activities under this Contract, at any time, in the best interests of the Authorized User. In the event of such suspension, the Contractor will be given a formal written notice outlining the particulars of such suspension. Examples of the reason for such suspension include, but are not limited to, a budget freeze or reduction in State spending, declaration of emergency, contract compliance issues or other circumstances. Upon issuance of such notice, the Contractor is not to accept any Purchase Orders, and shall comply with the suspension order. Activity may resume at such time as the Commissioner issues a formal written notice authorizing a resumption of performance under the Contract.

An Authorized User may issue a formal written notice for the suspension of work for which it has engaged the Contractor for reasons specified in the above paragraph. The written notice shall set forth the reason for such suspension and a copy of the written notice shall be provided to the Commissioner.

47. TERMINATION

a. For Cause: For a material breach that remains uncured for more than thirty calendar days or other specified period after written notice to the Contractor, the Contract or Purchase Order may be terminated by the Commissioner or Authorized User respectively, at the Contractor's expense where Contractor becomes unable or incapable of performing, or meeting any requirements or qualifications set forth in the Contract, or for non-performance, or upon a determination that Contractor is non-responsible. Such termination shall be upon written notice to the Contractor. In such event, the Commissioner or Authorized User may complete the contractual requirements in any manner it may deem advisable and pursue available legal or equitable remedies for breach.

b. For Convenience: By written notice, this Contract may be terminated at any time by the Commissioner for convenience upon sixty calendar days written notice or other specified period without penalty or other early termination charges due. Such termination of the Contract shall not affect any project or Purchase Order that has been issued under the Contract prior to the date of such termination. If the Contract is terminated pursuant to this subdivision, the Authorized User shall remain liable for all accrued but unpaid charges incurred through the date of the termination. Contractor shall use due diligence and provide any outstanding deliverables.

c. For Violation of Sections 139-j and 139-k of the State Finance Law: The Commissioner reserves the right to terminate the Contract in the event it is found that the certification filed by the Bidder in accordance with Section 139-k of the State Finance Law was intentionally false or intentionally incomplete. Upon such finding, the Commissioner may exercise his/her termination right by providing written notification to the Contractor in accordance with the written notification terms of the Contract.

d. For Violation of Section 5-a of the New York State Tax Law: The Commissioner reserves the right to terminate the contract in the event it is found that the certification filed by the Contractor in accordance with Section 5-a of the Tax Law is not timely filed during the term of the Contract or the certification furnished was intentionally false or intentionally incomplete. Upon such finding, the Commissioner may exercise his/her termination right by providing written notification to the Contractor in accordance with the written notification terms of the Contract.

e. For Non-Responsibility: The Bidder agrees that if it is found by the State that the Bidder's responses to the Vendor Responsibility Questionnaire were intentionally false or intentionally incomplete, on such finding, the Commissioner may terminate the Contract.

Upon written notice to the Contractor, and a reasonable opportunity to be heard with appropriate OGS officials or staff, the Contract may be terminated by the Commissioner or his or her designee at the Contractor's expense where the Contractor is determined by the Commissioner or his or her designee to be non-responsible. In such event, the Commissioner or his or her designee may complete the contractual requirements in any manner he or she may deem advisable and pursue available legal or equitable remedies for breach.

In no case shall such termination of the Contract by the State be deemed a breach thereof, nor shall the State be liable for any damages for lost profits or otherwise, which may be sustained by the Contractor as a result of such termination.

f. For refusal to testify, sign a waiver of immunity or answer questions

The Commissioner reserves the right in accordance with State Finance Law §139-a, to terminate the contract in the event it is found that a member, partner, director or officer of Contractor refused, when called before a grand jury, head of a state department, temporary state commission or other state agency, or the organized crime task force in the department of law, which is empowered to compel the attendance of witnesses and examine them under oath, to testify in an investigation, concerning any transaction or contract had with the state, any political subdivision thereof, a public authority or with any public department, agency or official of the state or of any political subdivision thereof or of a public authority, to sign a waiver of immunity against subsequent criminal prosecution or to answer any relevant question concerning such transaction or contract. Upon such finding, the Commissioner may exercise his/her termination right by providing written notification to the Contractor.

48. SAVINGS/FORCE MAJEURE A Force Majeure occurrence is an event or effect that cannot be reasonably anticipated or controlled and is not due to the negligence or willful misconduct of the affected party. Force Majeure includes, but is not limited to, acts of God, acts of war, acts of public enemies, terrorism, strikes, fires, explosions, actions of the elements, floods, or other similar causes beyond the control of the Contractor or the Commissioner in the performance of the Contract where non-performance, by exercise of reasonable diligence, cannot be prevented.

The affected party shall provide the other party with written notice of any Force Majeure occurrence as soon as the delay is known and provide the other party with a written contingency plan to address the Force Majeure occurrence, including, but not limited to, specificity on quantities of materials, tooling, people, and other resources that will need to be redirected to another facility and the process of redirecting them. Furthermore, the affected party shall use its commercially reasonable efforts to resume proper performance within an appropriate period of time. Notwithstanding the foregoing, if the Force Majeure condition continues beyond thirty (30) days, the Parties shall jointly decide on an appropriate course of action that will permit fulfillment of the Parties' objectives hereunder.

The Contractor agrees that in the event of a delay or failure of performance by the Contractor, under the Contract due to a Force Majeure occurrence:

a. The Commissioner may purchase from other sources (without recourse to and by the Contractor for the costs and expenses thereof) to replace all or part of the Products which are the subject of the delay, which purchases may be deducted from the Contract quantities without penalty or liability to the State, or

b. The Contractor will provide Authorized Users with access to Products first in order to fulfill orders placed before the Force Majeure event occurred. The Commissioner agrees that Authorized Users shall accept allocated performance or deliveries during the occurrence of the Force Majeure event.

Neither the Contractor nor the Commissioner shall be liable to the other for any delay in or failure of performance under the Contract due to a Force Majeure occurrence. Any such delay in or failure of performance shall not constitute default or give rise to any liability for damages. The existence of such causes of such delay or failure shall extend the period for performance to such extent as determined by the Contractor and the Commissioner to be necessary to enable complete performance by the Contractor if reasonable diligence is exercised after the cause of delay or failure has been removed.

Notwithstanding the above, at the discretion of the Commissioner where the delay or failure will significantly impair the value of the Contract to the State or to Authorized Users, the Commissioner may terminate the Contract or the portion thereof which is subject to delays, and thereby discharge any unexecuted portion of the Contract or the relative part thereof.

In addition, the Commissioner reserves the right, in his/her sole discretion, to make an equitable adjustment in the Contract terms and/or pricing should extreme and unforeseen volatility in the marketplace affect pricing or the availability of supply. "Extreme and unforeseen volatility in the marketplace" is defined as market circumstances which meet the following criteria: (i) the volatility is due to causes outside the control of Contractor; (ii) the volatility affects the marketplace or industry, not just the particular Contract source of supply; (iii) the effect on pricing or availability of supply is substantial; and (iv) the volatility so affects Contractor's performance that continued performance of the Contract would result in a substantial loss. Failure of the Contractor to agree to any adjustment shall be a dispute under the Disputes clause; provided however, that nothing in this clause shall excuse the Contractor from performing in accordance with the Contract as changed.

49. CONTRACT INVOICING

a. **Invoicing.** Contractor and the dealers/distributors/resellers designated by the Contractor, if any, shall provide complete and accurate billing invoices to each Authorized User in order to receive payment. Billing invoices submitted to an Authorized User must contain all information required by the Contract and the State Comptroller or other appropriate fiscal officer. Submission of an invoice and payment thereof shall not preclude the Commissioner from requesting reimbursement or demanding a price adjustment in any case where the Product delivered is found to deviate from the terms and conditions of the Contract or where the billing was inaccurate.

Contractor shall provide, upon request of the Commissioner, any and all information necessary to verify the accuracy of the billings. Such information shall be provided in a commercially reasonable manner as requested by the Commissioner. The Commissioner may direct the Contractor to provide the information to the State Comptroller or to any Authorized User of the Contract.

b. **Payment of Contract Purchases made by an Authorized User when the State Comptroller is responsible for issuing such payment** The Authorized User and Contractor agree that payments for invoices submitted by the Contractor shall only be rendered electronically unless payment by paper check is expressly authorized by the Commissioner, in the Commissioner's sole discretion, due to extenuating circumstances. Such electronic payments shall be made in accordance with ordinary State procedures and practices. The Contractor shall comply with the State Comptroller's procedures to authorize electronic payments. Authorization forms are available at the State Comptroller website at **www.osc.state.ny.us**, by e-mail at **HelpDesk@sfs.ny.gov**, or by telephone at (518) 457-7737 or toll free (877) 737-4185. Contractor acknowledges that it will not receive payment on any invoices submitted under this Contract that are payable by the State Comptroller if it does not comply with the State Comptroller's electronic payment procedures, except where the Commissioner has expressly authorized payment by paper check as set forth above.

c. **Payment of Contract Purchases made by an Authorized User when the State Comptroller is not responsible for issuing such payment** The Authorized User and Contractor agree that payments for such Contract purchases shall be billed directly by Contractor on invoices/vouchers, together with complete and accurate supporting documentation as required by the Authorized User. Such payments shall be as mandated by the appropriate governing law from the receipt of a proper invoice. Such Authorized User and Contractor are strongly encouraged to establish electronic payments.

50. DEFAULT – AUTHORIZED USER

a. **Breach by Authorized User.** An Authorized User's breach shall not be deemed a breach of the Centralized Contract; rather, it shall be deemed a breach of the Authorized User's performance under the terms and conditions of the Centralized Contract.

b. **Failure to Make Payment.** In the event a participating Authorized User fails to make payment to the Contractor for Products delivered, accepted and properly invoiced, within thirty calendar days of such delivery and acceptance, the Contractor may, upon five business days advance written notice to both the Commissioner and the Authorized User's purchasing official, suspend additional shipments of Product or provision of services to such entity until such time as reasonable arrangements have been made and assurances given by such entity for current and future Contract payments.

c. **Notice of Breach.** Notwithstanding the foregoing, the Contractor shall, at least ten business days prior to declaring a breach of Contract by any Authorized User, by certified or registered mail, notify both the Commissioner and the purchasing official of the breaching Authorized User of the specific facts, circumstances and grounds upon which a breach will be declared.

d. **Insufficient basis.** If the Contractor's basis for declaring a breach is insufficient, the Contractor's declaration of breach and failure to service an Authorized User may constitute a breach of the Contract, and the Authorized User may thereafter seek any remedy available at law or equity.

51. PROMPT PAYMENTS

a. **State Agencies** Upon acceptance of Product or as otherwise provided by Contract, Contractor may invoice for payment. The required payment date shall be thirty (30) calendar days, excluding legal holidays, from the receipt of a proper invoice, as determined in accordance with State Finance Law §179-f(2) and 2 NYCRR Part 18. The payment of interest on certain payments due and owed by Agency

may be made in accordance with State Finance Law §§179-d et. seq. and the implementing regulations (2 NYCRR §18.1 et seq.).

b. By Non-State Agencies Upon acceptance of Product or as otherwise provided by Contract, Contractor may invoice for payment. The required payment date shall be thirty calendar days, excluding legal holidays, or as mandated by the appropriate governing law from the receipt of a proper invoice. The terms of Article 11-A of the State Finance Law apply only to procurements by and the consequent payment obligations of Agencies. Neither expressly nor by any implication is the statute applicable to Non-State Authorized Users. Neither OGS nor the State Comptroller is responsible for payments on any purchases made by a Non-State Agency Authorized User.

c. By Contractor Should the Contractor be liable for any payments to the State hereunder, interest, late payment charges and collection fee charges will be determined and assessed pursuant to Section 18 of the State Finance Law.

52. REMEDIES FOR BREACH It is understood and agreed that all rights and remedies afforded below shall be in addition to all remedies or actions otherwise authorized or permitted by law:

a. Cover/Substitute Performance In the event of Contractor's material, uncured breach, the Commissioner may, with or without formally Bidding: (i) Purchase from other sources; or (ii) If the Commissioner is unsuccessful after making reasonable attempts, under the circumstances then-existing, to timely obtain acceptable service or acquire replacement Product of equal or comparable quality, the Commissioner may acquire acceptable replacement service or Product of lesser or greater quality.

Such purchases may be deducted from the Contract quantity without penalty or liability to the State. The Commissioner agrees that Authorized Users shall accept allocated performance or deliveries during a period where Contractor is making good faith efforts to cure a material breach.

b. Withhold Payment In any case where a reasonable question of material, uncured non-performance by Contractor arises, payment may be withheld in whole or in part at the discretion of the Commissioner. Should Contractor and the Commissioner fail to agree upon the question of "materiality" in an instance of non-performance, such failure to agree shall be a dispute under the Disputes clause.

c. Bankruptcy In the event that the Contractor files, or there is filed against Contractor, a petition under the U.S. Bankruptcy Code during the term of this Centralized Contract, Authorized Users may, at their discretion, make application to exercise its right to set-off against monies due the Debtor or, under the Doctrine of Recoupment, be credited the amounts owed by the Contractor arising out of the same transactions.

d. Reimbursement of Costs Incurred The Contractor agrees to reimburse the Authorized User promptly for any and all additional costs and expenses incurred for acquiring acceptable services, and/or replacement Product. Should the cost of cover be less than the Contract price, the Contractor shall have no claim to the difference. The Contractor covenants and agrees that in the event suit is successfully prosecuted for any default on the part of the Contractor, all costs and expenses, including reasonable attorney's fees awarded by a court of competent jurisdiction, shall be paid by the Contractor.

Where the Contractor fails to timely deliver pursuant to the guaranteed delivery terms of the Contract, the ordering Authorized User may obtain substitute Product temporarily and the cost of the replacement Product shall be deducted from the Contract quantity without penalty or liability to the State.

e. Deduction/Credit Sums due as a result of these remedies may be deducted or offset by the Authorized User from payments due, or to become due, the Contractor on the same or another transaction. If no deduction or only a partial deduction is made in such fashion the Contractor shall pay to the Authorized User the amount of such claim or portion of the claim still outstanding, on demand. The Commissioner reserves the right to determine the disposition of any rebates, settlements, restitution, damages, etc., that arise from the administration of the Contract.

53. ASSIGNMENT OF CLAIM Contractor hereby assigns to the State any and all claims for overcharges associated with this Contract that may arise under the antitrust laws of the United States, 15 USC Section 1, et. seq. and the antitrust laws of the State of New York, General Business Law Section 340, et. seq.

54. TOXIC SUBSTANCES Each Contractor furnishing a toxic substance, as defined by Section 875 of the Labor Law, shall provide such Authorized User with not less than two copies of a Material Safety Data Sheet, which sheet shall include for each such substance the information outlined in Section 876 of the Labor Law.

Before any chemical product is used or applied on or in any building, a copy of the product label and Material Safety Data Sheet must be provided to and approved by the Authorized User representative.

55. INDEPENDENT CONTRACTOR It is understood and agreed that the legal status of the Contractor, its agents, officers and employees under this Contract is that of an independent Contractor, and in no manner shall they be deemed employees of the Authorized User, and therefore are not entitled to any of the benefits associated with such employment.

56. SECURITY Contractor warrants, covenants and represents that it will comply fully with all security procedures of the Authorized User(s) in performance of the Contract including but not limited to physical, facility, documentary and cyber security rules, procedures and protocols.

57. COOPERATION WITH THIRD PARTIES The Contractor shall be responsible for fully cooperating with any third party, including but not limited to other Contractors or Subcontractors of the Authorized User, as necessary to ensure delivery or performance of Product.

58. CONTRACT TERM - RENEWAL In addition to any stated renewal periods in the Contract, any Contract or unit portion thereof let by the Commissioner may be extended by the Commissioner for an additional period(s) of up to one year with the written concurrence of the Contractor and Comptroller. Such extension may be exercised on a month-to-month basis or in other stated periods of time during the one year extension.

59. WARRANTIES

a. Product Performance Where Contractor, Product manufacturer or service provider generally offers additional or more advantageous warranties than set forth below, Contractor shall offer or pass through any such warranties to Authorized Users.

In addition, Contractor hereby warrants and represents that the Products acquired by the Authorized User under the terms and conditions of this Contract conform to the manufacturer's specifications, performance standards and documentation, and the

documentation fully describes the proper procedure for using the Products.

Contractor further warrants and represents that Products, components or deliverables specified and furnished by or through Contractor shall individually, and where specified and furnished as a system, be free from defects in material and workmanship and will conform with all requirements of the Contract for the warranty period, or for a minimum of one (1) year from the date of acceptance, whichever is longer ("Project warranty period").

Unless recycled or recovered materials are available in accordance with the Remanufactured, Recycled, Recyclable or Recovered Materials clause, Product offered shall be standard new equipment, current model or most recent release of regular stock product with all parts regularly used with the type of equipment offered. Contractor further warrants and represents that no attachment or part has been substituted or applied contrary to the manufacturer's recommendations and standard practice.

b. Title and Ownership Contractor warrants and represents that it has (i) full ownership, clear title free of all liens, or (ii) the right to transfer or deliver specified license rights to any Products acquired by Authorized User under this Contract. Contractor shall be solely liable for any costs of acquisition associated therewith. Contractor shall indemnify Authorized Users and hold Authorized Users harmless from any damages and liabilities (including reasonable attorneys' fees and costs) awarded by a court of competent jurisdiction arising from any breach of Contractor's warranties as set forth herein.

c. Product Warranty for Deliverables During the Project warranty period, defects in the materials or workmanship of components or deliverables specified and furnished by or through Contractor shall be repaired or replaced by Contractor at no cost or expense to the Authorized User. Contractor shall extend the Project warranty period for individual component(s), or for the system as a whole, as applicable, by the cumulative period(s) of time, after notification, during which an individual component or the system requires servicing or replacement (down time) or is in the possession of the Contractor, its agents, officers, Subcontractors, distributors, resellers or employees ("extended warranty").

Where Contractor, the Independent Software Vendor (ISV), or other third-party manufacturer markets any project deliverable delivered by or through Contractor with a standard commercial warranty, such standard warranty shall be in addition to, and not relieve the Contractor from, Contractor's warranty obligations during the Project warranty and extended warranty period(s). Where such standard commercial warranty covers all or some of the Project warranty or extended warranty period(s), Contractor shall be responsible for the coordination during the Project warranty or extended warranty period(s) with ISV or other third party manufacturer(s) for warranty repair or replacement of ISV or other third-party manufacturer's Product.

Where Contractor, ISV or other third-party manufacturer markets any Project Deliverable with a standard commercial warranty which goes beyond the Project warranty or extended warranty period(s), Contractor shall notify the Authorized User and pass through the manufacturer's standard commercial warranty to Authorized User at no additional charge; provided, however, that Contractor shall not be responsible for coordinating services under the third-party extended warranty after expiration of the Project warranty and extended warranty period(s).

The Commissioner agrees that Contractor is not responsible for any modification of the Products made by an Authorized User without Contractor's approval.

d. Replacement Parts Warranty If during the regular or extended warranty periods, parts or components break or fail to perform as intended, the Contractor shall promptly repair or, upon demand, replace the defective unit or component part affected. All costs for labor and material and transportation incurred to repair or replace defective Product during the warranty period(s) shall be borne solely by the Contractor, and the State or Authorized User shall in no event be liable or responsible therefor.

Any Product or parts thereof replaced by the Contractor under the Contract warranty shall be replaced at no cost to the Authorized User and guaranteed for the greater of: a) the Warranty Period set forth under paragraph (a) above; or b) if a separate warranty for that Product or parts thereof is generally offered by the manufacturer, the standard commercial warranty period offered by the manufacturer for the individual part or component.

e. Virus Warranty The Contractor represents and warrants that any Licensed Software acquired by the Authorized User does not contain any known viruses. Contractor is not responsible for viruses introduced at Licensee's site.

f. Date/Time Warranty Contractor warrants that Product furnished pursuant to this Contract shall, when used in accordance with the Product documentation, be able to accurately process date/time data (including, but not limited to, calculating, comparing, and sequencing) transitions, including leap year calculations. Where a Contractor proposes or an acquisition requires that specific Products must perform as a package or system, this warranty shall apply to the Products as a system.

Where Contractor is providing ongoing services, including but not limited to: i) consulting, integration, code or data conversion, ii) maintenance or support services, iii) data entry or processing, or iv) contract administration services (e.g., billing, invoicing, claim processing), Contractor warrants that services shall be provided in an accurate and timely manner without interruption, failure or error due to the inaccuracy of Contractor's business operations in processing date/time data (including, but not limited to, calculating, comparing, and sequencing) various date/time transitions, including leap year calculations. Contractor shall be responsible for damages resulting from any delays, errors or untimely performance resulting therefrom, including but not limited to the failure or untimely performance of such services.

This Date/Time Warranty shall survive beyond termination or expiration of this contract as long as the Product is used by the governmental entity, or its successor, for whom the Product was originally purchased." Nothing in this warranty statement shall be construed to limit any rights or remedies otherwise available under this Contract for breach of warranty.

g. Workmanship Warranty Contractor warrants that the services acquired under this Contract will be provided in a professional and workmanlike manner in accordance with industry standards. The Authorized User must notify Contractor of any services warranty deficiencies within ninety calendar days from performance of the services that gave rise to the warranty claim.

h. Miscellaneous The Authorized User shall promptly notify the Contactor and the Commissioner in writing of any claim of breach of any warranty provided herein.

The rights and remedies of the State and the Authorized Users provided in this clause are in addition to and do not limit any rights afforded to the State and the Authorized Users by any other clause of the Contract.

60. LEGAL COMPLIANCE Contractor represents and warrants that it shall secure all notices and comply with all applicable laws, ordinances, rules and regulations of any governmental entity in conjunction with the performance of obligations under the Contract. Prior to award and during the Contract term and any renewals thereof, Contractor must establish to the satisfaction of the Commissioner that it meets or exceeds all requirements of the Bid and Contract and any applicable laws, including but not limited to, permits, licensing, and shall provide such proof as required by the Commissioner. Failure to comply or failure to provide proof may constitute grounds for the Commissioner to terminate or suspend the Contract, in whole or in part, or to take any other action deemed necessary by the Commissioner. Contractor also agrees to disclose information and provide affirmations and certifications to comply with Sections 139-j and 139-k of the State Finance Law.

61. INDEMNIFICATION Contractor shall be fully liable for the actions of its agents, employees, partners or Subcontractors and shall fully defend, indemnify and hold harmless the Authorized Users from suits, actions, damages and costs of every name and description relating to personal injury and damage to real or personal tangible property caused by any intentional act or negligence of Contractor, its agents, employees, partners or Subcontractors, which shall arise from or result directly or indirectly from this Contract, without limitation; provided, however, that the Contractor shall not indemnify to the extent any claim, loss or damage arising hereunder solely due to the negligent act, failure to act, gross negligence or willful misconduct of the Authorized Users.

The Commissioner shall give Contractor: (i) prompt written notice of any action, claim or threat of suit, or other suit, (ii) the opportunity to take over, settle or defend such action, claim or suit at Contractor's sole expense, and (iii) assistance in the defense of any such action, claim or suit at the expense of Contractor.

In the event that an action or proceeding at law or in equity is commenced against the Authorized User arising out of a claim for death, personal injury or damage to real or personal tangible property caused by any intentional or willful act, gross negligence, or negligence of Contractor, its agents, employees, partners or Subcontractors, which shall arise from or result directly or indirectly from the Products supplied under this Contract, and Contractor is of the opinion that the allegations in such action in whole or in part are not covered by the indemnification and defense provisions set forth in the Contract, Contractor shall immediately notify the Authorized User and the New York State Office of the Attorney General in writing and shall specify to what extent Contractor believes it is obligated to defend and indemnify under the terms and conditions of the Contract and to what extent it is not so obligated to defend and indemnify. Contractor shall in such event attempt to secure a continuance to permit the State and the Authorized User to appear and defend their interests in cooperation with Contractor, as is appropriate, including any jurisdictional defenses the State and Authorized User may have. In the event of a dispute regarding the defense, the Contractor and the Attorney General shall try to reach an amicable resolution, but the Attorney General shall have the final determination on such matters.

62. INDEMNIFICATION RELATING TO THIRD PARTY RIGHTS The Contractor will also defend, indemnify and hold the Authorized Users harmless from and against any and all damages, expenses (including reasonable attorneys' fees), claims, judgments, liabilities and costs in any action for infringement of a patent, copyright, trademark, trade secret or other proprietary right provided: a) such claim arises solely out of the Products as supplied by the Contractor, and not out of any modification to the Products made by Authorized User or by someone other than Contractor at the direction of the Authorized User without Contractor's approval, or by reason of an off-the-shelf component; and b) Authorized User gives Contractor prompt written notice of any such action, claim suit or threat of suit alleging infringement.

At Authorized User's option, Contractor may be given the opportunity to take over, settle or defend such action, claim or suit at Contractor's sole expense, and to provide assistance in the defense of any such action, claim or suit at the expense of Contractor.

Such indemnity shall only be applicable in the event of claims, judgments, liabilities and/or costs that may be finally assessed against Authorized User in any action for infringement of a patent, or of any copyright, trademark, trade secret or other third party proprietary right except to the extent such claims, judgments, liabilities and/or costs arise solely from the Authorized Users negligent act, failure to act, gross negligence or willful misconduct.

If usage of a Product shall be enjoined for any reason or if Contractor believes that it may be enjoined, Contractor shall have the right, at its own expense and sole discretion to take action in the following order of precedence: (i) to procure for the Authorized User the right to continue Usage (ii) to modify the service or Product so that usage becomes non-infringing, and is of at least equal quality and performance; or (iii) to replace such Product or parts thereof, as applicable, with non-infringing Product of at least eqal quality and performance. If the above remedies are not available, the parties shall terminate the Contract, in whole or in part as necessary and applicable, provided that the Authorized User is given a refund for any amounts paid for the period during which usage was not feasible.

In the event that an action at law or in equity is commenced against the Authorized User arising out of a claim that the Authorized User's use of the Product under the Contract infringes any patent, copyright, trademark, trade secret or proprietary right, and Contractor is of the opinion that the allegations in such action in whole or in part are not covered by the indemnification and defense provisions set forth in the Contract, Contractor shall immediately notify the Authorized User and the Office of the Attorney General in writing and shall specify to what extent Contractor believes it is obligated to defend and indemnify under the terms and conditions of the Contract and to what extent it is not so obligated to defend and indemnify. Contractor shall in such event protect the interests of the Authorized User and seek to secure a continuance to permit the Authorized User to appear and defend their interests in cooperation with Contractor, as is appropriate, including any jurisdictional defenses the Authorized User may have. - -This constitutes the Authorized User's sole and exclusive remedy for patent infringement, or for infringement of any other third party proprietary right.

63. LIMITATION OF LIABILITY Except as otherwise set forth in the Indemnification clause and the Indemnification Relating to Third Party Rights clause, the limit of liability shall be as follows:

a. Contractor's liability for any claim, loss or liability arising out of, or connected with the Products provided, and whether based upon default, or other liability such as breach of contract, warranty, negligence, misrepresentation or otherwise, shall in no case exceed direct damages in: (i) an amount equal to two (2) times the charges specified in the Purchase Order for the Products and services, or parts thereof forming the basis of the Authorized User's claim (said amount

not to exceed a total of twelve (12) months charges payable under the applicable Purchase Order) or (ii) five hundred thousand dollars ($500,000), whichever is greater.

b. The Authorized User may retain such monies from any amount due Contractor as may be necessary to satisfy any claim for damages, costs and the like asserted against the Authorized User unless Contractor at the time of the presentation of claim shall demonstrate to the Authorized User's satisfaction that sufficient monies are set aside by the Contractor in the form of a bond or through insurance coverage to cover associated damages and other costs.

c. Notwithstanding the above, neither the Contractor nor the Authorized User shall be liable for any consequential, indirect or special damages of any kind which may result directly or indirectly from such performance, including, without limitation, damages resulting from loss of use or loss of profit by the Authorized User, the Contractor, or by others.

64. DISPUTES

a. Informal Dispute Resolution Process

1. It is the policy of OGS to provide vendors with an opportunity to administratively resolve disputes, complaints or inquiries related to OGS bid solicitations, contract awards or contract administration. If the Parties are not able to resolve their dispute between themselves as set forth below, OGS encourages vendors to seek resolution of disputes through consultation with OGS staff. Such consultation is voluntary. All such matters will be accorded impartial and timely consideration. Interested parties may also file formal written disputes. A copy of the Dispute Resolution Procedures for Vendors may be obtained by contacting the person identified in the Contract as a designated contact or through the OGS website (www.ogs.ny.gov).

2. In the event there is a dispute or controversy under this Centralized Contract, the Contractor, OGS and Authorized User agree to exercise their best efforts to resolve the dispute as soon as possible. The Contractor, OGS and Authorized User shall, without delay, continue to perform their respective obligations under this Centralized Contract which are not affected by the dispute. Primary responsibility for resolving any dispute arising under this Centralized Contract shall rest with the Authorized User's Contractor Coordinators and the Contractor's Account Executive and the State & Local Government Regional General Manager.

3. In the event the Authorized User is dissatisfied with the Contractor's Products provided under this Centralized Contract, the Authorized User shall notify the Contractor in writing pursuant to the terms of the Contract. In the event the Contractor has any disputes with the Authorized User, the Contractor shall so notify the Authorized User in writing. If either party notifies the other of such dispute or controversy, the other party shall then make good faith efforts to solve the problem or settle the dispute amicably, including meeting with the party's representatives to attempt diligently to reach a satisfactory result.

4. If negotiation between such persons fails to resolve any such dispute to the satisfaction of the parties within fourteen (14) business days or as otherwise agreed to by the Contractor and Authorized User, of such notice, then the matter shall be submitted to the State's Contract Administrator and the Contractor's senior officer of the rank of Vice President or higher as its representative. Such representatives shall meet in person and shall attempt in good faith to resolve the dispute within the next fourteen (14) business days or as otherwise agreed to by the parties. This meeting must be held before either party may seek any other method of dispute resolution, including judicial or governmental resolutions. Notwithstanding the foregoing, this section shall not be construed to prevent either party from seeking and obtaining temporary equitable remedies, including injunctive relief.

5. The Contractor shall extend the dispute resolution period for so long as the Authorized User continues to make reasonable efforts to cure the breach, except with respect to disputes about the breach of payment of fees or infringement of its or its licensors' intellectual property rights.

b. Formal Disputes

1. Definitions

a. Filed means the complete receipt of any document by OGS before its close of business.

b. Dispute means a written objection by Contractor to any of the following:

i. A solicitation or other request by OGS for offers for a contract for the procurement of commodities or services.

ii. The cancellation of the solicitation or other request by OGS.

iii. An award or proposed award of the Contract by OGS.

iv. A termination or cancellation of an award of the Contract by OGS.

v. Changes in the Scope of the Centralized Contract by the Commissioner.

vi. Determination of "materiality" in an instance of nonperformance or contractual breach.

vii. An equitable adjustment in the Centralized Contract terms and/or pricing made by the Commissioner during a Force Majeure event.

2. Submission of Disputes

a. A formal dispute by Contractor must be filed in writing to OGS by mail, email or facsimile.

3. The dispute must include:

a. Name, address, e-mail address, fax and telephone numbers of the filer.

b. Solicitation or Contract number.

c. Detailed statement of the legal and factual grounds for the dispute, including a description of resulting prejudice to the filer.

d. Copies of relevant documents.

e. Request for a ruling by the agency.

f. Statement as to the form of relief requested.

g. All information establishing that the filer is an interested party for the purpose of filing a dispute.

h. All information establishing the timeliness of the dispute.

Disputes must be filed with the Director of OGS New York State Procurement (NYSPro) at the following address:

New York State Office of General Services
Director, NYSPro
38th Floor, Corning Tower
Empire State Plaza
Albany, NY 12242
Facsimile: (518) 474-2347

Disputes concerning the administration of the Contract after award must be filed within twenty (20) business days by Contractor after the Authorized User and Contractor fails to reach resolution through the Informal Dispute Resolution Process.

4. Agency Response

1. OGS will consider all information relevant to the dispute, and may, at its discretion, suspend, modify, or cancel the disputed

procurement/Contract action prior to issuance of a formal dispute decision.

2. OGS reserves the right to require the Contractor to meet or participate in a conference call with OGS to discuss the dispute when, in its sole judgment, circumstances so warrant.

3. OGS reserves the right to waive or extend the time requirements for decisions and final determination on appeals herein prescribed when, in its sole judgment, circumstances so warrant.

4. OGS reserves the right to consider or reject the merits of any dispute.

5. Notice of Decision: A copy of the decision, stating the reason(s) upon which it is based and informing the filer of the right to appeal an unfavorable decision to the Chief Procurement Officer shall be sent to the filer or its agent by regular mail within thirty (30) business days of receipt of the dispute.

5. **Appeals**

a. Should the filer be dissatisfied with the dispute determination, a written appeal may be directed to:

Chief Procurement Officer
New York State Office of General Services
NYSPro
38th Floor, Corning Tower
Empire State Plaza
Albany, NY 12242
Facsimile: (518) 474-2347

b. Written notice of appeal of a determination must be received at the above address no more than ten (10) business days after the date the decision is received by the filer. The decision of the Director of NYSPro shall be a final and conclusive agency determination unless appealed to the Chief Procurement Officer within such time period.

c. The Chief Procurement Officer shall hear and make a final determination on all appeals or may designate a person or persons to act on his/her behalf. The final determination on the appeal shall be issued within twenty (20) business days of receipt of the appeal.

d. An appeal of the decision of the Director of NYSPro shall not include new facts and information unless requested in writing by the Chief Procurement Officer.

e. The decision of the Chief Procurement Officer shall be a final and conclusive agency determination.

6. **Legal Appeals** Nothing contained in these provisions is intended to limit or impair the rights of Contractor to seek and pursue remedies of law through the judicial process.

THE FOLLOWING CLAUSES PERTAIN TO TECHNOLOGY & NEGOTIATED CONTRACTS

65. SOFTWARE LICENSE GRANT Where Product is acquired on a licensed basis the following shall constitute the license grant:

a. License Scope Licensee is granted a non-exclusive, perpetual license to use, execute, reproduce, display, perform, or merge the Product within its business enterprise in the United States up to the maximum licensed capacity stated on the Purchase Order. Product may be accessed, used, executed, reproduced, displayed or performed up to the capacity measured by the applicable licensing unit stated on the Purchase Order (i.e., payroll size, number of employees, CPU, MIPS, MSU, concurrent user, workstation). Licensee shall have the right to use and distribute modifications or customizations of the Product to and for use by any Authorized Users otherwise licensed to use the Product, provided that any modifications, however extensive, shall not diminish Licensor's proprietary title or interest. No license, right or interest in any trademark, trade name, or service mark is granted hereunder.

b. License Term The License Term shall commence upon the License Effective Date, provided, however, that where an acceptance or trial period applies to the Product, the License Term shall be extended by the time period for testing, acceptance or trial.

c. Licensed Documentation If commercially available, Licensee shall have the option to require the Contractor to deliver, at Contractor's expense: (i) one (1) hard copy and one (1) master electronic copy of the Documentation in a mutually agreeable format; (ii) hard copy instructions for access by downloading from the Internet (iii) hard copies of the Product Documentation by type of license in the following amounts, unless otherwise mutually agreed:

- Individual/Named User License - one (1) copy per License
- Concurrent Users - 10 copies per site
- Processing Capacity - 10 copies per site

Software media must be in a format specified by the Authorized User, without requiring any type of conversion.

Contractor hereby grants to Licensee a perpetual license right to make, reproduce (including downloading electronic copies of the Product) and distribute, either electronically or otherwise, copies of Product Documentation as necessary to enjoy full use of the Product in accordance with the terms of license.

d. Product Technical Support & Maintenance Licensee shall have the option of electing the Product technical support and maintenance ("maintenance") set forth in the Contract by giving written notice to Contractor any time during the Centralized Contract term. Maintenance term(s) and any renewal(s) thereof are independent of the expiration of the Centralized Contract term and will not automatically renew.

Maintenance shall include, at a minimum, (i) the provision of error corrections, updates, revisions, fixes, upgrade and new releases to Licensee, and (ii) Help Desk assistance with locally accessible "800" or toll free, local telephone service, or alternatively on-line Help Desk accessibility. Contractor shall maintain the Products so as to provide Licensee with the ability to utilize the Products in accordance with the Product Documentation without significant functional downtime to its ongoing business operations during the maintenance term.

Authorized User shall not be required to purchase maintenance for use of Product, and may discontinue maintenance at the end of any current maintenance term upon notice to Contractor. In the event that Authorized User does not initially acquire or discontinues maintenance of licensed Product, it may, at any time thereafter, reinstate maintenance for Product without any additional penalties or other charges, by paying Contractor the amount which would have been due under the Contract for the period of time that such maintenance had lapsed, at then current NYS net maintenance rates.

e. Permitted License Transfers As Licensee's business operations may be altered, expanded or diminished, licenses granted hereunder may be transferred or combined for use at an alternative or consolidated site not originally specified in the license, including transfers between Agencies ("permitted license transfers"). Licensee(s) do not have to obtain the approval of Contractor for permitted license transfers, but must give thirty (30) days prior written notice to Contractor of such move(s) and certify in writing that the Product is not in use at the prior site. There shall be no additional

license or other transfer fees due Contractor, provided that: i) the maximum capacity of the consolidated machine is equal to the combined individual license capacity of all licenses running at the consolidated or transferred site (e.g., named users, seats, or MIPS); or ii) if the maximum capacity of the consolidated machine is greater than the individual license capacity being transferred, a logical or physical partition or other means of restricting access will be maintained within the computer system so as to restrict use and access to the Product to that unit of licensed capacity solely dedicated to beneficial use for Licensee. In the event that the maximum capacity of the consolidated machine is greater than the combined individual license capacity of all licenses running at the consolidated or transferred site, and a logical or physical partition or other means of restricting use is not available, the fees due Contractor shall not exceed the fees otherwise payable for a single license for the upgrade capacity.

f. Restricted Use By Outsourcers / Facilities Management, Service Bureaus / or Other Third Parties Outsourcers, facilities management or service bureaus retained by Licensee shall have the right to use the Product to maintain Licensee's business operations, including data processing, for the time period that they are engaged in such activities, provided that: 1) Licensee gives notice to Contractor of such party, site of intended use of the Product, and means of access; and 2) such party has executed, or agrees to execute, the Product manufacturer's standard nondisclosure or restricted use agreement which executed agreement shall be accepted by the Contractor ("Non-Disclosure Agreement"); and 3) if such party is engaged in the business of facility management, outsourcing, service bureau or other services, such third party will maintain a logical or physical partition within its computer system so as to restrict use and access to the program to that portion solely dedicated to beneficial use for Licensee. In no event shall Licensee assume any liability for third party's compliance with the terms of the Non-Disclosure Agreement, nor shall the Non-Disclosure Agreement create or impose any liabilities on the State or Licensee.

Any third party with whom a Licensee has a relationship for a state function or business operation, shall have the temporary right to use Product (e.g., JAVA Applets), provided that such use shall be limited to the time period during which the third party is using the Product for the function or business activity.

g. Archival Back-Up and Disaster Recovery Licensee may use and copy the Product and related Documentation in connection with: i) reproducing a reasonable number of copies of the Product for archival backup and disaster recovery procedures in the event of destruction or corruption of the Product or disasters or emergencies which require Licensee to restore backup(s) or to initiate disaster recovery procedures for its platform or operating systems; ii) reproducing a reasonable number of copies of the Product and related Documentation for cold site storage. "Cold Site" storage shall be defined as a restorable back-up copy of the Product not to be installed until and after the declaration by the Licensee of a disaster; iii) reproducing a back-up copy of the Product to run for a reasonable period of time in conjunction with a documented consolidation or transfer otherwise allowed herein. "Disaster Recovery" shall be defined as the installation and storage of Product in ready-to-execute, back-up computer systems prior to disaster or breakdown which is not used for active production or development.

h. Confidentiality Restrictions The Product is a trade secret, copyrighted and proprietary product. Licensee and its employees will keep the Product strictly confidential, and Licensee will not disclose or otherwise distribute or reproduce any Product to anyone other than as authorized under the terms of Contract. Licensee will not remove or destroy any proprietary markings of Contractor.

i. Restricted Use by Licensee Except as expressly authorized by the terms of license, Licensee shall not:

(i) Copy the Product;

(ii) Cause or permit reverse compilation or reverse assembly of all or any portion of the Product;

(iii) Export the Licensed Software in violation of any U.S. Department of Commerce export administration regulations.

66. <u>PRODUCT ACCEPTANCE</u> Unless otherwise provided by mutual agreement of the Authorized User and the Contractor, Authorized User(s) shall have thirty (30) days from the date of delivery to accept hardware Products and sixty (60) days from the date of delivery to accept all other Product. Where the Contractor is responsible for installation, acceptance shall be from completion of installation. Title or other property interest and risk of loss shall not pass from Contractor to the Authorized User until the Products have been accepted. Failure to provide notice of acceptance or rejection or a deficiency statement to the Contractor by the end of the period provided for under this clause constitutes acceptance by the Authorized User(s) as of the expiration of that period. The License Term shall be extended by the time periods allowed for trial use, testing and acceptance unless the Commissioner or Authorized User agrees to accept the Product at completion of trial use.

Unless otherwise provided by mutual agreement of the Authorized User and the Contractor, Authorized User shall have the option to run testing on the Product prior to acceptance, such tests and data sets to be specified by User. Where using its own data or tests, Authorized User must have the tests or representative set of data available upon delivery. This demonstration will take the form of a documented installation test, capable of observation by the Authorized User, and shall be made part of the Contractor's standard documentation. The test data shall remain accessible to the Authorized User after completion of the test.

In the event that the documented installation test cannot be completed successfully within the specified acceptance period, and the Contractor or Product is responsible for the delay, Authorized User shall have the option to cancel the order in whole or in part, or to extend the testing period for an additional thirty (30) day increment. Authorized User shall notify Contractor of acceptance upon successful completion of the documented installation test. Such cancellation shall not give rise to any cause of action against the Authorized User for damages, loss of profits, expenses, or other remuneration of any kind.

If the Authorized User elects to provide a deficiency statement specifying how the Product fails to meet the specifications within the testing period, Contractor shall have thirty (30) days to correct the deficiency, and the Authorized User shall have an additional sixty (60) days to evaluate the Product as provided herein. If the Product does not meet the specifications at the end of the extended testing period, Authorized User, upon prior written notice to Contractor, may then reject the Product and return all defective Product to Contractor, and Contractor shall refund any monies paid by the Authorized User to Contractor therefor. Costs and liabilities associated with a failure of the Product to perform in accordance with the functionality tests or product specifications during the acceptance period shall be borne fully by Contractor to the extent that said costs or liabilities shall not have been caused by negligent or willful acts or omissions of the Authorized User's agents or employees. Said costs shall be limited to the amounts set forth in the Limitation of Liability Clause for any liability for costs incurred at the direction or recommendation of Contractor. When Product is not accepted, it must be removed by the

Contractor from the premises of the Authorized User within ten calendar days of notification of non-acceptance by the Authorized User. Rejected items not removed by the Contractor within the ten calendar day period shall be regarded as abandoned by the Contractor and the Authorized User shall have the right to dispose of Product as its own property. The Contractor shall promptly reimburse the Authorized User for any costs incurred in storage or effecting removal or disposition after the ten calendar day period.

67. AUDIT OF LICENSED PRODUCT USAGE Contractor shall have the right to periodically audit, no more than annually, at Contractor's expense, use of licensed Product at any site where a copy of the Product resides provided that: (i) Contractor gives Licensee(s) at least thirty (30) days advance written notice, (ii) such audit is conducted during such party's normal business hours, (iii) the audit is conducted by an independent auditor chosen on mutual agreement of the parties. Contractor shall recommend a minimum of three (3) auditing/accounting firms from which the Licensee will select one (1). In no case shall the Business Software Alliance (BSA), Software Publishers Association (SPA), Software and Industry Information Association (SIIA) or Federation Against Software Theft (FAST) be used directly or indirectly to conduct audits, or be recommended by Contractor; (iv) Contractor and Licensee are each entitled to designate a representative who shall be entitled to participate, and who shall mutually agree on audit format, and simultaneously review all information obtained by the audit. Such representatives also shall be entitled to copies of all reports, data or information obtained from the audit; and (v) if the audit shows that such party is not in compliance, Licensee shall be required to purchase additional licenses or capacities necessary to bring it into compliance and shall pay for the unlicensed capacity at the NYS Net Price in effect at time of audit, or if none, then at the Contractor's U.S. Commercial list price. Once such additional licenses or capacities are purchased, Licensee shall be deemed to have been in compliance retroactively, and Licensee shall have no further liability of any kind for the unauthorized use of the software.

68. OWNERSHIP/TITLE TO PROJECT DELIVERABLES

a. Definitions

(i) For purposes of this clause, "Products." Deliverables furnished under this Contract by or through Contractor, including existing and custom Products, including, but not limited to: a) components of the hardware environment, b) printed materials (including but not limited to training manuals, system and user documentation, reports, drawings), whether printed in hard copy or maintained on diskette, CD, DVD or other electronic media c) third party software, d) modifications, customizations, custom programs, program listings, programming tools, data, modules, components, and e) any properties embodied therein, whether in tangible or intangible form (including but not limited to utilities, interfaces, templates, subroutines, algorithms, formulas, source code, object code).

(ii) For purposes of this clause, "Existing Products." Tangible Products and intangible licensed Products that exist prior to the commencement of work under the Contract. Contractor bears the burden of proving that a particular product was in existence prior to the commencement of the Project.

(iii) For purposes of this clause, "Custom Products." Products, preliminary, final or otherwise, which are created or developed by Contractor, its Subcontractors, partners, employees or agents for Authorized User under the Contract.

b. Title to Project Deliverables Contractor acknowledges that it is commissioned by the Authorized User to perform the services detailed in the Purchase Order. Unless otherwise specified in writing in the Bid or Purchase Order, the Authorized User shall have ownership and license rights as follows:

(i) Existing Products:

1. Hardware - Title and ownership of Existing Hardware Product shall pass to Authorized User upon Acceptance.

2. Software - Title and ownership to Existing Software Product(s) delivered by Contractor under the Contract that is normally commercially distributed on a license basis by the Contractor or other independent software vendor proprietary owner ("Existing Licensed Product"), whether or not embedded in, delivered or operating in conjunction with hardware or Custom Products, shall remain with Contractor or the proprietary owner of other independent software vendor(s) (ISV). Effective upon acceptance, such Product shall be licensed to Authorized User in accordance with the Contractor or ISV owner's standard license agreement, provided, however, that such standard license, must, at a minimum: (a) grant Authorized User a non-exclusive, perpetual license to use, execute, reproduce, display, perform, adapt (unless Contractor advises Authorized User as part of Contractor's proposal that adaptation will violate existing agreements or statutes and Contractor demonstrates such to the Authorized User's satisfaction) and distribute Existing Licensed Product to the Authorized User up to the license capacity stated in the Purchase Order or work order with all license rights necessary to fully effect the general business purpose(s) stated in the Bid or Authorized User's Purchase Order or work order, including the financing assignment rights set forth in paragraph (c) below; and (b) recognize the State of New York as the licensee where the Authorized User is a state agency, department, board, commission, office or institution. Where these rights are not otherwise covered by the ISV's owner's standard license agreement, the Contractor shall be responsible for obtaining these rights at its sole cost and expense. The Authorized User shall reproduce all copyright notices and any other legend of ownership on any copies authorized under this clause.

(ii) Custom Products: Effective upon creation of Custom Products, Contractor hereby conveys, assigns and transfers to Authorized User the sole and exclusive rights, title and interest in Custom Product(s), whether preliminary, final or otherwise, including all trademark and copyrights. Contractor hereby agrees to take all necessary and appropriate steps to ensure that the Custom Products are protected against unauthorized copying, reproduction and marketing by or through Contractor, its agents, employees, or Subcontractors. Nothing herein shall preclude the Contractor from otherwise using the related or underlying general knowledge, skills, ideas, concepts, techniques and experience developed under a Purchase Order, project definition or work order in the course of Contractor's business. Authorized User may, by providing written notice thereof to the Contractor, elect in the alternative to take a non-exclusive perpetual license to Custom Products in lieu of Authorized User taking exclusive ownership and title to such Products. In such case, Licensee on behalf of all Authorized Users shall be granted a non-exclusive perpetual license to use, execute, reproduce, display, perform, adapt and distribute Custom Product as necessary to fully effect the general business purpose(s) as stated in paragraph (b)(i)(2), above.

c. Transfers or Assignments to a Third Party Financing Agent It is understood and agreed by the parties that a condition precedent to the consummation of the purchase(s) under the Contract may be the obtaining of acceptable third party financing by the Authorized User. The Authorized User shall make the sole determination of the acceptability of any financing proposal. The Authorized User will make all reasonable efforts to obtain such financing, but makes no representation that such financing has been obtained as of the date of Bid receipt. Where financing is used, Authorized User may assign or transfer its rights in Licensed Products (existing or custom) to a third party financing entity or trustee ("Trustee") as collateral where required

by the terms of the financing agreement. Trustee's sole rights with respect to transferability or use of Licensed Products shall be to exclusively sublicense to Authorized User all of its Licensee's rights under the terms and conditions of the License Agreement; provided, further, however, in the event of any termination or expiration of such sublicense by reason of payment in full, all of Trustee's rights in such Licensed Product shall terminate immediately and Authorized User's prior rights to such Existing Licensed Product shall be revived.

d. Sale or License of Custom Products Involving Tax-Exempt Financing (i.e., Certificates of Participation - COPS) The Authorized User's sale or other transfer of Custom Products which were acquired by the Authorized User using third party, tax-exempt financing may not occur until such Custom Products are, or become, useable. In the event that the Contractor wishes to obtain ownership rights to Custom Product(s), the sale or other transfer shall be at fair market value determined at the time of such sale or other transfer, and must be pursuant to a separate written agreement in a form acceptable to the Authorized User which complies with the terms of this clause.

e. Contractor's Obligation with Regard to ISV (Third Party) Product Where Contractor furnishes Existing Licensed Product(s) as a Project Deliverable, and sufficient rights necessary to effect the purposes of this section are not otherwise provided in the Contractor or ISV's standard license agreement, Contractor shall be responsible for obtaining from the ISV third party proprietary owner/developer the rights set forth herein to the benefit of the Authorized User at Contractor's sole cost and expense.

69. PROOF OF LICENSE The Contractor must provide to each Licensee who places a Purchase Order either: (i) the Product developer's certified License Confirmation Certificates in the name of such Licensee; or (ii) a written confirmation from the Proprietary owner accepting Product invoice as proof of license. Contractor shall submit a sample certificate, or alternatively such written confirmation from the proprietary developer. Such certificates must be in a form acceptable to the Licensee.

70. PRODUCT VERSION Purchase Orders shall be deemed to reference Manufacturer's most recently released model or version of the Product at time of order, unless an earlier model or version is specifically requested in writing by Authorized User and Contractor is willing to provide such version.

71. CHANGES TO PRODUCT OR SERVICE OFFERINGS

a. Product or Service Discontinuance Where Contractor is the Product Manufacturer/Developer, and Contractor publicly announces to all U.S. customers ("date of notice") that a Product is being withdrawn from the U.S. market or that maintenance service or technical support provided by Contractor ("withdrawn support") is no longer going to be offered, Contractor shall be required to: (i) notify the Commissioner, each Licensee and each Authorized User then under contract for maintenance or technical support in writing of the intended discontinuance; and (ii) continue to offer Product or withdrawn support upon the Contract terms previously offered for the greater of: a) the best terms offered by Contractor to any other customer, or b) not less than twelve (12) months from the date of notice; and (iii) at Authorized User's option, provided that the Authorized User is under contract for maintenance on the date of notice, either: provide the Authorized User with a Product replacement or migration path with at least equivalent functionality at no additional charge to enable Authorized User to continue use and maintenance of the Product.

In the event that the Contractor is not the Product Manufacturer, Contractor shall be required to: (i) provide the notice required under the paragraph above, to the entities described within five (5) business days of Contractor receiving notice from the Product Manufacturer, and (ii) include in such notice the period of time from the date of notice that the Product Manufacturer will continue to provide Product or withdraw support.

The provisions of this subdivision (a) shall not apply or eliminate Contractor's obligations where withdrawn support is being provided by an independent Subcontractor. In the event that such Subcontractor ceases to provide service, Contractor shall be responsible for subcontracting such service, subject to State approval, to an alternate Subcontractor.

b. Product or Service Re-Bundling In the event that Contractor is the Product manufacturer and publicly announces to all U.S. customers ("date of notice") that a Product or maintenance or technical support offering is being re-bundled in a different manner from the structure or licensing model of the prior U.S. commercial offering, Contractor shall be required to: (i) notify the State and each Authorized User in writing of the intended change; (ii) continue to provide Product or withdrawn support upon the same terms and conditions as previously offered on the then-current NYS Contract for the greater of: a) the best terms offered by Contractor to any other customer, or b) not less than twelve (12) months from the date of notice; and (iii) shall submit the proposed rebundling change to the Commissioner for approval prior to its becoming effective for the remainder of the Contract term. The provisions of this section do not apply if the Contractor is not the Product manufacturer.

72. NO HARDSTOP/PASSIVE LICENSE MONITORING Unless an Authorized User is otherwise specifically advised to the contrary in writing at the time of order and prior to purchase, Contractor hereby warrants and represents that the Product and all Upgrades do not and will not contain any computer code that would disable the Product or Upgrades or impair in any way its operation based on the elapsing of a period of time, exceeding an authorized number of copies, advancement to a particular date or other numeral, or other similar self-destruct mechanisms (sometimes referred to as "time bombs," "time locks," or "drop dead" devices) or that would permit Contractor to access the Product to cause such disablement or impairment (sometimes referred to as a "trap door" device). Contractor agrees that in the event of a breach or alleged breach of this provision that Authorized User shall not have an adequate remedy at law, including monetary damages, and that Authorized User shall consequently be entitled to seek a temporary restraining order, injunction, or other form of equitable relief against the continuance of such breach, in addition to any and all remedies to which Authorized User shall be entitled.

73. SOURCE CODE ESCROW FOR LICENSED PRODUCT If Source Code or Source Code escrow is offered by either Contractor or Product manufacturer or developer to any other commercial customers, Contractor shall either: (i) provide Licensee with the Source Code for the Product; or (ii) place the Source Code in a third party escrow arrangement with a designated escrow agent who shall be named and identified to the State, and who shall be directed to release the deposited Source Code in accordance with a standard escrow agreement acceptable to the State; or (iii) will certify to the State that the Product manufacturer/developer has named the State, acting by and through the Authorized User, and the Licensee, as a named beneficiary of an established escrow arrangement with its designated escrow agent who shall be named and identified to the State and Licensee, and who shall be directed to release the deposited Source Code in accordance with the terms of escrow. Source Code, as well as any corrections or enhancements to such source code, shall be updated for each new release of the Product in the same manner as provided above and such

updating of escrow shall be certified to the State in writing. Contractor shall identify the escrow agent upon commencement of the Contract term and shall certify annually that the escrow remains in effect in compliance with the terms of this clause.

The State may release the Source Code to Licensees under this Contract who have licensed Product or obtained services, who may use such copy of the Source Code to maintain the Product.

INDEX

	Clause No.
A	
Advertising Results	13
Assignment	43
Assignment of Claim	53
Audit of Licensed Product Usage	67
B	
Bid Contents	7
Bid Evaluation	22
Bid Opening	4
Bid Submission	5
C	
Changes to Product or Service Offerings	71
Confidential/Trade Secret Materials	9
Contract Invoicing	49
Contract Creation/Execution	26
Contract Term - Renewal	58
Cooperation with Third Parties	57
D	
Default - Authorized User	50
Definitions	2
Disputes	64
Drawings	18
E	
Emergency Contracts	31
Employees/Subcontractors/Agents	42
Estimated/Specific Quantity Contracts	30
Ethics Compliance	1
Expenses Prior to Contract Execution	12
Extraneous Terms	8
I	
Indemnification	61
Indemnification Relating to Third Party Rights	62
Independent Contractor	55
Installation	40
International Bidding	3
L	
Late Bids Rejected	6
Legal Compliance	60
Limitation of Liability	63
M	
Modification of Contract Terms	28
N	
No Hardstop/Passive License Monitoring	72
O	
Ownership/Title to Project Deliverables	68

	Clause No.
P	
Participation in Centralized Contracts	27
Performance/Bid Bond	45
Prevailing Wage Rates - Public Works and Building Services Contracts	10
Pricing	17
Procurement Card	20
Product Acceptance	66
Product Delivery	33
Product References	14
Product Substitution	38
Product Version	70
Products Manufactured in Public Institutions	16
Prompt Payments	51
Proof of License	69
Purchase Orders	32
Q	
Quantity Changes Prior to Award	24
R	
Rejected Product	39
Re-Weighing Product	37
Remanufactured, Recycled, Recyclable or Recovered Materials	15
Remedies for Breach	52
Repaired or Replaced Product/Components	41
S	
Samples	21
Savings/Force Majeure	48
Scope Changes	29
Security	56
Site Inspection	19
Shipping/Receipt of Product	35
Software License Grant	65
Source Code Escrow for Licensed Product	73
Subcontractors and Suppliers	44
Suspension of Work	46
T	
Taxes	11
Termination	47
Tie Bids	23
Timeframe for Offers	25
Title and Risk of Loss	36
Toxic Substances	54
W	
Warranties	59
Weekend and Holiday Deliveries	34

APPENDIX C

Pricing Schedule

I. LOT I

For the first two years from contract execution:

Perfect Commerce Product in Scope	Includes	Fixed Price
PerfectShop OSN Procurement Manager	• Implementation • SaaS Product PerfectShop usage/subscription with maintenance and support included • Lot I Deliverables #1-8 (as identified in Section 4 of the base Contract) • Services – Train the Trainer • Travel (as described and subsequently agreed in the preliminary implementation plan) • Included Functions: Requisition Management, Workflow Management, eInvoicing, Catalog Management, Integration Platform, Standard Reporting, Advanced Reporting, Enterprise Administration, Online Help/Training Documentation, Punchout/Roundtrip Catalogs, Supplier Enablement and Content Services	$1,284,000

Beginning the first day after 2 years from contract execution:

Perfect Commerce Product in Scope	Includes	Price Per Year
PerfectShop OSN ProcurementManager	• Integration – maintenance • SaaS Product PerfectShop usage/subscription with maintenance and support included • Services – Train the Trainer • Travel (as described and subsequently agreed in the preliminary implementation plan) • Included Functions: Requisition Management, Workflow Management, eInvoicing, Catalog Management, Integration Platform, Standard Reporting, Advanced Reporting, Enterprise Administration, Online Help/Training Documentation, Punchout/Roundtrip Catalogs, Supplier Enablement and Content Services	$450,000

Additional travel expenses may be requested by the State and are subject to reimbursement, if preapproved by the State.

II. LOT II

LOT II offers eligible participating Authorized Users to purchase components independently from the LOT I purchase.

LOT II Rules of Purchase

1. Implementation, customization, training, and integration work are not included in the prices quoted in LOT II. These professional and development services are available for purchase on an hourly basis using the rates published herein or may be quoted using a fixed fee based on Perfect Commerce's estimates using the rates published herein. In nearly every case, a statement of work based on the hourly rates quoted herein will be required to deliver a usable functional component listed below.
2. There are many functional components that are listed and priced individually below, however, components must be purchased in one of the listed Combinations shown in the Combinations Table.
3. Perfect Commerce offers several products that may satisfy the minimum functional requirements shown in each combination. At the time of purchase, Perfect Commerce will indicate which named products are in scope.
4. Travel is not included in LOT II pricing or in Labor Rates.
5. Suppliers may engage separately with Perfect Commerce for advanced services resulting in fees payable directly from Suppliers to Perfect Commerce.
6. If an Authorized User entity purchases a lower Tier, but usage exceeds the stated limits, Authorized User will immediately be invoiced a catch up invoice for the current service year to date for the difference between the lower Tier price and the higher Tier price and will be invoiced going forward at the higher Tier rate.

Item	Functional Components	Tier I Annual Price	Tier II Annual Price	Tier III Annual Price
1	**Requisition Management**	**$15,000**	**$25,000**	**$30,000**
3	**Workflow Management**	**$4,500**	**$7,500**	**$7,500**
4	**eInvoicing**	**$15,000**	**$18,000**	**$22,000**
5	**Catalog Management**	**$12,000**	**$30,000**	**$42,000**
6	**Integration Platform**	**$4,500**	**$4,500**	**$9,000**
7	**Standard Reporting**	**$3,200**	**$3,200**	**$3,200**
8	**Advanced Reporting**	**$4,800**	**$4,800**	**$4,800**
9	Enterprise Administration	Included	Included	Included
10	Online Help /Training Documentation	Included	Included	Included
11	**Punchout/Roundtrip Catalogs**	**$5,000**	**$10,000**	**$13,000**
12	Supplier Enablement and Content Services	Included	Included	Included
13	**eSourcing (RFx and eAuction)**	**$18,000**	**$26,000**	**$45,000**

14	**Contract Management**	**$15,000**	**$22,000**	**$35,000**
15	**Vendor Management**	**$7,000**	**$7,000**	**$7,000**
16	**Purchase Order Management**	**$17,000**	**$27,000**	**$34,000**
17	**Receipt Management**	**$24,000**	**$30,000**	**$32,500**
TOTAL	**TOTAL PRICE FOR END TO END PROCUREMENT**	**$145,000**	**$215,000**	**$285,000**

LOT II TIERS		
Tier I	**Tier II**	**Tier III**
• Up to 500 Users during a contract year. • Up to 100 Catalogs during a year. • Up to 1 ERP System Integration Point • Up to 100,000 Invoices Annually • Unlimited Supplier Users	• 1000 Users during a contract year. • Up to 1000 Catalogs during a contract year. • Up to 1 ERP System Integration Point • Up to 300,000 Invoices Annually • Unlimited Supplier Users	• 1500 Users during a contract year. • Up to 1500 Catalogs during a contract year. • Up to 2 ERP Systems Integration Points • Up to 900,000 Invoices Annually • Unlimited Supplier Users

Combinations Table	
	Description (**bolded** items correspond with a fee in the table above)

A	End to End Procurement:
	• **eSourcing (RFx and eAuction)** – automated sourcing or bid process.
	• **Contract Management** – Automated Supplier Contracting Process.
	• **Vendor Management** – Automated supplier validation.
	• MarketPlace Catalog – establish an online hosted catalog site of goods and services.
	  • **Catalog Management**
	  • **Punchout/Roundtrip Catalogs**
	  • Supplier Enablement and Content Services
	  • Purchase Requisition – the integration with online vendor catalogs, which includes, but is not limited to approving products, displaying product with attributes and contract terms.
	• **Requisition Management**:
	  • Purchase Requisition – the integration with online vendor catalogs, which includes, but is not limited to approving products, displaying product with attributes and contract terms.
	  • Requisition Approval – Once a purchase requisition is created, it is routed for approval based on the business rules and criteria defined by the Authorized User.
	• **Workflow Management** and Enterprise Administration – The management, creation of user roles, rights and permissions to follow defined business rules.

	• **Purchase Order Management** and Delivery – The creation of Purchase Orders from approved requisitions and transmission of orders from the Authorized Users to the suppliers. • **eInvoicing** – Flipping Purchase Orders into invoices, and/or the delivery of invoices to the Authorized User in an automated goods receipt and reconciliation process. This includes the enablement of two or three way matching between Purchase Orders, invoices and goods receipt documents. • **Receipt Management** – enables goods receipt documents. • **Standard Reporting** – The ability of the solution to generate standard reports providing visibility into the transactions across Authorized Users and suppliers. • **Advanced Reporting** – The ability of the solution to generate customized queries and reports providing visibility into the transactions across Authorized Users and suppliers. • **Integration Platform** – Integrates to third party systems. • Online Help /Training Documentation

B	Decline One or More of the listed Options:
	• OPTION: **eSourcing (RFx and eAuction)** – automated sourcing or bid process.
	• OPTION: **Contract Management** – Automated Supplier Contracting Process.
	• **Vendor Management**
	• MarketPlace Catalog – establish an online hosted catalog site of goods and services. Includes:
	  • **Catalog Management**
	  • Supplier Enablement and Content Services
	  • Purchase Requisition – the integration with online vendor catalogs, which includes, but is not limited to approving products, displaying product with attributes and contract terms.
	Optional:
	  • **Punchout/Roundtrip Catalogs**
	• **Requisition Management**:
	  • Purchase Requisition – the integration with online vendor catalogs, which includes, but is not limited to approving products, displaying product with attributes and contract terms.
	  • Requisition Approval – Once a purchase requisition is created, it is routed for approval based on the business rules and criteria defined by the Authorized User.
	• **Workflow Management** and Enterprise Administration – The management, creation of user roles, rights and permissions to follow defined business rules.
	• **Purchase Order Management** and Delivery – The creation of Purchase Orders from approved requisitions and transmission of orders from the Authorized Users to the suppliers.
	• OPTION: **eInvoicing** – Flipping Purchase Orders into invoices, and/or the delivery of invoices to the Authorized User in an automated goods receipt and reconciliation process. This includes the enablement of two or three way matching between Purchase Orders, invoices and goods receipt documents.
	• OPTION: **Receipt Management** – enables goods receipt documents.
	• **Standard Reporting** – The ability of the solution to generate standard reports providing visibility into the transactions across Authorized Users and suppliers.

	• OPTION: **Advanced Reporting** – The ability of the solution to generate customized queries and reports providing visibility into the transactions across Authorized Users and suppliers. • OPTION: **Integration Platform** – Integrates to third party systems. • Online Help /Training Documentation

C	COMBINE Any or None of the following Options:
	• OPTION: **eSourcing (RFx and eAuction)** – automated sourcing or bid process.
	• OPTION: **Contract Management** – Automated Supplier Contracting Process.
	• OPTION: **Advanced Reporting** – The ability of the solution to generate customized queries and reports providing visibility into the transactions across Authorized Users and suppliers.
	• OPTION: **Integration Platform** – Integrates to third party systems.
	
	WITH:
	• MarketPlace Catalog – establish an online hosted catalog site of goods and services. Includes:
	  • **Catalog Management**
	  • Supplier Enablement and Content Services
	  • Purchase Requisition – the integration with online vendor catalogs, which includes, but is not limited to approving products, displaying product with attributes and contract terms.
	  Optional:
	  • **Punchout/Roundtrip Catalogs**
	
	• **Requisition Management**:
	  • Purchase Requisition – the integration with online vendor catalogs, which includes, but is not limited to approving products, displaying product with attributes and contract terms.
	  • Requisition Approval – Once a purchase requisition is created, it is routed for approval based on the business rules and criteria defined by the Authorized User.
	And/Or:
	• **Purchase Order Management** and Delivery – The creation of Purchase Orders from approved requisitions and transmission of orders from the Authorized Users to the suppliers.
	  • OPTIONAL: **Receipt Management** – enables goods receipt documents.
	  • OPTIONAL: **eInvoicing** – Flipping Purchase Orders into invoices, and/or the delivery of invoices to the Authorized User in an automated goods receipt and reconciliation process. This includes the enablement of two or three way matching between Purchase Orders, invoices and goods receipt documents.
	
	AND WITH:
	• **Workflow Management** and Enterprise Administration – The management, creation of user roles, rights and permissions to follow defined business rules.
	• **Standard Reporting** – The ability of the solution to generate standard reports providing visibility into the transactions across Authorized Users and suppliers.

	• **Vendor Management** • Online Help /Training Documentation
D	Choose one or more standalone products from the list below: • **eSourcing (RFx and eAuction)** – automated sourcing or bid process. • **Contract Management** – Automated Supplier Contracting Process. To Combine With: • **Workflow Management** and Enterprise Administration – The management, creation of user roles, rights and permissions to follow defined business rules. • **Standard Reporting** – The ability of the solution to generate standard reports providing visibility into the transactions across Authorized Users and suppliers. • **Vendor Management** • Online Help /Training Documentation
E	Any other combinations may be feasible but are subject to an individual price quote at Perfect Commerce's discretion.

III. Additional Services Menu

Rules for Labor Rates

1. These Labor Rates do not include travel.
2. The Special NY Rate applies only for work done or committed in a Statement of Work signed within one year of execution of this Contract.

Labor Rates

Item	Role	Standard Rate ($/hr)	Special NY Rate ($/hr)
1	Project Manager	$195	$176
2	Senior Functional Consultant	$195	$176
3	Senior Technical Consultant	$195	$176
4	Senior Implementation Consultant	$195	$176
5	Functional Consultant	$175	$158
6	Technical Consultant	$175	$158
7	Implementation Consultant	$175	$158
8	Junior Technical Consultant	$150	$135
9	Integration Specialist	$195	$176
10	Quality Assurance/Test Specialist	$165	$149
11	Junior QA/Test Specialist	$150	$135
12	Supplier Enablement Specialist	$165	$149
13	Catalog Content Cleansing Specialist	$165	$149
14	Training Specialist	$150	$135
15	User Documentation Specialist	$150	$135

APPENDIX D

SERVICE LEVEL AGREEMENT

DEFINITIONS

Unless otherwise defined in this Service Level Agreement ("SLA"), capitalized terms used herein shall have the meanings assigned to such terms in Section 1 of the Agreement. The following definitions shall be used for purposes of this SLA:

Managed Environment Availability. The total number of minutes in a period, less any Planned Downtime or downtime due to Force Majeure.

Planned Downtime. Scheduled unavailability of the Managed Environment, including but not limited to, the performance of system upgrades, enhancements and routine maintenance activities. Contractor will provide a schedule for recurring Planned Downtime (e.g. weekly system maintenance) and give the State not less than twenty-four (24) hours written notice of non-recurring Planned Downtime.

Unscheduled Service Outage. Interruptions to service that result in the unavailability of the Managed Environment to the State, not including Planned Downtime or interruptions due to Force Majeure.

MANAGED ENVIRONMENT

Contractor will use commercially reasonable efforts to provide a managed environment ("Managed Environment") that will include the hardware and software necessary to support the Managed Environment Availability service levels specified below. The Managed Environment is restricted to the production systems environment and the application(s) located at Contractor's hosting site. The Managed Environment specifically does not include: (i) development, staging or test environments, (ii) any elements of the Internet, (iii) any part of the State's environment not permanently located at the Contractor hosting site, or (iv) application components outside the Contractor site firewall. The Managed Environment shall only include hardware, software and equipment owned by Contractor. For purposes of this SLA, the Managed Environment will support the following software applications (or any successor or replacement software applications made available by Contractor):

Lot I

Lot II

MANAGED ENVIRONMENT AVAILABILITY

Contractor actively monitors the availability of the Managed Environment and will accumulate the number of downtime minutes during an Unscheduled Service Outage. Planned Downtime shall be necessary on a regular basis or in some emergencies to perform corrective maintenance.

Minimum Quarterly Managed Environment Availability During Peak Operating Times	State Service Credits
99.7%	$1,000 per minute below the Minimum Quarterly Managed Environment Availability During Peak Operating Times

"Peak Operating Times" means 7 am-6 pm Eastern Standard Time Monday through Friday.

The following metric shall be used to calculate the Quarterly Managed Environment Availability During Peak Operating Times percentage for each full month that this SLA is in effect:

(Managed Environment Availability – Unscheduled Service Outage) ÷ Managed Environment Availability

Minimum Monthly Managed Environment Availability	State Service Credits
98%	<98% ≥ 95% = 12.5% of the Monthly Fee <95% ≥ 90% = 25% of the Monthly Fee <90% = 50% of the Monthly Fee

The following metric shall be used to calculate the Monthly Managed Environment Availability percentage for each full month that this SLA is in effect:

(Managed Environment Availability – Unscheduled Service Outage) ÷ Managed Environment Availability

SERVICE CREDITS

In the event Contractor fails to meet any of the service levels herein, and such failure causes the Managed Environment Availability to fall below the applicable percentage set forth above, Contractor will credit the State as set forth above in accordance with the applicable percentage achieved. Credits will be computed and applied automatically and will be credited towards the next invoice following such failure to meet the applicable service level. This SLA states Contractor's sole and exclusive warranties. "Monthly Fee" shall mean: (i) the actual monthly fee paid by the State that corresponds to the software application whose Minimum Monthly Managed Environment Availability goal was not achieved, or (ii) in the event the State pays on an annual basis, an amount that is 1/12th of the annual fee paid by the State in the applicable year that corresponds to the software application whose Minimum Monthly Managed Environment Availability goal was not achieved. For Lot I, the annual fee shall be $450,000 per year for this purpose for years 1 and 2. No Service Credits will be given for events resulting from conduct of the State or its representatives, including (i) negligence of the State or its representatives, (ii) a failure or malfunction resulting from scripts, applications, equipment, or services provided by the State, or (iii) outages initiated by Contractor at the request or direction of the State for maintenance, back up, or other purposes.

SERVICE CREDIT RETURN

Service Credits awarded to the State for service during the last quarter can be earned back by Contractor during the subsequent three Quarters at a rate of $1,000 per minute of availability in excess of the Minimum Quarterly Managed Environment Availability During Peak Operating Times during a quarter. If the State experiences any Priority 1 or Priority 2 issues during a quarter during the period in which Service Credits are earned back by Contractor, the State may withhold the award of such Service Credits at its discretion for such quarter.

UNSCHEDULED SERVICE OUTAGE NOTIFICATION

Contractor shall use commercially reasonable efforts to provide the State with: (i) the apparent cause of an Unscheduled Service Outage, (ii) Contractor's response time to such Unscheduled Service Outage, and (iii) repair time information, following the resolution of an Unscheduled Service Outage that results in a service level falling below the level set forth herein. Please note that in the event of an Unscheduled Service Outage, Contractor's first priority shall be to re-establish service and restore the Managed Environment to full availability. Contractor has designed and implemented various methods for detecting outages as well as potential problems that might occur in the Managed Environment. The detection software is configured to notify support immediately. Contractor shall notify the State's designated contact(s) within sixty minutes of any Unscheduled Service Outage by email or by posting on Contractor's service desk and promptly again by email upon resolution.

PROBLEM MANAGEMENT AND SECURITY

Contractor's problem management and escalation process can be found on our website at www.perfect.com or sent via email upon request. A current version of this document is appended below, this document may be modified by Contractor by providing written notice to the State, provided that it continues to satisfy the written requirements from the RFP. All transactions between Contractor and the State that are the subject matter of this SLA will take place with 128 bit SSL encryption or using digital certificates, whichever is applicable. Both Contractor and the State will implement commercially reasonable levels of security protection against possible Internet aggression or corruption and upgrade such security protection against new threats when they are identified. Each Party has the responsibility of the physical security of their respective production platform. Contractor and the State must create a secure connection to allow data exchange and automatic integration between them, which is accessed by pulling/pushing asynchronous messages from/to Contractor or the State through the HTTPS protocol.

Customer Support Overview

Hours of Operation

First level of Customer Support is available as specified below:

America	EMEA	Asia / Pacific
Monday - Friday 8am - 8pm EST	Monday - Friday 9am - 6pm CET	Monday - Friday 9am - 5pm SGT
Note: After-hour and week-end support available for Emergency issues only		

Team Organization:

US Eastern Time	
Day Schedule	
US Team	8am to 6pm

US Team (Asia / Pacific Support)	6pm to 3am
Europe Team	3am to 12pm
Week Schedule	
From Sunday 6pm to Friday 8pm	

Contact Options

	America & Asia / Pacific	EMEA
Email	CustomerSupport@perfect.com	supporteurope@perfect.com
Phone	866-889-8533 (US only) 001-713-589-2462 (International)	33 (0) 170 169 026
help desk	http://support.perfect.com/en	http://support.perfect.com/en http://support.perfect.com/fr

Toll-free numbers are not accessible outside the U.S. International offices and suppliers must use direct dial numbers.

Email support has a maximum turnaround of 4 business hours. For this reason, we encourage any critical or high priority issues to be called in.

Required Information

For every call, email, or ticket received, an agent is required to establish the following detail:

- Customer Name
- User Name
- Role (Buyer/Supplier/Admin)
- Product (e.g. PerfectProcure)
- Impacted application and Status
- Problem Description or steps to recreate
- Exact Error Message or Repeated Behavior
- Timeframe in which error or behavior began appearing
- Browser version and Internet Connectivity (for performance problems and/or errors which cannot be recreated in-house)

In return the client can expect a case number and priority assigned to the issue, so they may establish expected response times as posted below.

Escalation Procedures

Issues that cannot be resolved within the Customer Support department are escalated to Application Support – a group of technicians who work with both Operations and Engineering to resolve the problem. If the issue appears to be a code-related bug, it will be recreated and then delivered to the QA team for investigation and write up.

Target response times for each priority level are available at the end of this document. These are not resolution times, but expected windows for our organization to provide updates to yours. Once an issue has been assigned a bug number the target response times will no longer apply. The bug will become part of the development cycle and scheduled into a maintenance or full feature release based on priority, development hours required, and overall impact on clients' business processes.

Problem MANAGEMENT

The following tables provide details describing each of the available Priority Levels:

Priority	Descriptions, Examples, Notes	Required Information

Priority 1 **'Urgent'**	· Application is unavailable. · No Workarounds exist. · Revenue stream interrupted (Business is down).	· Description of the Problem (*Actual vs. Expected Results*). · Actions/Steps to reproduce the Problem. · Sample/Supporting Data that illustrates the Problem (*Site URL's, Customer id's, Order #'s, SKU #'s, User id's, etc.*). · Documented Business Impacts. · Root Cause of the Problem.
Priority 2 **'High'**	· Application is not achieving its primary goal. · Workarounds exist – though business is still heavily impacted. · Impending Failure or Downtime of an Application.	· Description of the Problem (*Actual vs. Expected Results*). · Actions/Steps to reproduce the Problem. · Sample/Supporting Data that illustrates the Problem (*Site URL's, Customer id's, Order #'s, SKU #'s, User id's, etc.*). · Documented Business Impacts. · Root Cause of the Problem.
Priority 3 **'Medium'**	· Application is not achieving its primary goal. · Functionality does not appear to be working as expected. · Acceptable Workarounds do exist. · Enhancements that are now Work-In-Progress.	· Description of the Problem (*Actual vs. Expected Results*). · Actions/Steps to reproduce the Problem. · Root Cause of the Problem. · Sample/Supporting Data that illustrates the Problem (*Site URL's, Customer id's, Order #'s, SKU #'s, User id's, etc.*).
Priority 4 **'Low'**	· Default Value for New Requests · Application is not achieving its primary goal. · Functionality does not appear to be working as expected. · Acceptable Workarounds do exist and/or the business is not noticeably impacted. · The application is due for retirement in the short-term. · Repair costs are much greater than the Value-Add of the Repair. · New Enhancement Requests.	· Description of the Problem (*Actual vs. Expected Results*). · Actions/Steps to reproduce the Problem. · Sample/Supporting Data that illustrates the Problem (*Site URL's, Customer id's, Order #'s, SKU #'s, User id's, etc.*). · Root Cause of the Problem. · Enhancements and Changes also require Specifications and other Documentation before Work can Begin.

	Target Response Times			
Activity	**Priority 1**	**Priority 2**	**Priority 3**	**Priority 4**
1. Acknowledge / Respond to Requests.	1 hr	2 hr	1 business day	2 business days
2. Analyze requests and take ownership or re-route. (After the initial Acknowledge / Respond to Request time.)	1 hr	4 hrs	1 business day	5 business days
3. Frequency for communicating status updates to end users for individual Support Requests.	2 hrs	Daily	As communicated	Monthly or weekly

4. Maximum Elapsed Duration to Resolve User Requests (for visibility of issues)	Every 2 hours or as stated in initial response	Daily or as stated in initial response	Days or Weeks	Days, Weeks or Months

All response times begin upon notification of a problem through Customer's use of Perfect's Service Desk, provided Perfect reserves the right to classify each problem into the appropriate priority category listed above. Perfect shall use commercially reasonable efforts to provide an initial response, including a proposed action plan, within the response times above. Perfect does not guarantee a "fix" within the response times set forth herein. If Customer is unavailable for consultation, Perfect will not be liable for adhering to these response times. All work requested by Customer shall be performed pursuant to Perfect's regularly scheduled production rolls as published by Perfect from time to time.

Levels of Support

Level 1

Buyers & Suppliers Level 1 Support (Main scope of Services)	
Application Support	
Login failed	Unable to login
Inactive User	Usually due to multiple log-in failure
Inactive Organization	Coordination – Owners/Buyers required to re-activate supplier Customer account
Resetting Passwords	Passwords reset while the supplier is on the phone
Document Load error	Application Support will examine the error and will provide technical resolution
Timed Out Sessions	Clearing Cache or Compatibility Mode procedure
Services/Training Assistance	
Buyers	Event setup questions/training Adding suppliers Editing sections Changing open close dates & times Reactivating suppliers
Suppliers	Supplier Registration Assistance with entering responses Error in Response (assisting with Event Completion)

Level 2- Technical Account Manager (TAM)

Perfect Commerce is dedicated to excellent customer service with emphasis on owning, addressing and resolving customer issues. Technical Account Managers will have responsibility for providing their assigned customers a single point of contact for all technical issues related to Perfect Commerce software solutions. This may be for escalation activities, or updates to reported issues.

The TAM will have:

- strong customer management skills
- the ability to understand business concepts

- general technical knowledge
- strong problem resolution skills
- ability to communicate clearly (verbal and written).

Level 3 - Perfect Commerce Development Team

Perfect Commerce Development address any issues that cannot be handled by Level 1 or Level 2 and those that may require a code fix to repair the problem. These type of issues are brought to the team by our daily issue reviews or during our hot issues call. Issues are then scheduled by our steering committee and worked according to priority level. As a reminder, all issues raised as a P1 are looked at by development usually bypassing the typical support methods until solved.

Appendix E

Minority and Women-Owned Business Enterprises Equal Employment Opportunity Policy Statement

CONTRACTOR'S EXECUTIVE LAW, ARTICLE 15-A (M/WBE) REQUIREMENTS

MINORITY AND WOMEN-OWNED BUSINESS ENTERPRISES EQUAL EMPLOYMENT OPPORTUNITY POLICY STATEMENT

I, Charles Shannon, the COO (title) of Perfect Commerce, LLC (Contractor) agree that Perfect Commerce, LLC (Contractor) has adopted the following policies with respect to Contract Number PS66640

M/WBE

Contractor will make good faith efforts to achieve the M/WBE contract participations goals set by OGS for that area in which the State-funded project is located, by taking the following steps:

(1) Actively and affirmatively soliciting bids for subcontracts from qualified State certified MBEs or WBEs, including solicitations to MWBE contractor associations.
(2) Request a list of State-certified MWBEs from OGS and solicit bids from them directly.
(3) Ensure that plans, specifications, request for proposals and other documents used to secure bids will be made available in sufficient time for review by prospective M/WBEs.
(4) Where feasible, divide the work into smaller portions to enhanced participations by MWBEs and encourage the formation of joint venture and other partnerships among MWBE contractors to enhance their participation.
(5) Document and maintain records of bid solicitation, including those to MWBEs and the results thereof.
(6) Ensure that progress payments to M/WBEs are made on a timely basis so that undue financial hardship is avoided and provide appropriate support, including waiving bonding and other credit requirements where permissible, to encourage MWBE participation.

Agreed to this 17 day of October,
20 14
By
Print: Charles Shannon
Title: COO

EEO

(a) Contractor will not discriminate against any employee or applicant for employment because of race, creed, color, national origin, sex, age, disability or marital status, will undertake or continue existing programs of affirmative action to ensure that minority group members are afforded equal employment opportunities without discrimination, and shall make and document its conscientious and active efforts to employ and utilize minority group members and women in its work force on state contracts.
(b) Contractor shall state in all solicitation or advertisements for employees that in the performance of the State contract all qualified applicants will be afforded equal employment opportunities without discrimination because of race, creed, color, national origin, sex disability or marital status.
(c) At the request of the contracting agency, Contractor shall request each employment agency, labor union, or authorized representative will not discriminate on the basis of race, creed, color, national origin, sex, age, disability or marital status and that such union or representative will affirmatively cooperate in the implementation of Contractor's obligations herein.
(d) Contractor shall comply with the provisions of the Human Rights Law, all other State and Federal statutory and constitutional non-discrimination provisions. Contractor and subcontractors shall not discriminate against any employee or applicant for employment because of race, creed (religion), color, sex, national origin, sexual orientation, military status, age, disability, predisposing genetic characteristic, marital status or domestic violence victim status, and shall also follow the requirements of the Human Rights Law with regard to non-discrimination on the basis of prior criminal conviction and prior arrest.
(e) Contractor will include the provisions of sections (a) through (d) of this agreement in every subcontract in such a manner that the requirements of the subdivisions will be binding upon each subcontractor as to work in connection with the State contract.

APPENDIX F

Insurance Requirements

Upon tentative award, Bidder shall be required to procure, at its sole cost and expense, all required insurance. The Contractor shall procure at its sole cost and expense, and shall maintain in force at all times during the term of this Contract, policies of insurance as herein below set forth, written by companies licensed or authorized by the New York State Department of Financial Services to issue insurance in the State of New York with an A.M. Best Company rating of "A-" Class "VII" or better. If, during the term of the policy, a carrier's rating falls below "A-" Class "VII", the insurance must be replaced no later than the renewal date of the policy with an insurer acceptable to the New York State Office of General Services ("OGS") and rated at least "A-" Class "VII" or better in the most recently published Best's Insurance Report.

The Contractor shall deliver to OGS evidence of such policies in a form acceptable to OGS. These policies must be written in accordance with the requirements of the paragraphs below, as applicable. Acceptance and/or approval by OGS does not and shall not be construed to relieve Contractor of any obligations, responsibilities or liabilities under the Contract.

General Conditions

A. Conditions Applicable to Insurance. All policies of insurance required by this Contract must meet the following requirements:

1. ***Coverage Types and Policy Limits.*** The types of coverage and policy limits required from the Contractor are specified in Paragraph B *Insurance Requirements* below.

2. ***Policy Forms.*** Except as may be otherwise specifically provided herein or agreed to in writing by OGS, policies must be written on an occurrence basis.

3. ***Certificates of Insurance/Notices***. Contractor shall provide a Certificate or Certificates of Insurance, in a form satisfactory to OGS, upon tentative award, and thereafter within three (3) business days of request. Certificates shall reference the Contract Number. As applicable, the requested forms must name the New York State Office of General Services, New York State Procurement, 38th Floor, Corning Tower, Albany, New York 12242 as the entity requesting proof of coverage (the entity being listed as the Certificate Holder). Certificates shall be submitted to the Office of General Services, New York State Procurement, Corning Tower- 38th Floor, Empire State Plaza, Albany, NY 12242.

Unless otherwise agreed, policies shall be written so as to include a provision that the policy will not be canceled, materially changed, or not renewed without at least thirty (30) days prior written notice except in cases of cancellation for non-payment, in the event of which notice shall be provided as required by law to OGS. The Contractor shall not take any action, or omit to take any action that would suspend or invalidate any of the required coverages during the period of time such coverages are required to be in effect. Not less than thirty (30) days prior to the expiration date or renewal date, the Contractor shall supply OGS updated replacement Certificates of Insurance, and amendatory endorsements.

Certificates of Insurance shall:

- Be in the form approved by OGS;

- Disclose any deductible, self-insured retention, aggregate limit or any exclusion to the policy that materially changes the coverage required by the Contract;
- Be accompanied by an Additional Insured and a Waiver of Subrogation Endorsement as required herein;
- Refer to this Contract by number and any other attachments on the face of the certificate; and
- Be signed by an authorized representative of the insurance carrier or producer.

Only original documents (Certificates of Insurance and other attachments) will be accepted.

4. ***Primary Coverage.*** All insurance policies shall provide that the required coverage shall apply on a primary and not on an excess or contributing basis as to any other insurance that may be available to OGS or any Authorized User for any claim arising from the Contractor's work under this Contract, or as a result of the Contractor's activities. Any other insurance maintained by OGS or any Authorized User shall be excess of and shall not contribute with the Contractor's insurance.

5. ***Policy Renewal/Expiration.*** At least thirty (30) days prior to the expiration of any policy required by this Contract, evidence of renewal or replacement policies of insurance with terms no less favorable to OGS than the expiring policies shall be delivered to OGS in the manner required for service of notice in Paragraph A.3., *Certificates of Insurance/Notices,* above. If, at any time during the term of this Contract, the coverage provisions and limits of the policies required herein do not meet the provisions and limits set forth in the Contract or proof thereof is not provided to OGS, the Contractor shall immediately cease work. The Contractor shall not resume work until authorized to do so by OGS. Any delay, time lost, or additional cost incurred as a result of the Contractor not having insurance required by the Contract or not providing proof of the same in a form acceptable to OGS, shall not give rise to a delay claim or any other claim against OGS. Should the Contractor fail to provide or maintain any insurance required by this Contract, or proof thereof is not provided, OGS or the Authorized Users may withhold further contract payments, treat such failure as a breach or default of the contract.

6. ***Self-Insured Retention/Deductibles***. Certificates of Insurance must indicate the applicable deductible/self insured retention on each policy. Deductibles or self-insured retentions above $100,000 are subject to approval from OGS, which shall not be unreasonably withheld or delayed. The Contractor shall be solely responsible for all claim expenses and loss payments within the deductible or self-insured retention.

7. ***Subcontractors.*** Should the Contractor engage a Subcontractor, the Contractor shall require all Subcontractors, prior to commencement of an agreement between Contractor and the Subcontractor, to secure and keep in force during the term of this Contract the insurance requirements of this document on the Subcontractor, as applicable. Proof thereof shall be supplied to OGS.

As applicable, insurance required by the Contract shall name The People of the State of New York, its officers, agents, and employees as additional insureds hereunder (General Liability Additional Insured Endorsement shall be on Insurance Service Office's (ISO) form number CG 20 26 11 85 or the equivalent). Specifically, the additional insured requirement does not apply to Workers Compensation, Disability or Professional Liability coverage.

APPENDIX F

B. Insurance Requirements

The Contractor, throughout the term of this Contract, or as otherwise required by this Contract, shall obtain and maintain in full force and effect, the following insurance with limits not less than those described below and as required by the terms of this Contract, or as required by law, whichever is greater (limits may be provided through a combination of primary and umbrella/excess policies):

a) **Commercial General Liability Insurance** with a limit of not less than $2,000,000 each occurrence. Such liability shall be written on the ISO occurrence form CG 00 01 01 96, or a substitute form providing equivalent coverages and shall cover liability arising from premises operations, independent contractors, products-completed operations, broad form property damage, personal & advertising injury, cross liability coverage, liability assumed in a contract (including the tort liability of another assumed in a contract) and explosion, collapse & underground coverage.

1. Policy shall include bodily injury, property damage and broad form contractual liability coverage.
   - General Aggregate $2,000,000
   - Products – Completed Operations Aggregate $2,000,000
   - Personal and Advertising Injury $1,000,000
   - Each Occurrence $2,000,000

Coverage shall include, but not be limited to, the following:

- Premises liability;
- Independent contractors;
- Blanket contractual liability, including tort liability of another assumed in a contract;
- Defense and/or indemnification obligations, including obligations assumed under this contract;
- Cross liability for additional insureds;
- Products/completed operations for a term of no less than three (3) years, commencing upon acceptance of the work, as required by the contract;
- Explosion, collapse and underground hazards; and
- Contractor means and methods.

The following ISO forms must be endorsed to the policy:

a. CG 00 01 01 96 or an equivalent Commercial General Liability Coverage Form;
b. CG 20 10 11 85 or an equivalent- Additional Insured-Owner, Lessees or Contractors (Form B); and
c. Waiver of Subrogation Endorsement.

Limits may be provided through a combination of primary and umbrella/excess liability policies.

b) **Comprehensive Business Automobile Liability Insurance** with a limit of not less than $2,000,000.00 each accident. Such insurance shall cover liability arising out of any automobile including owned, leased, hired and non-owned automobiles.

Waiver of Subrogation. Contractor shall cause to be include in each of the above referenced policies insuring against loss, damage or destruction by fire or other insured casualty a waiver of the insurer's right of subrogation against OGS, or, if such waiver is unobtainable (i) an express agreement that such policy shall not be invalidated if Contractor waives or has waived before the casualty, the right of recovery against OGS or (ii) any other form of permission for the release of OGS. A Waiver of Subrogation Endorsement shall be provided upon tentative award, and thereafter, within three (3) days of request.

c) **Professional Liability**: The Contractor shall maintain errors and omissions liability insurance with a limit of not less than $2,000,000 per loss.

1. Such insurance shall apply to professional errors, acts, or omissions arising out of the scope of services covered by this Contract.

2. If coverage is written on a claims-made policy, the Contractor warrants that any applicable retroactive date precedes the start of work; and that continuous coverage will be maintained, or an extended discovery period exercised, throughout the performance of the services and for a period of not less than three years from the time work under this Contract is completed. Written proof of this extended reporting period must be provided to OGS prior to the policy's expiration or cancellation.

3. The policy shall cover professional misconduct or lack of ordinary skill for those positions defined in the Scope of Services of this contract.

Each Claim	$1,000,000
Annual Aggregate	$2,000,000

d) **Technology Errors and Omissions:**

Professional Liability insurance in the amount of $2,000,000.00 for damages arising from computer related services including the following: consulting, data processing, programming, system integration, software development, installation, distribution or maintenance, systems analysis or design, training, staffing or other support services, any electronic equipment, computer hardware or software developed, manufactured, distributed, licensed, marketed or sold.

C. **Workers' Compensation Insurance and Disability Benefits Requirements**
Workers' Compensation Law (WCL) §57 & §220 requires the heads of all municipal and state entities to ensure that businesses applying for permits, licenses or contracts, document that they have appropriate workers' compensation and disability benefits insurance coverage. These requirements apply to both original contracts and renewals, whether the governmental agency is having the work done or is simply issuing the permit, license or contract. Failure to provide proof of such coverage or a legal exemption will result in a rejection of a bid or renewal. **A bidder may not be awarded a contract unless proof of workers' compensation and disability insurance is provided to OGS.**

APPENDIX F

1. **Proof of Compliance with Workers' Compensation Coverage Requirements: An ACORD form (certificate of insurance) is NOT acceptable proof of workers' compensation coverage.** In order to provide proof of compliance with the requirements of the Workers' Compensation Law pertaining to workers' compensation coverage, a contractor shall:
   A) Be legally exempt from obtaining Workers' Compensation insurance coverage; or
   B) Obtain such coverage from an insurance carrier; or
   C) Be a Workers' Compensation Board-approved self-insured employer or participate in an authorized self-insurance plan.

   A Contractor seeking to enter into a contract with the State of New York shall provide one of the following forms to OGS at the time of bid submission or within three (3) days of request:
   A) Form CE-200, Certificate of Attestation for New York Entities With No Employees and Certain Out of State Entities, That New York State Workers' Compensation and/or Disability Benefits Insurance Coverage is Not Required, which is available on the Workers' Compensation Board's website (www.wcb.state.ny.us); (Reference applicable RFP and Group #s on the form.);
   B) Certificate of Workers' Compensation Insurance:
      1) Form C-105.2 (9/07) if coverage is provided by the Contractor's insurance carrier, Contractor must request its carrier to send this form to OGS, or
      2) Form U-26.3 if coverage is provided by the State Insurance Fund, contractor must request that the State Insurance Fund send this form to OGS;
   C) Form SI-12, Certificate of Workers' Compensation Self-Insurance available from the New York State Workers' Compensation Board's Self-Insurance Office; or
   D) Form GSI-105.2, Certificate of Participation in Workers' Compensation Group Self-Insurance available from the contractor's Group Self-Insurance Administrator.

2. **Proof of Compliance with Disability Benefits Coverage Requirements:** In order to provide proof of compliance with the requirements of the Workers' Compensation Law pertaining to disability benefits, a contractor shall:
   A) Be legally exempt from obtaining disability benefits coverage; or
   B) Obtain such coverage from an insurance carrier; or
   C) Be a Board-approved self-insured employer.

   A Contractor seeking to enter into a contract with the State of New York shall provide one of the following forms to OGS at the time of bid submission or within three (3) days of request:
   A) Form CE-200, Certificate of Attestation for New York Entities With No Employees and Certain Out of State Entities, That New York State Workers' Compensation and/or Disability Benefits Insurance Coverage is Not Required, which is available on the Workers' Compensation Board's website

(www.wcb.state.ny.us); (Reference applicable RFP and Group #s on the form.);

B) Form DB-120.1, Certificate of Disability Benefits Insurance. Contractor must request its business insurance carrier to send this form to OGS; or

C) Form DB-155, Certificate of Disability Benefits Self-Insurance. The Contractor must call the Board's Self-Insurance Office at 518-402-0247 to obtain this form.

Proof of coverage or an exemption shall be submitted to the Office of General Services, New York State Procurement, Corning Tower- 38th Floor, Empire State Plaza, Albany, NY 12242.

Appendix G

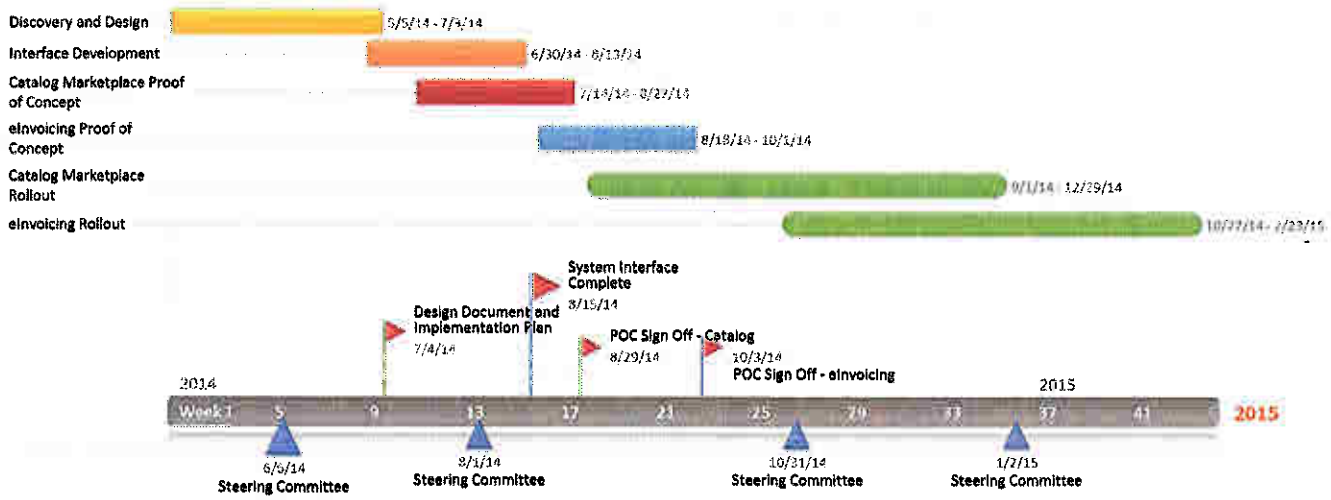
1 Implementation Plan

1.1 Purpose

This Implementation Plan is intended to be a living document and serves as an initial outline of the Implementation Plan. Details will be added or modified as necessary to accomplish overall project objectives.

1.2 Illustrative Project Schedule

Perfect is proposing a two-year phased implementation, where the MarketPlace Catalog and eInvoicing solutions will be deployed 10 months after project initiation. The overall project schedule is shown below, while the detailed steps and activities in Lot I are described in Section 3.1.2.



Note: Dates shown above are illustrative and assumed a start date of May 5, 2014. The actual start date will likely occur in the fourth quarter of calendar year 2014.

Phase 1: Months 1-10

- Project Management Plan
- Communication Plan
- Change Management Plan
- Interface developments with SFS and FileNet, to include testing for the MarketPlace Catalog and eInvoicing
- Onboarding of the State's centralized contract suppliers to the MarketPlace Catalog, as defined by the State
- Enrollment of suppliers into the eInvoicing solution as defined by the State
- Training Plan
- User Acceptance Testing, deployment, and certification of production environment
- Documentation for interfaces and process flow through the solutions
- Go-Live support and ongoing Help desk availability
- Out-of-the-Box reporting
- Parallel Test Environment (as applicable)
- Maintenance of all integration points
- System Documentation
- Risk Management Plan

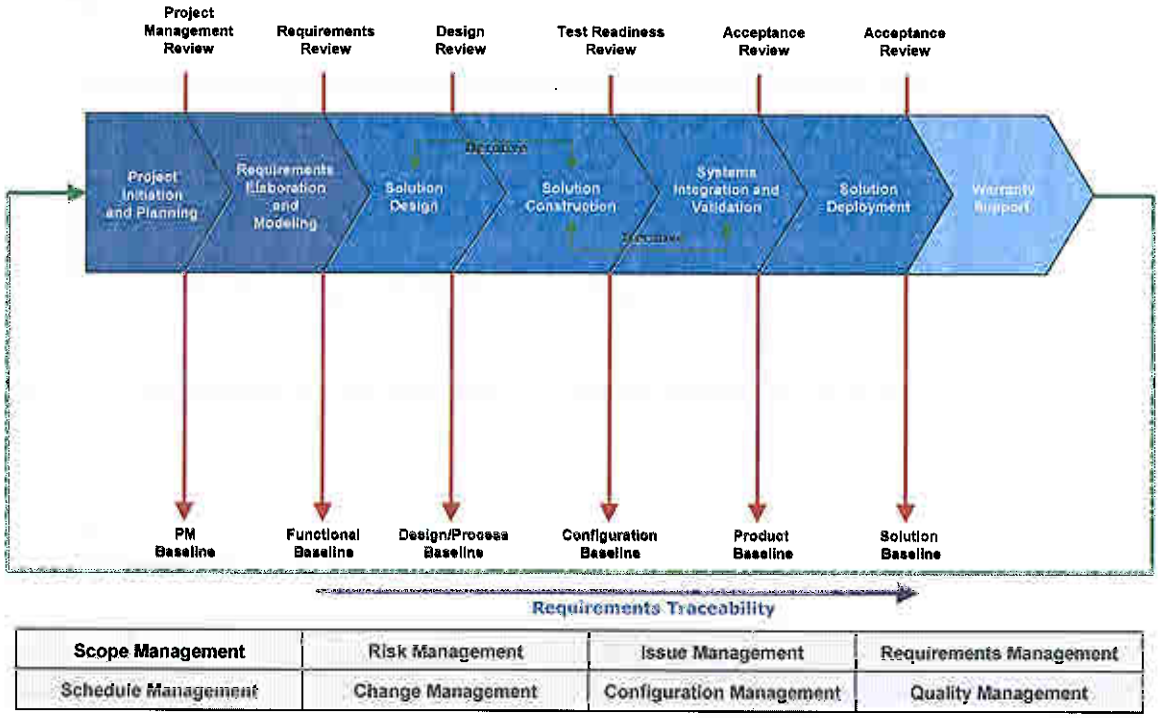
Phase 2: Months 10-24

Appendix G

- Continued support
- Continued onboarding of the State's contracted suppliers to the MarketPlace Catalog
- Continued enrollment of suppliers into the eInvoicing solution, as defined by the State
- Custom reporting
- Vendor performance management

1.2.1 Project Methodology

The Perfect team strongly believes that successful projects result from the appropriate use of project management tools and practices. We have taken our overall project management approach and tailored it to produce a methodology for managing, adapting, and implementing packaged software solutions and the associated operations. This methodology involves a structured framework with tasks, techniques, examples, templates, best practices, and other information to provide consistency and measurability. Our methodology, called the Packaged Solution Implementation (PSI) and depicted below, has been used successfully on a large number of projects. Perfect uses this standard methodology for each system project, but maps against each project's unique needs. For NYS, Perfect would be modify our process to use SOM templates.



Perfect Commerce Methodology - System Integration Lifecycle

The PSI methodology blends the elements of our project management methodology with the components of our standard lifecycle and then adds the other project tasks to encompass the project as a whole. Our field-proven approach is the result of a depth of experience in implementing and integrating complex IT projects. Our standard project and software methodologies, after reviewing the MI PMM document, are synonymous; Perfect is confident that we can manage the project with regard to the requirements laid down in the PMM material.

Each phase of the methodology produces set outcomes or deliverables that NYS can review and approve. By continually keeping NYS involved in the process, we will present no surprises when we implement the eProcurement System.

Each stage of our lifecycle has specific associated activities:

Appendix G

- **Project Initiation.** Perfect and the client define and organize the project.
- **Requirements Analysis (Confirmation).** We closely examine the requirements and determine any necessary modifications or construction options. The team assesses current processes and envisions the way that things "Could-Be" via diagram and white board techniques. The team also designs the "To-Be" future based on these possibilities and develops functional and technical specifications for the modification and configuration of the software package. Perfect recognizes that NYS has done significant work in defining requirements, and mapping out and detailing existing workflows and processes; this provides a solid foundation for understanding your requests and how the system will satisfy your business needs.
- **Solution Design and Configuration.** The team develops the "To-Be" future, tailors and configures the software package, builds the links between new and existing systems, and creates all other add-ons required to implement the business solution. Conversion software is also built. Since Perfect Commerce provides stable, functional, and configurable solutions, traditional "development work" is minimized, allowing the focus to shift to configuration and integration tasks.
- **System Integration Testing.** Testing of the software takes place. This testing will cover functional aspects, integration, performance, and user acceptance.
- **Solution Implementation Rollout.** The client tests the system for acceptance, the live system or modules are rolled out, and any necessary conversion activity is performed.

Perfect will use the PSI methodology to ensure that modifications and system interfaces exceed NYS's requirements and easily meet the proposed schedule. We understand the importance of the provision of the eProcurement system to NYS, and we believe our proposal provides the lowest risk solution by presenting extensive implementation experience and a proven eProcurement application.

1.2.2 Detailed Activities for Lot I

We have developed a preliminary project workplan based on both our understanding of the information provided in the RFP, and our past experience working in similar client environments. Our assumptions will be validated in our initial Discovery and Design phase; however, the durations and work efforts based on our preliminary plan is included in the proposal as requested. The table below summarizes the detailed workplan, indicating the major deliverables, time commitments, and durations of each task required to deliver Lot I, including the MarketPlace Catalog and eInvoicing solutions.

Task	Major Deliverables	From Contract Start	Perfect Mandays	NYS Mandays
Discovery and Design	• Project Management Plan • Communication Plan • Change Management Plan • Interface Design • Implementation Workplan • Training Plan	2 months	45	30
Interface Development	• File layouts • End-to-End system test • System interface	3 months	22	20
Catalog POC	• Loaded catalog • Supplier pilot test • End-to-end user test	4 months	80	75
eInvoice POC	• Invoice interface • Supplier pilot test	5 months	81	75
Catalog Rollout	• Solution Rollout	8 months	57	60
eInvoice Rollout	• Solution Rollout	10 months	54	60

Appendix G

1.3 Risk Management Plan

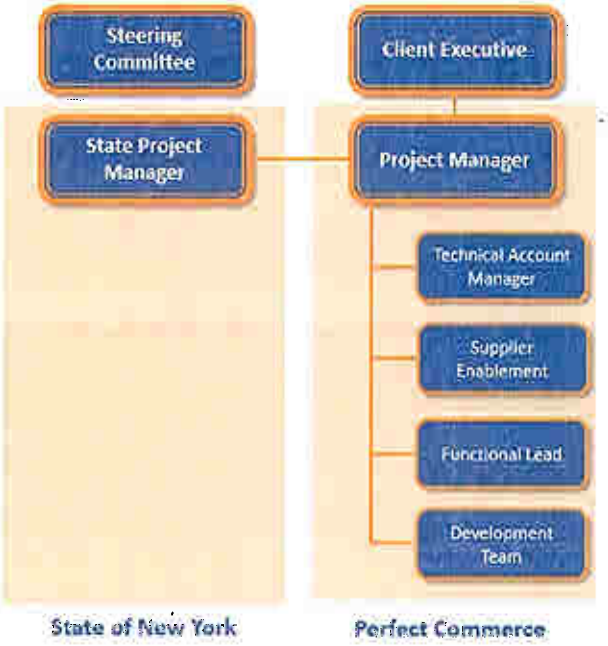
Below are the key project risks identified. A detailed risk register can be completed after the scope & validation phase is completed.

Risks	Impact	Mitigation Strategy	Frequency/ Probability
Change resistance, the ability of NYS personnel to cope with the transition in addition to other concurrent business changes, and the delivery of effective change management.	• Inability to fulfill the project's business objectives or deliver the project benefits. • Delay the implementation.	• Select Perfect's user-friendly system—other companies have experienced relatively low levels of user resistance and change impact during our implementations. • Select Perfect's proven implementation team—we are skilled in the delivery of implementation services and facilitating change. • Continue using the existing FileNet and SFS systems. • Provide for the development of clear processes, procedures, and training material so that user testing and training is clear and simple. • Provide comprehensive communication to all potentially affected users.	Medium
Integration with NYS's ERP systems. Availability of resources for any integration requirements.	• Delay the implementation.	• Address the design and development early in the project planning process. • If possible, reduce dependence on external suppliers by designing any interfaces in a manner that NYS personnel can develop and maintain.	Medium
Training and appropriate usage of the new processes and system.	• Inability to fulfil the project's business objectives or deliver the project benefits. • Delay the implementation.	• Select Perfect's user-friendly system—other companies have experienced relatively low levels of user resistance and change impact during our implementations. • Provide for the development of clear processes, procedures, and training material so that user testing and training is clear and simple. • Provide comprehensive communication to all potentially affected users.	Low

Supplier buy-in or mandate to use system.	• Catalogs not available to users from day one.	• Select Perfect's proven implementation team—we have experience in dealing with all tier suppliers. • Communicate with suppliers in conjunction with NYS informing them of the benefit to both NYS and the supplier.	Medium
Supplier technical capability or lack thereof.	• Inability to fulfill the project's business objective of a fully automated ordering process.	• Selection Perfect's proven implementation team—we can provide tools to assist suppliers regardless of their technical capability	Medium

1.4 Staffing Plan

Perfect's Professional Services Organization, who will be responsible for implementation, is comprised of individuals with significant experience in procurement and sourcing. Each member of this team has worked in the field in similar practitioner roles as those stakeholders we will interact with at NYS, both in the field and at your corporate location. Because our staff brings unique expertise and understanding to this project, our implementation will address specific business challenges the State is facing.



Perfect will take the control and direct responsibility for supplier enablement from NYS, and our Supplier & Content Services Organization will remain engaged with NYS through the life of your contract. This team will introduce unique tools, process, and training to ensure a successful enablement endeavor. Post implementation, your Project Manager and other resources will continue to enable suppliers, and visit onsite to ensure that the quality of your content, the enablement of product features, and the business process in place at NYS are working together to meet the goals of the business.

Account Management

NYS will also have a Client Executive assigned for the duration of your contract who will work with you to ensure success with Perfect's solutions and keep you educated on changes, enhancement, and new initiatives from both Perfect and the market, which may add value to NYS's business. The CE will work closely with NYS, meeting on a frequent schedule, and conducting Quarterly Business Reviews to review our performance and discuss challenges and opportunities which Perfect can help influence within the business.

A Technical Account Manager will be assigned specifically to NYS. This individual will be aware of and personally ensure than any support issues logged by NYS will be resolved, and the TAM will follow all issues through to their resolution.

Appendix G

Implementation Project Management

Perfect's Product Management Organization will meet periodically with NYS to understand product usage within the user community. NYS will have opportunity to share ideas and influence product direction.

We suggest structuring the project team so that it is guided by a strong Steering Committee made up of key NYS stakeholders from key purchasing functions, IT, and operations who act as the project owners.

The Steering Committee members resolve issues, advocate adoption, and work within their respective organizations to seek input and drive change. The key roles filled by Perfect are described in the section above, with more detail in the table below. The Perfect Commerce Project Manager will be NYS's single point of contact for the duration of the contract. The Project Manager will receive all communications and requests during implementation. This point of contact may elect to have other team members work with the State to define solution requirements and coordinate implementation and training activities.

Role	Reports to	Duties
Project Manager	Project Lead for NYS	Single line of communication for NYS. Project definition, communication, execution, and risk mitigation. Project definition, communication, execution, and risk mitigation.
Technical Lead	Project Manager	Perform discovery. Define project scope. Perform demonstrations and act as subject matter expert.
Trainer	Project Manager	Create training plan, materials, and training guides. Coordinate delivery and train administrators and users on use of the solution.
Functional Lead	Project Manager	Setup, configuration, and implementation of the solution.
Business Analyst	Functional Lead	Assisting configuration lead by checking the solution configuration meets the requirements outlined by the Technical Lead in conjunction with NYS's needs.

Appendix G

The table below summarizes the estimated number of mandays that each Perfect Commerce resource will spend on the implementation of Lot I. These mandays represent the total effort for each role, but may be staffed by several individuals. As shown, we estimate devoting a total of 320 mandays on the implementation, staffed by 3-6 different individuals.

Role	Design	Interface	Catalog POC	eInvoice POC	Catalog Rollout	eInvoice Rollout	Total
Project Manager	10	2	20	20	16	15	83
Supplier Enablement Specialist	5	0	25	26	26	24	106
Integration Specialist	10	20	5	5	5	5	50
Implementation Consultant	20	0	30	30	10	10	100
Total	30	20	75	75	60	60	320

In terms of resources from the NYS team, we estimate needed involvement from 5-10 different individuals on the core project team. These core team members will be responsible for gathering requirements and validating functionality with other stakeholders within NYS. As shown, we estimate devoting a total of 320 mandays on the implementation, staffed by 5-10 different individuals over the course of the 10 month project.

Role	Individuals	Average Days/Month	Duration (Months)	Est. Days
Project Manager	1	5-10	10	70
Commodity Specialists	3-4	5-10	8	160
Integration Specialist	1-2	5-10	4	30
AP Specialist	1-2	5-10	6	30
Supplier Specialist	1-3	5-10	6	30
				320

Below are representative staff profiles for the key Perfect Commerce resources on the team.

Michael Ereli: Executive Sponsor & Chief of Customer Care

As the Vice President of Customer Care at Perfect Commerce, Mr. Ereli has all of the groups that will support the State of New York (from implementation through the life of the relationship with Perfect Commerce) reporting to him. This reporting structure allows Mr. Ereli to balance all of Perfect Commerce's resources to ensure customer satisfaction. With over 28 years as an IT professional, Mr. Ereli served as President of Supply Chain Connect, a provider of on-demand, fully configurable supply chain solutions and internet-based negotiation tools with supporting services, before joining Perfect Commerce in the spring of 2012. Mr. Ereli was responsible for building this business under ChemConnect, Inc. as VP of Supply Chain Solutions over the course of seven years before he personally acquired the business in 2007. With over 13 years' experience in large

enterprise change engagements, Mr. Ereli has experienced all aspects of systems development, project management, business process reengineering, and strategic consulting. Mr. Ereli has a Bachelor of Arts degree from Harvard University.

A sample of some of the large scale projects Mr. Ereli has worked on during his career includes:

- Federal Mogul, Web EDI – 2010-2012
- HB Fuller, Strategic Sourcing – 2007-2008
- Honeywell EC&C, Procurement Portal – 2005-2007
- Corning Cable Systems, SAP SRM, 2009-2011
- General Cable, eProcurement, 2005-2011
- Chevron Products, SAP R/3, 1994

Beth Skillin: Project Manager/Engagement Manager

Beth Skillin is an Executive Consultant with Perfect Commerce, bringing over 8 years of experience with eProcurement solutions. She has held various roles at Perfect Commerce, starting as a QA Analyst and progressing to QA Director. Beth has spent the last three years in a strategic Product Management role, owning the Perfect**Shop** suite of products. She was primarily responsible for migrating all customers to the most current version. Recently she has transitioned into a professional services role, working with customers to deploy the Perfect Commerce solutions. Her deep knowledge base and experience enables her to work with customers to achieve maximum value from their investment.

Beth provides subject matter expertise in the areas of catalog search and content management, working with some of the following customers to enable them to reach or exceed their spend management goals.

- Halliburton
- Tetra Pak
- l'Oreal
- Evergreen Packaging
- JCI
- G6 Hospitality
- Schneider Electric
- BNP Paribas
- Skandia
- Rotech

Helene Richard: Supplier Enablement Specialist

Helene is a 15- year veteran in eProcurement solutions, dedicating over 10 years at Perfect Commerce leading the Supplier Enablement group with her expert knowledge in Indirect Spends, Supplier Onboarding process, and Content optimization for international organizations. She managed supplier activities for successful eProcurement implementations including BNP Paribas, L'Oreal, Tetra Pak, Johnson Controls, and ITT. Helene's two main goals has always been to help customers establish an environment that optimizes spend management through the procurement solution and to improve content quality in order to create better user experience and drive adoption.

Prior to joining Perfect Commerce, Helene was working for Answork, a French Marketplace, managing Indirect Sales strategy and Development for Bank shareholders as Distributors and Supplier Sourcing (indirect spends) to offer negotiated pricing to small & mid-size customers.

David Bates: Integration Specialist

With over 14 years of experience in the software development industry, David Bates has held several technical management and leadership roles ranging from Director of Software Engineering to Product Manager. David utilizes his background in development, quality assurance, and project and product management to drive and deliver quality products and solutions to market.

David graduated from the Virginia Military Institute with a Bachelor of Science degree in Computer Science and minors in Mathematics and Spanish. He is also Pragmatic Marketing certified.

Jim Galichia: Implementation Consultant

As a Senior Consultant, Mr. Galichia brings significant industry experience and knowledge in MRO Procurement and Supply Chain Management from 20+ years of experience in procurement, manufacturing, and supply chain consulting. In his 13 years at Perfect Commerce, Mr. Galichia has led dozens of procurement transformation projects for large and mid-sized companies and government entities across many industries and commodities.

Appendix G

He has managed projects for customers including: Hostess, Caremark, ITT, Johnson Controls, PACCAR, RockTenn, YRC Worldwide, Georgia Center for Non-Profits, Nielsen, Rent-A-Center, and others. Prior to coming to Perfect Commerce, Mr. Galichia worked as a business consultant for BDO Seidman and PricewaterhouseCoopers, leading teams in ERP and eProcurement Solutions Implementation at companies including: Atlas Weathering Systems, SOLO Cup, and General Motors. Prior to this, Mr. Galichia worked in Product Development, Inventory Management, Procurement, and Information Technology for several multi-national companies such as RCA Consumer Electronics Division and Courtaulds Packaging. Mr. Galichia holds a Bachelor of Science degree in Plastics Engineering Technology from Pittsburg State University and a Master of Business Administration from St Ambrose University.

1.4.1 Project Organization Chart

1.5 Communications Plan

Through the assignment of a local Client Executive and Technical Account Manager to every client, we stay in close communications with our customers to discuss any new requirements that arise from either business process enhancement requests or legislative change requests.

Perfect's first line of communication to any customer is the assigned Client Executive (CE). This Client Executive is a professional-level employee who serves as the single point of contact for a customer on all issues for the duration of their contract. The CE works with customers to ensure the success of Perfect's solutions and keep clients educated on changes, enhancements, and new initiatives from both Perfect and the market (potentially adding value to their business). The CE will work closely with the State, meeting on a frequent schedule and conducting Quarterly Business Reviews to review our performance and discuss challenges and opportunities which Perfect can help influence within the business.

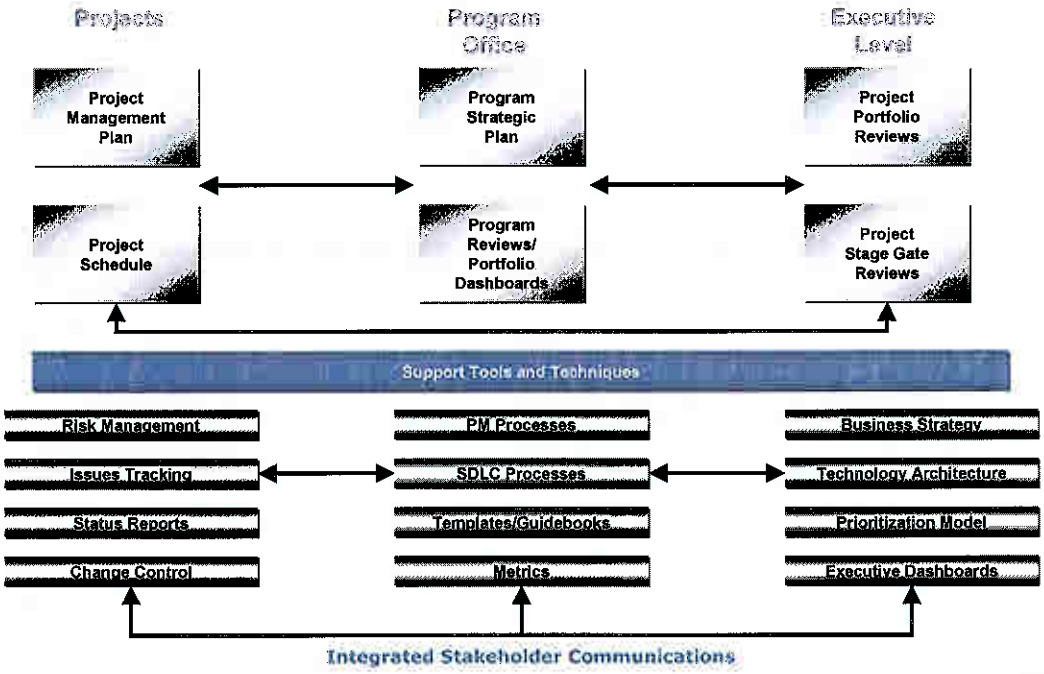
To support the Client Executive, Perfect Commerce assigns a Technical Account Manager to each of our customers. The Technical Account Manager will be aware of any support issues, and will personally ensure logged issues will be resolved. In addition, Perfect provides local Level One support which helps with logging any issues or requests from customers.

Appendix G

In the Perfect Commerce Methodology, the communication plan provides a critical vehicle for defining the audience and establishing the strategies that ensure effective visibility into the project by all stakeholders. Communication will focus on the internal project communications and those issues affecting the primary stakeholders directly associated with the project. The communication avenues may take the form of using collaboration tools such as SharePoint, weekly status reporting, weekly deliverable reviews and working product demos, and planned formal reviews, providing a clear understanding of the progress of the project.

Communication requirements will vary depending on the stage in the project lifecycle and the size and complexity of the organization. Specific communication vehicles and frequencies will be adopted to support the various needs of different audiences to ensure that clear visibility into the project is maintained and accurate information is provided to facilitate effective business decisions.

A communication plan will define the layout, structure and timing of standing meetings and formal reviews. A key mechanism for supporting effective meeting is the development of agendas and the documentation of minutes. Prior to any meeting a detailed agenda will be issued to those who should. This agenda will summarize what will be covered and the time allowed for the various topics. Expectations of meeting results will also be documented. This agenda will be distributed prior to each meeting or review in a manner outlined in the communication plan. The Perfect team will provide minutes of each of those meetings held with project team members, published within the pre-defined time limits of each meeting. Those minutes will provide an on-going journal of decisions, issues, and risks that occur during the course of a project, and provide a key ingredient to effective communication within and potentially external to the core project team.



High Level Communication Structure

Any topic brought up that is outside the scope of meeting will generally result in a new follow-up meeting being scheduled with a separate agenda constructed, and applicable to only those with stake in the topics. This is done to make certain that all project team members and client staff time devoted to the project is utilized in the most efficient and productive manner possible and that we have the right individuals involved for the subject matter.

The Perfect Commerce team understands the reality of trying to perform "business as usual" while still addressing the needs of a project and the demands on the State's business and technology user communities. Therefore it is essential that all meetings which require attendance of client staff be carefully planned, with the purpose and objectives defined in advance.

Appendix G

The goal in our communication planning is to ensure effective visibility into the project by executive management, provide timely communication to all key stakeholders, and ensure the project team has the information they need to do their work efficiently -getting the right information to the right people at the right time.

After the State is in production the Administrators are notified well in advance of a planned release. The releases are done first to the State's test environment so that the Administrators and power users will have a chance to test and QA the new release. Perfect will give the State 30 days to test the release. Once vetted by our customers, the release is rolled to our Production environment. The releases to production are usually done on Saturdays when our users typically are not in the system.

1.6 Issue Management Plan

Perfect Commerce provides exceptional support to its customers backed with its global support team. Sections below outline the support operation and specifically handling of defects/bugs.

First level procurement/OSN support is available Monday through Friday from 8:00 a.m. to 8:00 p.m. Eastern, excluding U.S. holidays. Support for business critical issues after hours can be reached through all posted toll-free or direct dial numbers. E-mail support is not available between the hours of 8:00 p.m. and 8:00 a.m. Eastern.

Issues that cannot be resolved within the Customer Support department are escalated to Application Support, a group of technicians who work with both Operations and Engineering to resolve the problem. If the issue appears to be a code-related bug, it will be delivered to the Quality Assurance (QA) team for investigation and write up.

Appendix G

Target response times for each priority level are available below. These are not resolution times, but expected windows for our organization to provide updates to customers. Once an issue has been assigned to development the target response times will no longer apply. The defect will become part of the development cycle and scheduled into a maintenance or full feature release based on priority, development hours required, and overall impact on clients' business processes.

Priority	Descriptions, Examples & Notes	Required Information
Priority 1 'Urgent'	• Application is unavailable. • No workarounds exist. • Revenue stream interrupted (Business is down).	• Description of the problem (Actual vs. Expected Results). • Actions/Steps to reproduce the problem. • Sample/Supporting data that illustrates the problem (Site URLs, Customer IDs, Order #s, SKU #s, User IDs, etc.). • Documented business impacts. • Root cause of the problem.
Priority 2 'High'	• Application is not achieving its primary goal. • Workarounds exist – though business is still heavily impacted. • Impending failure or downtime of an application.	• Description of the problem (Actual vs. Expected Results). • Actions/Steps to reproduce the problem. • Sample/Supporting data that illustrates the problem (Site URLs, Customer IDs, Order #s, SKU #s, User IDs, etc.). • Documented business impacts. • Root cause of the problem.
Priority 3 'Medium'	• Application is not achieving its primary goal. • Functionality does not appear to be working as expected. • Acceptable workarounds do exist. • Enhancements that are now work-in-progress.	• Description of the problem (Actual vs. Expected Results). • Actions/Steps to reproduce the problem. • Root cause of the problem. • Sample/Supporting Data that illustrates the Problem (Site URLs, Customer IDs, Order #s, SKU #s, User IDs, etc.).
Priority 4 'Low'	• Default value for new requests • Application is not achieving its primary goal. • Functionality does not appear to be working as expected. • Acceptable workarounds do exist and/or the business is not noticeably impacted. • The application is due for retirement in the short-term. • Repair costs are much greater than the value-add of the repair. • New enhancement requests.	• Description of the problem (Actual vs. Expected Results). • Actions/Steps to reproduce the problem. • Sample/Supporting Data that illustrates the Problem (Site URLs, Customer IDs, Order #s, SKU #s, User IDs, etc.). • Root cause of the problem. • Enhancements and changes also require specifications and other documentation before work can begin.

Appendix G

Activity	Target Response Times			
	Priority 1	Priority 2	Priority 3	Priority 4
Acknowledge/Respond to requests.	1 hour	2 hour	1 business day	2 business days
Analyze requests and take ownership or re-route (after initial Acknowledge/Respond to request time).	1 hour	4 hours	1 business day	5 business days
Frequency for communicating status updates to end users for individual Support Requests.	2 hours	Daily	As communicated	Monthly or weekly
Maximum elapsed duration to resolve user requests (for visibility of issues).	Every 2 hours during Customer Support Hours of Operations or as stated in initial response	Daily or as stated in initial response	Days or Weeks	Days, weeks or months

Perfect Commerce's Service Level Agreement reads as follows:

Force Majeure. Events or conditions beyond Perfect Commerce's reasonable control, including, without limitation, acts of common enemy, earthquakes, floods, fires, epidemics, terrorist attacks, embargoes, lack of internet availability, and inability to secure products or services from third parties.

Managed Environment Availability. The total number of minutes in a calendar month, less any Planned Downtime or downtime due to Force Majeure.

Planned Downtime. Scheduled unavailability of the Managed Environment, including but not limited to, the performance of system upgrades, enhancements and routine maintenance activities. Perfect Commerce will provide a schedule for recurring Planned Downtime (e.g., weekly system maintenance) and give the State not less than twenty-four (24) hours' notice of non-recurring Planned Downtime.

Unscheduled Service Outage. Interruptions to service that result in the unavailability of the Managed Environment to the State, not including Planned Downtime or interruptions due to Force Majeure.

1.7 Change Management Plan

Perfect uses the methodologies and approaches already described to maintain control of the engagement. The Project Management Plan (which includes the schedule), plus other planning deliverables, are considered living documents and will be updated as needed during the project, invoking appropriate change control as needed.

The schedule will be updated on a weekly basis to reflect progress made against the plan. Any changes to the schedule, resulting from various change processes, are entered to the schedule and their impact assessed. The baseline schedule identifies task and dependencies. Each week the project manager or team lead will update the tasks in Microsoft Project with actuals and completions as a percentage. Care will be taken to ensure that the percentages are meaningful by restricting the percentages to very few values (e.g. 0%, 25%, 50%, 75%, and 100% complete).

Corrective actions are initiated when the observed project performance falls outside pre-established thresholds for planned activities or when progress toward completion indicates the schedule is at risk. Projected slippages are identified by the team leads in their weekly reports or are discovered as part of regular project management procedures. In this way the slippage is often identified before it occurs rather than after.

Appendix G

The first corrective action is to determine what is causing the change to the plan, which is done through investigation by the project manager with the team leads. This will often involve the client management and the subject matter experts (SMEs). Once the cause for the slippage has been determined, the team will check other areas to see if the same problem may be simmering elsewhere and can be preempted.

A variety of corrective actions can be applied to recover the plan. When unforeseen problems arise, it may be necessary to take immediate measures to mitigate damage and develop new contingency plans. Corrective actions can alter schedules, staffing, or resource allocation to recover from slipped milestones. Problems of a serious magnitude may require solutions that redefine the basis for the commitments between organizations and the customer, and any significant change to the approach must be reviewed and approved by relevant management.

Corrective actions may include the following:

- Scope change
- Entire elimination of requirement(s)
- Re-allocation of requirements from developed software to manual procedures or to commercial off-the-shelf (COTS) software
- Allocation of personnel
- Additional allocation of development resources
- Re-planning
- Process changes

Tasks roll up to higher level tasks and significant deliverables/milestones. The project manager meets with the team leads to review progress at the rolled-up level, gather input from the leads, and take the pulse of the project. This is reported at the management level during weekly or monthly management meetings conducted by the Perfect Project Manager with NYS Project Manager. The Project Management Plan will be reviewed and updated as needed on a monthly basis to reflect changes in organization, resources, processes, or plans.

Status reports are automatically generated from MS Project to reflect the project's condition. Typical reports are Gantt and PERT charts and resource utilization reports. Date-driven reports provide information on start and end dates related to baseline, planned, and actual. Reports reflect variances between actual and baseline timeframes while the planned dates reflect the current ahead, on-target, or behind disposition of the project as related to the baseline timeframes based on a task's percent complete. Graphical reports will display the project's critical path. The following are examples of metrics that will be gathered to monitor project progress:

- Hours expended vs. hours planned
- Remaining hours to complete
- Tasks completed by date against planned date
- Phases completed vs. planned completion dates

Appendix G

In addition to reports generated from MS Project, Perfect uses other methods to assess project condition including, for example, summary spreadsheets or dashboards to communicate status more succinctly to senior management.

Sample - Executive Level Project Schedule Management Status Report for Discussion

					Time Management					
	WBS #	Tasks	Start Date	Finish Date	Planned Hrs.	Actual Hrs.	Schedule Variance	% Schedule Variance	% Work Complete	Ref. #
Last Week	**2.6**	**Text**	**1-Mar**	**5-Mar**	**110**	**133**	**23**	**21%**	**90%**	
	2.6.1	Text	1-Mar	1-Mar	10	15	5	50%	100%	1
	2.6.2	Text	1-Mar	2-Mar	20	33	13	65%	80%	2
	2.6.3	Text	1-Mar	3-Mar	30	40	10	33%	80%	3
	2.6.4	Text	1-Mar	5-Mar	50	45	-5	-10%	100%	4
	2.6.5	**Text**	**2-Mar**	**5-Mar**	**100**	**148**	**48**	**48%**	**80%**	
	2.6.5.1	Text	2-Mar	3-Mar	20	20	0	0%	100%	
	2.6.5.2	Text	2-Mar	4-Mar	40	78	38	95%	80%	5
	2.6.5.3	Text	2-Mar	5-Mar	40	50	10	25%	60%	6
	2.6.6	**Text**	**3-Mar**	**5-Mar**	**90**	**114**	**24**	**27%**	**95%**	
	2.6.6.1	Text	3-Mar	5-Mar	30	24	-6	-20%	100%	7
	2.6.6.2	Text	3-Mar	5-Mar	30	40	10	33%	75%	8
	2.6.6.3	Text	3-Mar	5-Mar	30	50	20	67%	80%	9
Next Week	**2.7**	**Text**	**8-Mar**	**19-Mar**	**440**	**0**	**-440**	**-100%**	**0%**	
	2.7.1	Text	8-Mar	12-Mar	50	0	-50	-100%	0%	
	2.7.1.1	Text	8-Mar	12-Mar	50	0	-50	-100%	0%	
	2.7.1.2	Text	8-Mar	12-Mar	50	0	-50	-100%	0%	
	2.7.1.3	Text	8-Mar	12-Mar	50	0	-50	-100%	0%	
	2.7.1.4	Text	10-Mar	19-Mar	80	0	-80	-100%	0%	
	2.7.1.5	Text	10-Mar	19-Mar	80	0	-80	-100%	0%	
	2.7.1.6	Text	10-Mar	19-Mar	80	0	-80	-100%	0%	

Our approach and Excel-based tools for Progress Analysis of the Project Plan is one example of the tools we bring to each client engagement

1.8 Security Strategy

Security is a critical concern when enterprise systems operate on the internet. The internet and its associated technologies were not inherently designed or intended for secure communications, and ensuring security for transactions carried over the internet is a challenging task. Perfect Commerce addresses the security vulnerabilities of internet communications and access with the Perfect Commerce Security Architecture -- a layered approach that integrates Perfect Commerce's security expertise with unique architecture and the technologies that support this architecture.

Perfect Commerce's Security Architecture includes:

- Highly qualified security experts and network engineers.
- Aggressive internal intrusion and threat detection.
- Continuous 24x7x365 monitoring by experienced security personnel.
- Maintenance and testing of software, hardware, and security patches in a mirrored test environment before release into the production environment.
- Use of proven, policy-based procedures along with the latest technologies to accurately track incidents, identify potential security breaches and provide rapid, appropriate response.
- Perfect Commerce's comprehensive security expertise, architecture, and technology deliver the total solution clients need to safely and reliable migrate their critical business applications to the web.
- 128 bit encryption is used with dual factor authentication.
- Authentication is required on both source and destination systems prior to electronic transmission of Data.
- No anonymous or guest accounts.
- All accounts are uniquely identified and authenticated.
- All user accounts require passwords.
- Password expiration is enforced.
- Accounts force password change upon first logon.
- Accounts are locked out after 5 or less invalid logon attempts, and lockout duration is at least 30 minutes.

Appendix G

Perfect Commerce protects the confidentiality of data by requiring authentication of each person's identification. For example, this authentication is obtained when you enter your user ID and secret password when logging into Perfect Commerce applications. User IDs and passwords are assigned and maintained by Perfect Commerce personnel. State information will be protected to the fullest extent utilizing Perfect Commerce's authentication processes, making it impossible for exploitation/use of information by unauthorized individuals within Perfect.

For additional information, our Information Security Guide is included in Appendix B of this proposal. It provides further clarity as to Perfect Commerce's compliance with the security protocol outlined in RFP Attachment 5—IT Provisions.

1.9 Quality Assurance Strategy

Minor and major releases of our software are subject to stringent quality assurance processes including functional, performance and capacity tests. Quality Assurance is critical to Perfect Commerce, as it should be for any cloud-based SaaS vendor of mission critical software for the enterprise. Attached is Perfect's Release Process Guide which includes the details of our releasing process for all production changes. Our software development process is based on the Lean-Agile methodology.

Quality is at the core of our software development methodology and is embedded in the heart of our development. During the development process, our quality team remains engaged, preparing the Quality Assurance (QA) plans to ensure that necessary quality assurance tasks take place (i.e., continuous code reviews, unit testing, automatic code quality analysis, automated integration building, and execution of automated tests).

Prepared QA plans engage users and organizations to ensure our suite's capabilities include all of the necessary requirements as well as additional requests from each individual customer. User Acceptance Testing (UAT) creates a stage environment to allow users to test and verify new releases before the features are put into production. Perfect team members work in two week sprints to produce new software; each sprint is individually assessed by Quality Assurance processes before the next sprint begins. This ensures that we test our new developments as we develop them.

The screenshot below illustrates a sample coverage report.

		Best Buy Canada (BB)	Cox Communications (CX)	ADP Vendorbase on AP	Campbell's Soup (CS)	Campbell's Soup Accounts Payables (AP2AB)	Fansteel Management (114)	Fiserv (FS)	Library (LIB)	Mobile Tech Services (MT)	Pathway (PW)	Pulte (117)	Purchasing	Sherwin Williams (SW)	Walgreens
2	Desktop Setup														
2.2	Desktop Setup	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
3	Integration Test Scripts														
3.1	Requests														
3.1.1	Off-Catalog Request Creation with Approval	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
3.1.2	Request Modification - Increase	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
3.1.3	Request Modification - Decrease	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
3.1.4	Request Cancellation	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
3.1.5	Request with Multiple Accounting Lines	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
3.1.6	Reconciling Request	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
3.1.7	Catalog Request	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
3.1.8	Request Creation Without Approval	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
3.1.9	Request Rejection	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
3.2	Purchase Orders														
3.2.1	PO Creation from Request with Approval	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
3.2.2	Multiple PO Creation from 1 Request	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
3.2.3	PO Modification - Increase		✓	✓	✓							✓			
3.2.4	PO Modification - Decrease		✓	✓	✓							✓			
3.2.5	PO Cancellation		✓	✓	✓							✓			
3.2.6	PO with Multiple Accounting Lines	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
3.2.7	PO Creation with 1099 Reportable Vendor	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA
3.2.8	PO Creation with non-1099 Reportable Vendor	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA
3.2.9	PO Creation with SSN Vendor	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA

Sample Test Coverage Report

Appendix G

Prepared test scripts such as the one depicted below are assigned to individual team members and data is aggregated from the team to finalize the quality report.

		Pass/Fail	Description
3			Desktop Setup
3.2	Update Desktop Setup		Verify completed
8			Integration Test Scripts
8.2	Requests		
8.2.1	Off-Catalog Request Creation with Approval		
8.2.2	Request Modification - Increase		
8.2.3	Request Modification - Decrease		
8.2.4	Request Cancellation		
8.2.5	Request with Multiple Accounting Lines		
8.2.6	RoundTrip Request		
8.2.7	Catalog Request		
8.2.8	Request Creation without Approval		
8.2.9	Request Rejection		
8.3	Purchase Orders		
8.3.1	PO Creation from Request with Approval		
8.3.2	Multiple PO Creation from 1 Request		
8.3.3	PO Modification - Increase		
8.3.4	PO Modification - Decrease		
8.3.5	PO Cancellation		
8.3.6	PO with Multiple Accounting Lines		
8.3.10	PO Rejection		
8.9	Catalogs		
8.9.1	Catalog Generation from Solicitation – Single Year Pricing		
8.9.2	Catalog Generation from Solicitation – Multi Year Pricing		
8.4	Contracts		
8.4.1	Contract Wizard		
8.4.2	Contract Generation from Solicitation		
8.4.3	Contract Amendment		
8.4.4	Associating a Catalog to a Contract		
8.5	Invoices/Payments		
8.5.1	Invoice Creation with Approval		
8.5.2	Invoice Modification - Increase		

Sample Test Script

Our issue tracker, OnTime™, is utilized during this period to report defects, ideas, enhancements and any other issues. The development team responds to the reported tickets and prepares the fixes while the configuration management team manages scheduled deployment to the test environment to verify the resolution and to close the tickets.

The names and logos for OnTime™ are registered trademarks of Axosoft, LLC.

A release passes functional testing based on a pre-defined and agreed upon criteria such as *"There may be no critical or high priority issues. Medium issue count may not exceed 3 and low priority issue count may not exceed 10."* Reaching this goal signifies completion of the functional testing process.

High concurrency is nature of the technology in the multi-tenant environment above and beyond the basics of the solicitation process. Systems rules and how they are enforced in a high concurrency environment where seconds matter is ensured by our performance testing and verification process. Our quality and engineering teams utilize tools such as LoadRunner, Visual Studio Test Edition/Test Professional and JMeter to conform the performance requirements on high concurrency environment. During these test data volume and system reliability are also confirmed under high stress environment. The figure on the following page illustrates system performance report under high volume of transactions around solicitation/sourcing module.

Appendix G

Transaction Name	SLA Status	Minimum	Average	Maximum	Std. Deviation	90 Percent	Pass	Fail	Stop
Action_Transaction		15.297	17.267	19.156	0.972	18.789	50	0	0
AddItems		1.048	1.523	3.528	0.422	2.024	50	0	0
AddSupplier		2.075	2.462	3.45	0.322	2.912	50	0	0
BrowseLib		0.294	0.515	0.78	0.153	0.713	50	0	0
CreateSol		0.265	0.413	0.792	0.128	0.602	50	0	0
EditHeader		0.256	0.419	0.804	0.134	0.598	50	0	0
FormalSol		0.866	1.193	1.602	0.166	1.417	50	0	0
ItemSpec		0.155	0.252	0.509	0.1	0.399	50	0	0
Login		1.651	2.097	2.924	0.325	2.611	50	0	0
Logout		0.099	0.134	0.232	0.027	0.171	50	0	0
SelectOrg		0.206	0.291	0.49	0.076	0.42	50	0	0
SolSummary		1.201	2.03	3.165	0.447	2.488	50	0	0
SubmitSol		0.778	0.966	1.367	0.109	1.067	50	0	0
SupplierSelection		4.66	4.988	5.649	0.244	5.319	50	0	0
vuser_end_Transaction		0	0	0	0	0	25	0	0
vuser_init_Transaction		0	0	0.002	0	0.002	25	0	0

Service Level Agreement Legend: Pass Fail No Data

HTTP Responses Summary

HTTP Responses	Total	Per second
HTTP_200	6,0508.705	

Solicitation Module Performance Test Results Example

About 20% of the organization is dedicated to the quality assurance of the product. Similar to customer satisfaction, service quality is measured through the tracking of several product systems. Our Help desk system is used to measure support tickets and resolutions along with resolution periods. Frequent reviews of support and development processes are performed to follow our SSAE 16 (SAS 70) guidelines and measurements. Help desk reports are provided to the CIO and shared with the management and executive teams to ensure quality products, services and client relationships.

1.10 Training Plan

The project team will conduct a series of end user training sessions for designated State personnel. Using a "train-the-trainer" model, coursework in buyer, supplier and administrative processes will be taught. In addition, support-related training for issues management and maintenance will be provided. All coursework will include training materials.

In addition to the training programs provided to the State's personnel, our product offers variety of options to streamline training of the State's large supplier community including context sensitive help, web base trainings, videos and others.

Trainings for the State's buyer users, are designed and planned to be completed prior to User Acceptance Testing period in order to prepare the State's staff to use Perfect's software during user acceptance period.

1.10.1 Our Training Approach

Perfect Commerce's training approach is built upon the success of our past training experience on other implementation projects. The strength of our approach derives from our ability to integrate "Just in Time" training with application implementation and to customize our training programs and delivery approach to meet specific end-user/organizational needs. In order to control the project cost of training, Perfect Commerce is recommending a Train the Trainer approach along with additional training aides to help the State achieve complete end user training during the project and the State-wide rollout of Perfect**Shop**. Perfect Commerce offers a variety of training formats to successfully train end users.

Training options include:

Appendix G

- On-site training sessions
- Computer Based Tutorials
- Video recordings of instructor lead training sessions

The Perfect Commerce training curriculum includes:

- On-site Training
- Train-the-Trainer
- System Administration Certification
- Supplier Management

On-Site Training

Perfect Commerce will conduct a total of 12 on-site web-based training sessions throughout the project. Training exercises will be conducted on a live training environment, the most effective hands-on learning experience. Trainees will be guided through extensive customized training activities based on the State's business processes.

Below is the suggested breakdown of the end user trainings conducted by a Perfect Commerce head trainer included in the proposed project:

Focus Area	Session Duration	# of times class conducted	Max recommended # of attendees
Formal/Informal Solicitations	3 hours	3	15
Reports	1 hours	3	15
Approval Module	1 hours	3	15
Identified during the project	2 hours	3	15

A Perfect Commerce head instructor conducts the training session(s) with support from a State assistant instructor. The training session(s) are customized based on the needs of that particular group of trainees. We recommend limiting the training sessions to fifteen people per session to ensure that trainees receive ample personal attention.

Upon successful completion of a session, users will receive the appropriate reference materials. Documentation includes quick reference guides for each tool, Dictionary of Buttons and Icon, electronic access to the User Reference Manual and web based tutorials for each module of the system. Users will also have access to our comprehensive and easy-to-use online help tool.

Perfect's online help is context sensitive. The interface design uses wizards to help move users step by step through different procurement processes. All icons are tagged to help users more easily navigate the system. Online help will be updated to reflect any new functionality or enhancements to the product with each new major release.

Train-the-Trainer

The Train-the-Trainer program has proven to be the most effective method to encourage State ownership and system usage. To begin to build confidence using Perfect the identified State internal trainers will participate in all on-site training sessions on each module of the Perfect system lead by a Perfect Commerce head instructor. A Perfect Commerce instructor will observe the internal trainers as they conduct their first independent sessions. Once the internal trainers have, under observation, successfully trained on each module, the trainers will receive certification and reference materials so they can

schedule and conduct future sessions independent of a Perfect Commerce instructor. We are confident that by participating in the Train-the-Trainer program, the State's users will use the system's full functionality and quickly realize the benefits of Perfect's software suite.

System Administration

Continuing with the effort to achieve self-sufficiency, New York will identify State system administrators who will be eligible for System Administration training to manage and administer the statewide configuration for the State of New York. The administrators will learn how to use the system administration tool to add/delete users and organizations, manage the approval workflow, assign security and access to system users, maintain location addresses, maintain supplier accounts and manage payment information. Following the system administration training, the administrator will configure a test department that will mirror the State's business rules and can later be used as the State's training environment. A Perfect Commerce representative will review the administrator's work and award certification.

Supplier Management Administration

The State will identify New York Supplier Management Administrators. The Supplier Management Administrators, upon completion of the training, will control supplier profile status and access within the State's hierarchy. The status of a supplier will determine the supplier's visibility and availability for the State's solicitation opportunities.

1.11 SUBCONTRACTORS

There will be no subcontractors or sub-consultants needed for this project, however Perfect will use subcontractors as designated in its MWBE Utilization Plan.

APPENDIX H

CAIQ

Consensus Assessments Initiative Questionnaire v1.1

DID	Domain	Control Group	CGID	CID	Consensus Assessment Questions		Comments and Notes	CCMv1.1 Compliance Mapping: COBIT	HIPAA	ISO27001	SP800_53	FedRAMP	PCI_DSS	BITS	GAPP
CO	Compliance														
CO	Compliance	Audit Planning	CO-01	CO-01.1	Do you produce audit assertions using a structured, industry accepted format (ex. CloudAudit/A6 URI Ontology, CloudTrust, SCAP/CYBEX, GRC XML, ISACA's Cloud Computing Management Audit/Assurance Program, etc.)?	Yes	We use a third party resource to audit the effectiveness of our services provided and the internal controls and security for such services. The third party will identify any control deficiencies within our organization. In addition, the third party will assess the quality of, and our ability to support, our attestations regarding our internal controls.	COBIT 4.1 ME 2.1, ME 2.2 PO 9.5 PO 9.6	45 CFR 164.312(b)	Clause 4.2.3 e) Clause 4.2.3b Clause 5.1 g Clause 6 A.15.3.1	NIST SP800-53 R3 CA-2 NIST SP800-53 R3 CA-7 NIST SP800-53 R3 PL-6	NIST SP800-53 R3 CA-2 NIST SP800-53 R3 CA-2 (1)NIST SP800-53 R3 CA-7 NIST SP800-53 R3 CA-7 (2) NIST SP800-53 R3 PL-6	PCI DSS v2.0 2.1.2.b	SIG v6.0: L.1, L.2, L.7, L.9, L.11	GAPP Ref 10.2.5
CO	Compliance	Independent Audits	CO-02	CO-02.1	Do you allow tenants to view your SAS70 Type II/SSAE 16 SOC2/ISAE3402 or similar third party audit reports?	Yes		COBIT 4.1 DS5.5, ME2.5, ME 3.1 PO 9.6	45 CFR 164.308 (a)(8)	Clause 4.2.3e Clause 5.1 g	NIST SP800-53 R3 CA-1	NIST SP800-53 R3 CA-1	PCI DSS v2.0 11.2	SIG v6.0: L.2, L.4, L.7, L.9,	GAPP Ref 1.2.5 GAPP Ref 1.2.7
CO	Compliance		CO-02	CO-02.2	Do you conduct network penetration tests of your cloud service infrastructure regularly as prescribed by industry best practices and guidance?	Yes		COBIT 4.1 DS5.5, ME2.5, ME 3.1 PO 9.6	45 CFR 164.308 (a)(8) 45 CFR	Clause 4.2.3e Clause 5.1 g Clause 5.2.1 d)	NIST SP800-53 R3 CA-1 NIST SP800-53	NIST SP800-53 R3 CA-1 NIST SP800-53	PCI DSS v2.0 11.2 PCI DSS v2.0	SIG v6.0: L.2, L.4, L.7, L.9, L.11	GAPP Ref 1.2.5 GAPP Ref 1.2.7 GAPP Ref 4.2.1
CO	Compliance		CO-02	CO-02.3	Do you conduct regular application penetration tests of your cloud infrastructure as prescribed by industry best practices and guidance?	Yes		COBIT 4.1 DS5.5, ME2.5, ME 3.1 PO 9.6	45 CFR 164.308 (a)(8)	Clause 4.2.3e Clause 5.1 g	NIST SP800-53 R3 CA-1	NIST SP800-53 R3 CA-1	PCI DSS v2.0 11.2	SIG v6.0: L.2, L.4, L.7, L.9,	GAPP Ref 1.2.5 GAPP Ref 1.2.7
CO	Compliance		CO-02	CO-02.4	Do you conduct internal audits regularly as prescribed by industry best practices and guidance?	Yes		COBIT 4.1 DS5.5, ME2.5, ME 3.1 PO 9.6	45 CFR 164.308 (a)(8)	Clause 4.2.3e Clause 5.1 g	NIST SP800-53 R3 CA-1	NIST SP800-53 R3 CA-1	PCI DSS v2.0 11.2	SIG v6.0: L.2, L.4, L.7, L.9,	GAPP Ref 1.2.5 GAPP Ref 1.2.7
CO	Compliance		CO-02	CO-02.5	Do you conduct external audits regularly as prescribed by industry best practices and guidance?	Yes		COBIT 4.1 DS5.5, ME2.5, ME 3.1 PO 9.6	45 CFR 164.308 (a)(8)	Clause 4.2.3e Clause 5.1 g	NIST SP800-53 R3 CA-1	NIST SP800-53 R3 CA-1	PCI DSS v2.0 11.2	SIG v6.0: L.2, L.4, L.7, L.9,	GAPP Ref 1.2.5 GAPP Ref 1.2.7
CO	Compliance		CO-02	CO-02.6	Are the results of the network penetration tests available to tenants at their request?	Yes		COBIT 4.1 DS5.5, ME2.5, ME 3.1 PO 9.6	45 CFR 164.308 (a)(8)	Clause 4.2.3e Clause 5.1 g	NIST SP800-53 R3 CA-1	NIST SP800-53 R3 CA-1	PCI DSS v2.0 11.2	SIG v6.0: L.2, L.4, L.7, L.9,	GAPP Ref 1.2.5 GAPP Ref 1.2.7
CO	Compliance		CO-02	CO-02.7	Are the results of internal and external audits available to tenants at their request?	Yes		COBIT 4.1 DS5.5, ME2.5, ME 3.1 PO 9.6	45 CFR 164.308 (a)(8)	Clause 4.2.3e Clause 5.1 g	NIST SP800-53 R3 CA-1	NIST SP800-53 R3 CA-1	PCI DSS v2.0 11.2	SIG v6.0: L.2, L.4, L.7, L.9,	GAPP Ref 1.2.5 GAPP Ref 1.2.7
CO	Compliance	Third Party Audits	CO-03	CO-03.1	Do you permit tenants to perform independent vulnerability assessments?	Yes		COBIT 4.1 ME 2.6, DS 2.1, DS 2.4	45 CFR 164.308(b)(1) (New)	A.6.2.3 A.10.2.1 A.10.2.2	NIST SP800-53 R3 CA-3 NIST SP800-53		PCI DSS v2.0 2.4 PCI DSS v2.0 12.8.2	AUP v5.0 C.2 SIG v6.0: C.2.4,C.2.6,	GAPP Ref 1.2.11 GAPP Ref 4.2.3
CO	Compliance		CO-03	CO-03.2	Do you have external third-party conduct vulnerability scans and periodic penetration tests on your applications and networks?	Yes		COBIT 4.1 ME 2.6, DS 2.1, DS 2.4	45 CFR 164.308(b)(1)	A.6.2.3 A.10.2.1	NIST SP800-53 R3 CA-3		PCI DSS v2.0 2.4 PCI DSS v2.0	AUP v5.0 C.2 SIG v6.0:	GAPP Ref 1.2.11
CO	Compliance	Contact / Authority Maintenance	CO-04	CO-04.1	Do you maintain liaisons and points of contact with local authorities in accordance with contracts and appropriate regulations?	Yes		COBIT 4.1 ME 3.1		A.6.1.6 A.6.1.7	NIST SP800-53 R3 AT-5 NIST SP800-53 R3 IR-6 NIST SP800-53 R3 SI-5	NIST SP800-53 R3 AT-5 NIST SP800-53 R3 IR-6 NIST SP800-53 R3 IR-6 (1) NIST SP800-53 R3 SI-5	PCI DSS v2 11.1.e PCI PCI DSS v2 12.5.3 PCI DSS v2 12.9	SIG v6.0: L1	GAPP Ref 1.2.7 GAPP Ref 10.1.1 GAPP Ref 10.2.4
CO	Compliance	Information System Regulatory Mapping	CO-05	CO-05.1	Do you have the ability to logically segment or encrypt customer data such that data may be produced for a single tenant only, without inadvertently accessing another tenant's data?	Yes	This control will likely move to the Legal domain in v2.0.	COBIT 4.1 ME 3.1		ISO/IEC 27001:2005 Clause 4.2.1 b) 2)			PCI DSS v2.0 3.1.1 PCI DSS v2.0 3.1	SIG v6.0: L.1, L.2, L.4, L.7, L.9	GAPP Ref 1.2.2 GAPP Ref 1.2.4 GAPP Ref 1.2.6 GAPP Ref
CO			CO-05	CO-05.2	Do you have capability to logically segment and recover data for a specific customer in the case of a failure or data loss?	Yes		COBIT 4.1 ME 3.1		ISO/IEC 27001:2005 Clause 4.2.1 b) 2)			PCI DSS v2.0 3.1.1 PCI DSS v2.0 3.1	SIG v6.0: L.1, L.2, L.4, L.7, L.9	GAPP Ref 1.2.2 GAPP Ref 1.2.4 GAPP Ref 1.2.6 GAPP Ref
CO	Compliance	Intellectual Property	CO-06	CO-06.1	Do you have policies and procedures in place describing what controls you have in place to protect tenants intellectual property?	Yes				Clause 4.2.1 A.6.1.5 A.7.1.3 A.10.8.2 A.12.4.3 A.15.1.2	NIST SP800-53 R3 SA-6 NIST SP800-53 R3 SA-7 NIST SP800-53 R3 PM-5	NIST SP800-53 R3 SA-6 NIST SP800-53 R3 SA-7 NIST SP800-53 R3 PM-5		SIG v6.0: L.4	
CO	Compliance	Intellectual Property	CO-07	CO-07.1	If utilization of tenants services housed in the cloud is mined for cloud provider benefit, are the tenants IP rights preserved?	Yes	This control will likely move to the Legal domain in v2.0.								
CO	Compliance	Intellectual Property	CO-08	CO-08.1	If utilization of tenants services housed in the cloud is mined for cloud provider benefit, do you provide tenants the ability to opt-out?	Yes	This control will likely move to the Legal domain in v2.0.								
DG	Data Governance														

DG	Data Governance	Ownership / Stewardship	DG-01	DG-01.1	Do you follow a structured data-labeling standard (ex. ISO 15489, Oasis XML Catalog Specification, CSA data type guidance)?	Yes		COBIT 4.1 DS5.1, PO 2.3	45 CFR 164.308 (a)(2)	A.6.1.3 A.7.1.2 A.15.1.4	NIST SP800-53 R3 CA-2 NIST SP800-53 R3 PM-5 NIST SP800-53 R3 PS-2 NIST SP800-53 R3 RA-2 NIST SP800-53 R3 SA-2	NIST SP800-53 R3 CA-2 NIST SP800-53 R3 CA-2 (1) NIST SP800-53 R3 PM-5 NIST SP800-53 R3 PS-2 NIST SP800-53 R3 RA-2 NIST SP800-53 R3 SA-2		SIG v6.0: C.2.5.1, C.2.5.2, D.1.3, L.7	GAPP Ref 6.2.1
DG	Data Governance	Classification	DG-02	DG-02.1	Do you provide a capability to identify virtual machines via policy tags/metadata (ex. Tags can be used to limit guest operating systems from booting/instantiating/transporting data in the wrong country, etc.)?	Yes		COBIT 4.1 PO 2.3, DS 11.6		A.7.2.1	NIST SP800-53 R3 RA-2 NIST SP800-53 R3 AC-4	NIST SP800-53 R3 RA-2 NIST SP800-53 R3 AC-4	PCI DSS v2.0 9.7.1 PCI DSS v2.0 9.10	SIG v6.0: D.1.3, D.2.2	GAPP Ref 1.2.3 GAPP Ref 1.2.6 GAPP Ref 4.1.2 GAPP Ref 8.2.1
DG	Data Governance		DG-02	DG-02.2	Do you provide a capability to identify hardware via policy tags/metadata/hardware tags (ex. TXT/TPM, VN-Tag, etc.)?	Yes		COBIT 4.1 PO 2.3, DS 11.6		A.7.2.1	NIST SP800-53 R3 RA-2	NIST SP800-53 R3 RA-2	PCI DSS v2.0 9.7.1	SIG v6.0: D.1.3, D.2.2	GAPP Ref 1.2.3 GAPP Ref 1.2.6
DG	Data Governance		DG-02	DG-02.3	Do you have a capability to use system geographic location as an authentication factor?	No	Our solution does not "roam" like an Amazon Cloud service. We control where the VMs are located.	COBIT 4.1 PO 2.3, DS 11.6		A.7.2.1	NIST SP800-53 R3 RA-2 NIST SP800-53 R3 AC-4	NIST SP800-53 R3 RA-2 NIST SP800-53 R3 AC-4	PCI DSS v2.0 9.7.1 PCI DSS v2.0 9.10	SIG v6.0: D.1.3, D.2.2	GAPP Ref 1.2.3 GAPP Ref 1.2.6 GAPP Ref 4.1.2 GAPP Ref 8.2.1
DG	Data Governance		DG-02	DG-02.4	Can you provide the physical location/geography of storage of a tenant's data upon request?	Yes		COBIT 4.1 PO 2.3, DS 11.6		A.7.2.1	NIST SP800-53 R3 RA-2	NIST SP800-53 R3 RA-2	PCI DSS v2.0 9.7.1	SIG v6.0: D.1.3, D.2.2	GAPP Ref 1.2.3 GAPP Ref 1.2.6
DG	Data Governance		DG-02	DG-02.5	Do you allow tenants to define acceptable geographical locations for data routing or resource instantiation?	Yes	If you have a special request then we may make appropriate changes. However, this is outside the normal scope of operations.	COBIT 4.1 PO 2.3, DS 11.6		A.7.2.1	NIST SP800-53 R3 RA-2 NIST SP800-53 R3 AC-4	NIST SP800-53 R3 RA-2 NIST SP800-53 R3 AC-4	PCI DSS v2.0 9.7.1 PCI DSS v2.0 9.10	SIG v6.0: D.1.3, D.2.2	GAPP Ref 1.2.3 GAPP Ref 1.2.6 GAPP Ref 4.1.2 GAPP Ref 8.2.1
DG	Data Governance	Handling / Labeling / Security Policy	DG-03	DG-03.1	Are Polices and procedures established for labeling, handling and security of data and objects which contain data?	Yes		COBIT 4.1 PO 2.3, DS 11.6		A.7.2.2 A.10.7.1	NIST SP800-53 R3 AC-16	NIST SP800-53 R3 AC-16	PCI DSS v2.0 9.5 PCI DSS v2.0 9.6	AUP v5.0 G.13 SIG v6.0: D.2.2	GAPP Ref 1.1.2 GAPP Ref 5.1.0
DG	Data Governance		DG-03	DG-03.2	Are mechanisms for label inheritance implemented for objects that acts as aggregate containers for data?	Yes		COBIT 4.1 PO 2.3, DS 11.6		A.7.2.2 A.10.7.1	NIST SP800-53 R3 AC-16	NIST SP800-53 R3 AC-16	PCI DSS v2.0 9.5 PCI DSS v2.0 9.6	AUP v5.0 G.13 SIG v6.0: D.2.2	GAPP Ref 1.1.2 GAPP Ref 5.1.0
DG	Data Governance	Retention Policy	DG-04	DG-04.1	Do you have technical control capabilities to enforce tenant data retention policies?	Yes		COBIT 4.1 DS 4.1, DS 4.2, DS 4.5, DS 4.9, DS 11.6	45 CFR 164.308 (a)(7)(ii)(A)	Clause 4.3.3 A.10.5.1	NIST SP800-53 R3 CP-2		PCI DSS v2.0 3.1 PCI DSS v2.0	SIG v6.0: D.2.2.9	GAPP Ref 5.1.0 GAPP Ref 5.1.1
DG	Data Governance		DG-04	DG-04.2	Do you have a documented procedure for responding to requests for tenant data from governments or third parties?	Yes	If a request comes from a third party or government, we will first inform the relevant owner of the data, who may then have an opportunity to seek an injunction.	COBIT 4.1 DS 4.1, DS 4.2, DS 4.5, DS 4.9, DS 11.6	45 CFR 164.308 (a)(7)(ii)(A) 45 CFR 164.310 (d)(2)(iv) 45 CFR	Clause 4.3.3 A.10.5.1 A.10.7.3	NIST SP800-53 R3 CP-2 NIST SP800-53 R3 CP-6 NIST SP800-53		PCI DSS v2.0 3.1 PCI DSS v2.0 3.1.1 PCI DSS v2.0 3.2 PCI DSS v2.0	SIG v6.0: D.2.2.9	GAPP Ref 5.1.0 GAPP Ref 5.1.1 GAPP Ref 5.2.2 GAPP Ref 8.2.6
DG	Data Governance	Secure Disposal	DG-05	DG-05.1	Do you support secure deletion (ex. degaussing / cryptographic wiping) of archived data as determined by the tenant?	Yes		COBIT 4.1 DS 11.4	45 CFR 164.310 (d)(2)(i)	A.9.2.6 A.10.7.2	NIST SP800-53 R3 MP-6	NIST SP800-53 R3 MP-6	PCI DSS v2.0 3.1.1	SIG v6.0: D.2.2.10,	GAPP Ref 5.1.0 GAPP Ref 5.2.3
DG	Data Governance		DG-05	DG-05.2	Can you provide a published procedure for exiting the service arrangement, including assurance to sanitize all computing resources of tenant data once a customer has exited your environment or has vacated a resource?	Yes	Upon request, we will certify that all computer resources with tenant data will be degaussed, and destroyed.	COBIT 4.1 DS 11.4	45 CFR 164.310 (d)(2)(i) 45 CFR 164.310 (d)(2)(ii)	A.9.2.6 A.10.7.2	NIST SP800-53 R3 MP-6 NIST SP800-53 R3 PE-1	NIST SP800-53 R3 MP-6 NIST SP800-53 R3 MP-6 (4) NIST SP800-53 R3 PE-1	PCI DSS v2.0 3.1.1 PCI DSS v2.0 9.10 PCI DSS v2.0 9.10.1	SIG v6.0: D.2.2.10, D.2.2.11, D.2.2.14,	GAPP Ref 5.1.0 GAPP Ref 5.2.3
DG	Data Governance	Nonproduction Data	DG-06	DG-06.1	Do you have procedures in place to ensure production data shall not be replicated or used in non-production environments?	Yes			45 CFR 164.308(a)(4)(ii)(B)	A.7.1.3 A.10.1.4 A.12.4.2 A.12.5.1	NIST SP800-53 R3 SA-11 NIST SP800-53 R3 CM-04	NIST SP800-53 R3 SA-11 NIST SP800-53 R3 SA-11 (1) NIST SP800-53 R3 CM-04	PCI DSS v2.0 6.4.3	SIG v6.0: I.2.18	GAPP Ref 1.2.6
DG	Data Governance	Information Leakage	DG-07	DG-07.1	Do you have controls in place to prevent data leakage or intentional/accidental compromise between tenants in a multi-tenant environment?	Yes		COBIT 4.1 DS 11.6		A.10.6.2 A.12.5.4	NIST SP800-53 R3 AC-2 NIST SP800-53		PCI DSS v2.0 1.2 PCI DSS v2.0 6.5.5	SIG v6.0: I.2.18	GAPP Ref 7.2.1 GAPP Ref 8.1.0 GAPP Ref 8.1.1
DG	Data Governance		DG-07	DG-07.2	Do you have a Data Loss Prevention (DLP) or extrusion prevention solution in place for all systems which interface with your cloud service offering?	Yes		COBIT 4.1 DS 11.6		A.10.6.2 A.12.5.4	NIST SP800-53 R3 AC-2 NIST SP800-53		PCI DSS v2.0 1.2 PCI DSS v2.0 6.5.5	SIG v6.0: I.2.18	GAPP Ref 7.2.1 GAPP Ref 8.1.0 GAPP Ref 8.1.1
DG	Data Governance	Risk Assessments	DG-08	DG-08.1	Do you provide security control health data in order to allow tenants to implement industry standard Continuous Monitoring (which allows continual tenant validation of your physical and logical control status?)	No	We do provide tenants access to our realtime monitoring solution; however, we do report on our SLAs, etc.	COBIT 4.1 PO 9.1, PO 9.2, PO 9.4, DS 5.7	45 CFR 164.308(a)(1)(ii)(A) (New) 45 CFR 164.308(a)(8) (New)	Clause 4.2.1 c) & g) Clause 4.2.3 d) Clause 4.3.1 & 4.3.3 Clause 7.2 & 7.3 A.7.2 A.15.1.1 A.15.1.3 A.15.1.4	NIST SP800-53 R3 CA-3 NIST SP800-53 R3 RA-2 NIST SP800-53 R3 RA-3 NIST SP800-53 R3 MP-8 NIST SP800-53 R3 PM-9 NIST SP800-53 R3 SI-12	NIST SP800-53 R3 CA-3 NIST SP800-53 R3 RA-2 NIST SP800-53 R3 RA-3 NIST SP800-53 R3 MP-8 NIST SP800-53 R3 PM-9 NIST SP800-53 R3 SI-12	PCI DSS v2.0 12.1 PCI DSS v2.0 12.1.2	SIG v6.0: L.4, L.5, L.6, L.7	GAPP Ref 1.2.4 GAPP Ref 8.2.1
FS	Facility Security														

FS	Facility Security	Policy	FS-01	FS-01.1	Can you provide evidence that policies and procedures have been established for maintaining a safe and secure working environment in offices, rooms, facilities and secure areas?	Yes		COBIT 4.1 DS5.7, DS 12.1, DS 12.4 DS 4.9	45 CFR 164.310 (a)(1) 45 CFR 164.310 (a)(2)(ii) 45 CFR 164.308(a)(3)(ii)(A) (New) 45 CFR 164.310 (a)(2)(iii) (New)	A.5.1.1 A.9.1.3 A.9.1.5	NIST SP800-53 R3 CA-2 NIST SP800-53 R3 PE-1 NIST SP800-53 R3 PE-6 NIST SP800-53 R3 PE-7 NIST SP800-53 R3 PE-8	NIST SP800-53 R3 CA-2 NIST SP800-53 R3 CA-2 (1) NIST SP800-53 R3 PE-1 NIST SP800-53 R3 PE-6 NIST SP800-53 R3 PE-6 (1) NIST SP800-53 R3 PE-7 NIST SP800-53 R3 PE-7 (1) NIST SP800-53 R3 PE-8	PCI DSS v2.0 9.1 PCI DSS v2.0 9.2 PCI DSS v2.0 9.3 PCI DSS v2.0 9.4	AUP v5.0 F.2 SIG v6.0: F.1.1, F.1.2 F.1.3, F.1.4, F1.5, F.1.6, F.1.7, F.1.8, F.1.9, F.2.1, F.2.2, F.2.3, F.2.4, F.2.5, F2.6, F.2.7, F.2.8, F.2.9, F.2.10, F.2.11, F.2.12, F.2.13, F.2.14, F.2.15, F.2.16, F.2.17, F.2.18,F.2.19, F.2.20	GAPP Ref 8.1.0 GAPP Ref 8.1.1 GAPP Ref 8.2.1
FS	Facility Security	User Access	FS-02	FS-02.1	Pursuant to local laws, regulations, ethics and contractual constraints are all employment candidates, contractors and third parties subject to background verification?	Yes			45 CFR 164.310(a)(1) (New) 45 CFR 164.310(a)(2)(ii) (New) 45 CFR 164.310(b) (New) 45 CFR 164.310 (c) (New)	A.9.1.1 A.9.1.2	NIST SP800-53 R3 PE-2 NIST SP800-53 R3 PE-3 NIST SP800-53 R3 PE-4 NIST SP800-53 R3 PE-5 NIST SP800-53 R3 PE-6	NIST SP800-53 R3 PE-2 NIST SP800-53 R3 PE-2 (1) NIST SP800-53 R3 PE-3 NIST SP800-53 R3 PE-4 NIST SP800-53 R3 PE-5 NIST SP800-53 R3 PE-6 NIST SP800-53 R3 PE-6 (1)	PCI DSS v2.0 9.1	AUP v5.0 H.6 SIG v6.0: F.1.2.3, F.1.2.4, F.1.2.5, F.1.2.6, F.1.2.8, F.1.2. 9, F.1.2.10, F.1.2.11, F.1.2.12, F.1.2.13, F.1.2.14, F.1.2.15, F.1.2.24, F.1.4.2, F1.4.6, F.1.4.7, F.1.7, F.1.8, F.2.13, F.2.14, F.2.15, F.2.16, F.2.17, F.2.18	GAPP Ref 8.2.1 GAPP Ref 8.2.2 GAPP Ref 8.2.3
FS	Facility Security	Controlled Access Points	FS-03	FS-03.1	Are physical security perimeters (fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks and security patrols) implemented?	Yes		COBIT 4.1 DS 12.3		A.9.1.1	NIST SP800-53 R3 PE-2 NIST SP800-53 R3 PE-3 NIST SP800-53 R3 PE-6 NIST SP800-53 R3 PE-18	NIST SP800-53 R3 PE-2 NIST SP800-53 R3 PE-2 (1) NIST SP800-53 R3 PE-3 NIST SP800-53 R3 PE-6 NIST SP800-53 R3 PE-6 (1) NIST SP800-53 R3 PE-18	PCI DSS v2.0 9.1		GAPP Ref 8.2.3
FS	Facility Security	Secure Area Authorization	FS-04	FS-04.1	Do you allow tenants to specify which of your geographic locations their data is allowed to traverse into/out of (to address legal jurisdictional considerations based on where data is stored vs. accessed)?	No	After a user is authenticated, the user can access data anywhere through a browser with Internet access. Also, certain data may be transmitted via email and retreived anywhere with internet access.	DS 12.2, DS 12.3		A.9.1.1 A.9.1.2	NIST SP800-53 R3 PE-2 NIST SP800-53 R3 PE-3 NIST SP800-53 R3 PE-6 NIST SP800-53	NIST SP800-53 R3 PE-2 NIST SP800-53 R3 PE-2 (1) NIST SP800-53 R3 PE-3 NIST SP800-53	PCI DSS v2.0 9.1 PCI DSS v2.0 9.1.1 PCI DSS v2.0 9.1.2 PCI DSS v2.0 9.1.3		GAPP Ref 8.2.3
FS	Facility Security	Unauthorized Persons Entry	FS-05	FS-05.1	Are ingress and egress points such as service areas and other points where unauthorized personnel may enter the premises monitored, controlled and isolated from data storage and process?	Yes		COBIT 4.1 DS 12.3		A.9.1.6	NIST SP800-53 R3 PE-7 NIST SP800-53 R3 PE-16 NIST SP800-53 R3 PE-18	NIST SP800-53 R3 PE-7 NIST SP800-53 R3 PE-7 (1) NIST SP800-53 R3 PE-16 NIST SP800-53 R3 PE-18			GAPP Ref 8.2.3
FS	Facility Security	Offsite Authorization	FS-06	FS-06.1	Do you provide tenants with documentation that describes scenarios where data may be moved from one physical location to another? (ex. Offsite backups, business continuity failovers, replication)	Yes			45 CFR 164.310 (d)(1) (New)	A.9.2.7 A.10.1.2	NIST SP800-53 R3 MA-1 NIST SP800-53 R3 MA-2 NIST SP800-53 R3 PE-16	NIST SP800-53 R3 MA-1 NIST SP800-53 R3 MA-2 NIST SP800-53 R3 MA-2 (1) NIST SP800-53 R3 PE-16	PCI DSS v2.0 9.8 PCI DSS v2.0 9.9	AUP v5.0 G.21 SIG v6.0:F.2.18	GAPP Ref 8.2.5 GAPP Ref 8.2.6

FS	Facility Security	Offsite equipment	FS-07	FS-07.1	Do you provide tenants with documentation describing your policies and procedures governing asset management and repurposing of equipment?	Yes			45 CFR 164.310 (c) 45 CFR 164.310 (d)(1) (New) 45 CFR 164.310 (d)(2)(i) (New)	A.9.2.5 A.9.2.6	NIST SP800-53 R3 AC-17 NIST SP800-53 R3 MA-1 NIST SP800-53 R3 PE-1 NIST SP800-53 R3 PE-16 NIST SP800-53 R3 PE-17		PCI DSS v2.0 9.8 PCI DSS v2.0 9.9 PCI DSS v2.0 9.10	SIG v6.0:F.2.18, F.2.19,	
FS	Facility Security	Asset Management	FS-08	FS-08.1	Do you maintain a complete inventory of all of your critical assets which includes ownership of the asset?	Yes			45 CFR 164.310 (d)(2)(iii)	A.7.1.1 A.7.1.2	NIST SP800-53 R3 CM-8	NIST SP800-53 R3 CM-8	PCI DSS v2.0 9.9.1	AUP v5.0 D.1 SIG v6.0: D.1.1,	
FS	Facility Security		FS-08	FS-08.2	Do you maintain a complete inventory of all of your critical supplier relationships?	Yes			45 CFR 164.310 (d)(2)(iii)	A.7.1.1 A.7.1.2	NIST SP800-53 R3 CM-8	NIST SP800-53 R3 CM-8	PCI DSS v2.0 9.9.1	AUP v5.0 D.1 SIG v6.0: D.1.1,	
HR	Human Resources														
HR	Human Resources Security	Background Screening	HR-01	HR-01.1	Pursuant to local laws, regulations, ethics and contractual constraints are all employment candidates, contractors and third parties subject to background verification?	Yes		COBIT 4.1 PO 7.6		A.8.1.2	NIST SP800-53 R3 PS-2 NIST SP800-53 R3 PS-3	NIST SP800-53 R3 PS-2 NIST SP800-53 R3 PS-3	PCI DSS v2.0 12.7 PCI DSS v3.0 12.8.3	AUP v5.0 E.2 SIG v6.0: E.2	GAPP Ref 1.2.9
HR	Human Resources Security	Employment Agreements	HR-02	HR-02.1	Do you specifically train your employees regarding their role vs. the tenant's role in providing information security controls?	Yes		COBIT DS 2.1	45 CFR 164.310(a)(1)	A.6.1.5 A.8.1.3	NIST SP800-53 R3 PL-4	NIST SP800-53 R3 PL-4	PCI DSS v2.0 12.4	AUP v5.0 C.1 SIG v6.0: E.3.5	GAPP Ref 1.2.9 GAPP Ref 8.2.6
			HR-02	HR-02.2	Do you document employee acknowledgment of training they have completed?	Yes		COBIT DS 2.1	45 CFR 164.310(a)(1)	A.6.1.5 A.8.1.3	NIST SP800-53 R3 PL-4	NIST SP800-53 R3 PL-4	PCI DSS v2.0 12.4	AUP v5.0 C.1 SIG v6.0: E.3.5	GAPP Ref 1.2.9 GAPP Ref 8.2.6
HR	Human Resources Security	Employment Termination	HR-03	HR-03.1	Are Roles and responsibilities for following performing employment termination or change in employment procedures assigned, documented and communicated?	Yes		COBIT 4.1 PO 7.8	45 CFR 164.308 (a)(3)(i)(C)	A.8.3.1	NIST SP800-53 R3 PS-4 NIST SP800-53 R2 PS-5	NIST SP800-53 R3 PS-4 NIST SP800-53 R3 PS-5		SIG v6.0: E.6	GAPP Ref 8.2.2 GAPP Ref 10.2.5
IS	Information														
IS	Information Security	Management Program	IS-01	IS-01.1	Do you provide tenants with documentation describing your Information Security Management Program (ISMP)?	Yes		COBIT 4.1 R2 DS5.2 COBIT 4.1 R2 DS5.5	45 CFR 164.308(a)(1)(i) 45 CFR 164.308(a)(1)(ii)(B) 45 CFR 164.316(b)(1)(i) 45 CFR 164.308(a)(3)(i) (New) 45 CFR 164.306(a) (New)	Clause 4.2 Clause 5 A.6.1.1 A.6.1.2 A.6.1.3 A.6.1.4 A.6.1.5 A.6.1.6 A.6.1.7 A.6.1.8	NIST SP800-53 R3 PM-1 NIST SP800-53 R3 PM-2 NIST SP800-53 R3 PM-3 NIST SP800-53 R3 PM-4 NIST SP800-53 R3 PM-5 NIST SP800-53 R3 PM-6 NIST SP800-53 R3 PM-7 NIST SP800-53 R3 PM-8 NIST SP800-53 R3 PM-9 NIST SP800-53 R3 PM-10 NIST SP800-53 R3 PM-11	NIST SP800-53 R3 PM-1 NIST SP800-53 R3 PM-2 NIST SP800-53 R3 PM-3 NIST SP800-53 R3 PM-4 NIST SP800-53 R3 PM-5 NIST SP800-53 R3 PM-6 NIST SP800-53 R3 PM-7 NIST SP800-53 R3 PM-8 NIST SP800-53 R3 PM-9 NIST SP800-53 R3 PM-10 NIST SP800-53 R3 PM-11	PCI DSS v2.0 12.1 PCI DSS v2.0 12.2	SIG v6.0: A.1, B.1	GAPP Ref 8.2.1
IS	Information Security	Management Support / Involvement	IS-02	IS-02.1	Are policies in place to ensure executive and line management take formal action to support information security through clear documented direction, commitment, explicit assignment and verification of assignment execution?	Yes		COBIT 4.1 DS5.1	45 CFR 164.316 (b)(2)(ii) 45 CFR 164.316 (b)(2)(iii)	Clause 5 A.6.1.1	NIST SP800-53 R3 CM-1 NIST SP800-53 R3 PM-1 NIST SP800-53 R3 PM-11	NIST SP800-53 R3 CM-1 NIST SP800-53 R3 PM-1 NIST SP800-53 R3 PM-11	PCI DSS v2.0 12.5	SIG v6.0: C.1	GAPP Ref 8.2.1
IS	Information Security	Policy	IS-03	IS-03.1	Do your information security and privacy policies align with particular industry standards (ISO-27001, ISO-22307, CoBIT, etc.)?	Yes	We align with these standards and best practices for the industry which are validated with our annual audit.	COBIT 4.1 DS5.2	45 CFR 164.316 (a) 45 CFR 164.316 (b)(1)(i)	Clause 4.2.1 Clause 5 A.5.1.1 A.8.2.2			PCI DSS v2.0 12.1 PCI DSS v2.0 12.2	SIG v6.0:B.1	GAPP Ref 8.1.0 GAPP Ref 8.1.1
Can you provide				IS-03.2	Do you have agreements which ensure your providers adhere to your information security and privacy policies?	Yes									
				IS-03.3	Can you provide evidence of due diligence mapping of your controls, architecture and processes to regulations and/or standards?	Yes	Our controls are discussed in our SSAE 16 document.								
IS	Information Security	Baseline Requirements	IS-04	IS-04.1	Do you have documented information security baselines for every component of your infrastructure (ex. Hypervisors, operating systems, routers, DNS servers, etc.)?	Yes		COBIT 4.1 AI2.1 COBIT 4.1 AI2.2 COBIT 4.1 AI3.3		A.12.1.1 A.15.2.2	NIST SP800-53 R3 CM-2 NIST SP800-53	NIST SP800-53 R3 CM-2 NIST SP800-53	PCI DSS v1.2 1.1 PCI DSS v1.2 1.1.1	AUP v5.0 L.2 SIG v6.0: L.2, L.5, L.7 L.8, L.9,	GAPP Ref 1.2.6 GAPP Ref 8.2.1 GAPP Ref 8.2.7
IS	Information Security		IS-04	IS-04.2	Do you have a capability to continuously monitor and report the compliance of your infrastructure against your information security baselines?	Yes		COBIT 4.1 AI2.1 COBIT 4.1 AI2.2 COBIT 4.1 AI3.3		A.12.1.1 A.15.2.2	NIST SP800-53 R3 CM-2 NIST SP800-53	NIST SP800-53 R3 CM-2 NIST SP800-53	PCI DSS v1.2 1.1 PCI DSS v1.2 1.1.1	AUP v5.0 L.2 SIG v6.0: L.2, L.5, L.7 L.8, L.9,	GAPP Ref 1.2.6 GAPP Ref 8.2.1 GAPP Ref 8.2.7

IS	Information Security		IS-04	IS-04.3	Do you allow your clients to provide their own trusted virtual machine image to ensure conformance to their own internal standards?	No	We have standard, proprietary images that we use for our application services. These are designed, engineered, and tested to meet our specific application requirements.	COBIT 4.1 AI2.1 COBIT 4.1 AI2.2 COBIT 4.1 AI3.3 COBIT 4.1 DS2.3 COBIT 4.1 DS11.6		A.12.1.1 A.15.2.2	NIST SP800-53 R3 CM-2 NIST SP800-53 R3 SA-2 NIST SP800-53 R3 SA-4	NIST SP800-53 R3 CM-2 NIST SP800-53 R3 CM-2 (1) NIST SP800-53 R3 CM-2 (3)	PCI DSS v1.2 1.1 PCI DSS v1.2 1.1.1 PCI DSS v1.2 1.1.2 PCI DSS v1.2	AUP v5.0 L.2 SIG v6.0: L.2, L.5, L.7 L.8, L.9, L.10	GAPP Ref 1.2.6 GAPP Ref 8.2.1 GAPP Ref 8.2.7
IS	Information Security	Policy Reviews	IS-05	IS-05.1	Do you notify your tenants when you make material changes to your information security and/or privacy policies?	Yes		COBIT 4.1 DS 5.2 DS 5.4	45 CFR 164.316 (b)(2)(iii) 45 CFE 164.306(e) (New)	Clause 4.2.3 f) A.5.1.2			PCI DSS v2.0 12.1.3	AUP v5.0 B.2 SIG v6.0: B.1.33. B.1.34,	GAPP Ref 1.2.1 GAPP Ref 8.2.7 GAPP Ref 10.2.3
IS	Information Security	Policy Enforcement	IS-06	IS-06.1	Is a formal disciplinary or sanction policy established for employees who have violated security policies and procedures?	Yes		COBIT 4.1 PO 7.7	45 CFR 164.308 (a)(1)(ii)(C)	A.8.2.3	NIST SP800-53 R3 PL-4	NIST SP800-53 R3 PL-4		SIG v6.0:B.1.5	GAPP Ref 10.2.4
IS	Information Security		IS-06	IS-06.2	Are employees made aware of what action might be taken in the event of a violation and stated as such in the policies and procedures?	Yes		COBIT 4.1 PO 7.7	45 CFR 164.308 (a)(1)(ii)(C)	A.8.2.3	NIST SP800-53 R3 PL-4 NIST SP800-53	NIST SP800-53 R3 PL-4 NIST SP800-53		SIG v6.0:B.1.5	GAPP Ref 10.2.4
IS	Information Security	User Access Policy	IS-07	IS-07.1	Do you have controls in place ensuring timely removal of systems access which is no longer required for business purposes?	Yes		COBIT 4.1 DS 5.4	45 CFR 164.308 (a)(3)(i)	A.11.1.1 A.11.2.1	NIST SP800-53 R3 AC-1	NIST SP800-53 R3 AC-1	PCI DSS v2.0 3.5.1	AUP v5.0 B.1 SIG v6.0: B.1.8,	GAPP Ref 8.1.0
IS	Information Security		IS-07	IS-07.2	Do you provide metrics which track the speed with which you are able to remove systems access which is no longer required for business purposes?	Yes		COBIT 4.1 DS 5.4	45 CFR 164.308 (a)(3)(i) 45 CFR 164.312	A.11.1.1 A.11.2.1 A.11.2.4	NIST SP800-53 R3 AC-1 NIST SP800-53	NIST SP800-53 R3 AC-1 NIST SP800-53	PCI DSS v2.0 3.5.1 PCI DSS v2.0	AUP v5.0 B.1 SIG v6.0: B.1.8, B.1.21, B.1.28,	GAPP Ref 8.1.0
IS	Information Security	User Access	IS-08	IS-08.1	Do you document how you grant and approve access to tenant data?	Yes		COBIT 4.1 DS5.4	45 CFR 164.308 (a)(3)(i)	A.11.2.1	NIST SP800-53 R3 AC-3		PCI DSS v2.0 7.1	SIG v6.0: H.2.4, H.2.5,	GAPP Ref 8.2.2
IS	Information Security		IS-08	IS-08.2	Do you have a method of aligning provider and tenant data classification methodologies for access control purposes?	No	Tenents are not provided direct access to their data. Data would be delivered upon request in a manner that meets or exceeds tenant's requirements.	COBIT 4.1 DS5.4	45 CFR 164.308 (a)(3)(i) 45 CFR 164.308 (a)(3)(ii)(A) 45 CFR 164.308	A.11.2.1 A.11.2.2 A.11.4.1 A 11.4.2 A.11.6.1	NIST SP800-53 R3 AC-5 NIST SP800-53		PCI DSS v2.0 7.1 PCI DSS v2.0 7.1.1 PCI DSS v2.0 7.1.2	SIG v6.0: H.2.4, H.2.5,	GAPP Ref 8.2.2
IS	Information Security	User Access Revocation	IS-09	IS-09.1	Is timely deprovisioning, revocation or modification of user access to the organizations systems, information assets and data implemented upon any change in status of employees, contractors, customers, business partners or third parties?	Yes		COBIT 4.1 DS 5.4	45 CFR 164.308(a)(3)(ii)(C)	ISO/IEC 27001:2005 A.8.3.3 A.11.1.1	NIST SP800-53 R3 AC-2 NIST SP800-53 R3 PS-4	NIST SP800-53 R3 AC-2 NIST SP800-53 R3 AC-2 (1)	PCI DSS v2.0 8.5.4 PCI DSS v2.0 8.5.5	AUP v5.0 H.2 SIG v6.0: E.6.2, E.6.3	GAPP Ref 8.2.1
IS	Information Security		IS-09	IS-09.2	Is any change in status intended to include termination of employment, contract or agreement, change of employment or transfer within the organization?	Yes		COBIT 4.1 DS 5.4	45 CFR 164.308(a)(3)(ii)(C)	ISO/IEC 27001:2005 A.8.3.3	NIST SP800-53 R3 AC-2 NIST SP800-53	NIST SP800-53 R3 AC-2 NIST SP800-53	PCI DSS v2.0 8.5.4 PCI DSS v2.0	AUP v5.0 H.2 SIG v6.0: E.6.2, E.6.3	GAPP Ref 8.2.1
IS	Information Security	User Access Reviews	IS-10	IS-10.1	Do you require at least annual certification of entitlements for all system users and administrators (exclusive of users maintained by your tenants)?	Yes		COBIT 4.1 DS5.3 COBIT 4.1 DS5.4	45 CFR 164.308 (a)(3)(ii)(B) 45 CFR 164.308	A.11.2.4	NIST SP800-53 R3 AC-2 NIST SP800-53			SIG v6.0:H.2.6, H.2.7, H.2.9,	GAPP Ref 8.2.1 GAPP Ref 8.2.7
IS	Information Security		IS-10	IS-10.2	If users are found to have inappropriate entitlements, are all remediation and certification actions recorded?	Yes		COBIT 4.1 DS5.3 COBIT 4.1 DS5.4	45 CFR 164.308 (a)(3)(ii)(B)	A.11.2.4	NIST SP800-53 R3 AC-2			SIG v6.0:H.2.6, H.2.7, H.2.9,	GAPP Ref 8.2.1 GAPP Ref 8.2.7
IS	Information Security		IS-10	IS-10.3	Will you share user entitlement remediation and certification reports with your tenants, if inappropriate access may have been allowed to tenant data?	Yes		COBIT 4.1 DS5.3 COBIT 4.1 DS5.4	45 CFR 164.308 (a)(3)(ii)(B) 45 CFR 164.308	A.11.2.4	NIST SP800-53 R3 AC-2 NIST SP800-53			SIG v6.0:H.2.6, H.2.7, H.2.9,	GAPP Ref 8.2.1 GAPP Ref 8.2.7
IS	Information Security	Training / Awareness	IS-11	IS-11.1	Do you provide or make available a formal security awareness training program for cloud-related access and data management issues (i.e., multi-tenancy, nationality, cloud delivery model segregation of duties implications, and conflicts of interest) for all persons with access to tenant data?	Yes		COBIT 4.1 PO 7.4	45 CFR 164.308 (a)(5)(i) 45 CFR 164.308 (a)(5)(ii)(A)	Clause 5.2.2 A.8.2.2	NIST SP800-53 R3 AT-1 NIST SP800-53 R3 AT-2 NIST SP800-53 R3 AT-3 NIST SP800-53 R3 AT-4	NIST SP800-53 R3 AT-1 NIST SP800-53 R3 AT-2 NIST SP800-53 R3 AT-3 NIST SP800-53 R3 AT-4	PCI DSS v2.0 12.6 PCI DSS v2.0 12.6.1 PCI DSS v2.0 12.6.2	AUP v5.0 E.1 SIG v6.0:E.4	GAPP Ref 1.2.10 GAPP Ref 8.2.1
IS	Information Security		IS-11	IS-11.2	Are administrators and data stewards properly educated on their legal responsibilities with regard to security and data integrity?	Yes		COBIT 4.1 PO 7.4	45 CFR 164.308 (a)(5)(i)	Clause 5.2.2 A.8.2.2	NIST SP800-53 R3 AT-1	NIST SP800-53 R3 AT-1	PCI DSS v2.0 12.6	AUP v5.0 E.1 SIG v6.0:E.4	GAPP Ref 1.2.10
IS	Information Security	Industry Knowledge / Benchmarking	IS-12	IS-12.1	Do you participate in industry groups and professional associations related to information security?	Yes				A.6.1.7	NIST SP800-53 R3 AT-5 NIST SP800-53	NIST SP800-53 R3 AT-5 NIST SP800-53		SIG v6.0:C.1.8	
IS			IS-12	IS-12.2	Do you benchmark your security controls against industry standards?	Yes				A.6.1.7				SIG v6.0:C.1.8	
IS	Information Security	Roles / Responsibilities	IS-13	IS-13.1	Do you provide tenants with a role definition document clarifying your administrative responsibilities vs. those of the tenant?	Yes		COBIT 4.1 DS5.1		Clause 5.1 c) A.6.1.2 A.6.1.3	NIST SP800-53 R3 AT-3 NIST SP800-53	NIST SP800-53 R3 AT-3 NIST SP800-53		AUP v5.0 B.1 SIG v6.0: B.1.5, D.1.1,D.1.3.3,	GAPP Ref 1.2.9 GAPP Ref 8.2.1

IS	Information Security	Management Oversight	IS-14	IS-14.1	Are Managers responsible for maintaining awareness of and complying with security policies, procedures and standards that are relevant to their area of responsibility?	Yes		COBIT 4.1 DS5.3 COBIT 4.1 DS5.4 COBIT 4.1 DS5.5		Clause 5.2.2 A.8.2.1 A.8.2.2 A 11.2.4 A.15.2.1	NIST SP800-53 R3 AT-2 NIST SP800-53 R3 AT-3 NIST SP800-53 R3 CA-1 NIST SP800-53 R3 CA-5 NIST SP800-53 R3 CA-6 NIST SP800-53 R3 CA-7 NIST SP800-53 R3 PM-10	NIST SP800-53 R3 AT-2 NIST SP800-53 R3 AT-3 NIST SP800-53 R3 CA-1 NIST SP800-53 R3 CA-5 NIST SP800-53 R3 CA-6 NIST SP800-53 R3 CA-7 NIST SP800-53 R3 CA-7 (2) NIST SP800-53 R3 PM-10	PCI DSS v2.0 12.6.1 PCI DSS v2.0 12.6.2	AUP v5.0 E.1 SIG v6.0: E.4	GAPP Ref 1.1.2 GAPP Ref 8.2.1
IS	Information Security	Segregation of Duties	IS-15	IS-15.1	Do you provide tenants with documentation on how you maintain segregation of duties within your cloud service offering?	Yes		COBIT 4.1 DS 5.4	45 CFR 164.308 (a)(1)(ii)(D) 45 CFR 164.308 (a)(3)(ii)(A) 45 CFR 164.308(a)(4)(ii)(A) (New) 45 CFR 164.308 (a)(5)(ii)(C) 45 CFR 164.312 (b)	A.10.1.3	NIST SP800-53 R3 AC-1 NIST SP800-53 R3 AC-2 NIST SP800-53 R3 AC-5 NIST SP800-53 R3 AC-6 NIST SP800-53 R3 AU-1 NIST SP800-53 R3 AU-6 NIST SP800-53 R3 SI-1 NIST SP800-53 R3 SI-4		PCI DSS v2.0 6.4.2	SIG v6.0:G.2.13. G.3, G.20.1, G.20.2, G.20.5	GAPP Ref 8.2.2
IS	Information Security	User Responsibility	IS-16	IS-16.1	Are users made aware of their responsibilities for maintaining awareness and compliance with published security policies, procedures, standards and applicable regulatory requirements?	Yes		COBIT 4.1 PO 4.6	45 CFR 164.308 (a)(5)(ii)(D)	Clause 5.2.2 A.8.2.2 A.11.3.1	NIST SP800-53 R3 AT-2 NIST SP800-53	NIST SP800-53 R3 AT-2 NIST SP800-53	PCI DSS v2.0 8.5.7 PCI DSS v2.0	AUP v5.0 E.1 SIG v6.0: E.4	GAPP Ref 1.2.10 GAPP Ref 8.2.1
IS	Information Security		IS-16	IS-16.2	Are users made aware of their responsibilities for maintaining a safe and secure working environment?	Yes		COBIT 4.1 PO 4.6	45 CFR 164.308 (a)(5)(ii)(D)	Clause 5.2.2 A.8.2.2	NIST SP800-53 R3 AT-2	NIST SP800-53 R3 AT-2	PCI DSS v2.0 8.5.7	AUP v5.0 E.1 SIG v6.0: E.4	GAPP Ref 1.2.10
IS	Information Security		IS-16	IS-16.3	Are users made aware of their responsibilities for leaving unattended equipment in a secure manner?	Yes		COBIT 4.1 PO 4.6	45 CFR 164.308 (a)(5)(ii)(D)	Clause 5.2.2 A.8.2.2	NIST SP800-53 R3 AT-2	NIST SP800-53 R3 AT-2	PCI DSS v2.0 8.5.7	AUP v5.0 E.1 SIG v6.0: E.4	GAPP Ref 1.2.10
IS	Information Security	Workspace	IS-17	IS-17.1	Do your data management policies and procedures address tenant and service level conflicts of interests?	Yes	This control will likely have a new name in v2.0.			Clause 5.2.2 A.8.2.2	NIST SP800-53 R3 AC-11	NIST SP800-53 R3 AC-11		AUP v5.0 E.1 SIG v6.0: E.4	GAPP Ref 8.2.3
IS	Information Security		IS-17	IS-17.2	Do your data management policies and procedures include a tamper audit or software integrity function for unauthorized access to tenant data?	Yes				Clause 5.2.2 A.8.2.2 A.9.1.5	NIST SP800-53 R3 AC-11 NIST SP800-53	NIST SP800-53 R3 AC-11 NIST SP800-53		AUP v5.0 E.1 SIG v6.0: E.4	GAPP Ref 8.2.3
IS	Information Security		IS-17	IS-17.3	Does the virtual machine management infrastructure include a tamper audit or software integrity function to detect changes to the build/configuration of the virtual machine?	Yes				Clause 5.2.2 A.8.2.2 A.9.1.5	NIST SP800-53 R3 AC-11 NIST SP800-53	NIST SP800-53 R3 AC-11 NIST SP800-53		AUP v5.0 E.1 SIG v6.0: E.4	GAPP Ref 8.2.3
IS	Information Security	Encryption	IS-18	IS-18.1	Do you have a capability to allow creation of unique encryption keys per tenant?	Yes		COBIT 4.1 DS5.8 COBIT 4.1 DS5.10	45 CFR 164.312 (a)(2)(iv)	A.10.6.1 A.10.8.3	NIST SP800-53 R3 AC-18		PCI-DSS v2.0 2.1.1		GAPP Ref 8.1.1 GAPP Ref 8.2.1
IS	Information Security		IS-18	IS-18.2	Do you support tenant generated encryption keys or permit tenants to encrypt data to an identity without access to a public key certificate. (e.g. identity based encryption)?	No	Encryption is handled by our internal staff.	COBIT 4.1 DS5.8 COBIT 4.1 DS5.10 COBIT 4.1 DS5.11	45 CFR 164.312 (a)(2)(iv) 45 CFR 164.312	A.10.6.1 A.10.8.3 A.10.8.4	NIST SP800-53 R3 AC-18 NIST SP800-53		PCI-DSS v2.0 2.1.1 PCI-DSS v2.0		GAPP Ref 8.1.1 GAPP Ref 8.2.1 GAPP Ref 8.2.5
IS	Information Security	Encryption Key Management	IS-19	IS-19.1	Do you encrypt tenant data at rest (on disk/storage) within your environment?	Yes		COBIT 4.1 DS5.8	45 CFR 164.312 (a)(2)(iv)	Clause 4.3.3 A.10.7.3	NIST SP800-53 R3 SC-12	NIST SP800-53 R3 SC-12	PCI-DSS v2.0 3.4.1	SIG v6.0: L.6	GAPP Ref 8.1.1 GAPP Ref 8.2.1
IS	Information Security		IS-19	IS-19.2	Do you leverage encryption to protect data and virtual machine images during transport across and between networks and hypervisor instances?	No	However, through our replication technology and our private, dedicated point-to-point connection, we are able to protect any data or VM in motion between networks.	COBIT 4.1 DS5.8	45 CFR 164.312 (a)(2)(iv) 45 CFR 164.312(e)(1) (New)	Clause 4.3.3 A.10.7.3 A.12.3.2 A.15.1.6	NIST SP800-53 R3 SC-12 NIST SP800-53 R3 SC-13 NIST SP800-53 R3 SC-17	NIST SP800-53 R3 SC-12 NIST SP800-53 R3 SC-12 (2) NIST SP800-53 R3 SC-12 (5)	PCI-DSS v2.0 3.4.1 PCI-DSS v2.0 3.5 PCI-DSS v2.0 3.5.1	SIG v6.0: L.6	GAPP Ref 8.1.1 GAPP Ref 8.2.1 GAPP Ref 8.2.5
IS	Information Security		IS-19	IS-19.3	Do you have a capability to manage encryption keys on behalf of tenants?	Yes		COBIT 4.1 DS5.8	45 CFR 164.312 (a)(2)(iv)	Clause 4.3.3 A.10.7.3	NIST SP800-53 R3 SC-12	NIST SP800-53 R3 SC-12	PCI-DSS v2.0 3.4.1	SIG v6.0: L.6	GAPP Ref 8.1.1 GAPP Ref 8.2.1
IS	Information Security		IS-19	IS-19.4	Do you maintain key management procedures?	Yes		COBIT 4.1 DS5.8	45 CFR 164.312	Clause 4.3.3	NIST SP800-53	NIST SP800-53	PCI-DSS v2.0	SIG v6.0: L.6	GAPP Ref 8.1.1
IS	Information Security	Vulnerability / Patch Management	IS-20	IS-21.1	Do you conduct network-layer vulnerability scans regularly as prescribed by industry best practices?	Yes		COBIT 4.1 AI6.1 COBIT 4.1 AI3.3	45 CFR 164.308 (a)(1)(i)(ii)(A)	A.12.5.1 A.12.5.2	NIST SP800-53 R3 CM-3		PCI-DSS v2.0 2.2	AUP v5.0 I.4 SIG v6.0:	GAPP Ref 1.2.6 GAPP Ref 8.2.7
IS	Information Security		IS-20	IS-20.2	Do you conduct application-layer vulnerability scans regularly as prescribed by industry best practices?	Yes		COBIT 4.1 AI6.1 COBIT 4.1 AI3.3	45 CFR 164.308 (a)(1)(i)(ii)(A)	A.12.5.1 A.12.5.2	NIST SP800-53 R3 CM-3		PCI-DSS v2.0 2.2	AUP v5.0 I.4 SIG v6.0:	GAPP Ref 1.2.6 GAPP Ref 8.2.7
IS	Information Security		IS-20	IS-20.3	Do you conduct local operating system-layer vulnerability scans regularly as prescribed by industry best practices?	Yes		COBIT 4.1 AI6.1 COBIT 4.1 AI3.3	45 CFR 164.308 (a)(1)(i)(ii)(A)	A.12.5.1 A.12.5.2	NIST SP800-53 R3 CM-3		PCI-DSS v2.0 2.2	AUP v5.0 I.4 SIG v6.0:	GAPP Ref 1.2.6 GAPP Ref 8.2.7
IS	Information Security		IS-20	IS-20.4	Will you make the results of vulnerability scans available to tenants at their request?	Yes		COBIT 4.1 AI6.1 COBIT 4.1 AI3.3	45 CFR 164.308 (a)(1)(i)(ii)(A)	A.12.5.1 A.12.5.2	NIST SP800-53 R3 CM-3		PCI-DSS v2.0 2.2	AUP v5.0 I.4 SIG v6.0:	GAPP Ref 1.2.6 GAPP Ref 8.2.7
IS	Information Security		IS-20	IS-20.5	Do you have a capability to rapidly patch vulnerabilities across all of your computing devices, applications, and systems?	Yes		COBIT 4.1 AI6.1 COBIT 4.1 AI3.3	45 CFR 164.308 (a)(1)(i)(ii)(A)	A.12.5.1 A.12.5.2	NIST SP800-53 R3 CM-3		PCI-DSS v2.0 2.2	AUP v5.0 I.4 SIG v6.0:	GAPP Ref 1.2.6 GAPP Ref 8.2.7
IS	Information Security		IS-20	IS-20.6	Will you provide your risk-based systems patching timeframes to your tenants upon request?	Yes		COBIT 4.1 AI6.1 COBIT 4.1 AI3.3	45 CFR 164.308 (a)(1)(i)(ii)(A)	A.12.5.1 A.12.5.2	NIST SP800-53 R3 CM-3		PCI-DSS v2.0 2.2	AUP v5.0 I.4 SIG v6.0:	GAPP Ref 1.2.6 GAPP Ref 8.2.7

IS	Information Security	Antivirus / Malicious Software	IS-21	IS-21.1	Do you have anti-malware programs installed on all systems which support your cloud service offerings?	Yes		COBIT 4.1 DS5.9	45 CFR 164.308 (a)(5)(ii)(B)	A.10.4.1	NIST SP800-53 R3 SA-7	NIST SP800-53 R3 SA-7	PCI-DSS v2.0 5.1	SIG v6.0:G.7	GAPP Ref 8.2.2
IS	Information Security		IS-21	IS-21.2	Do you ensure that security threat detection systems which use signatures, lists, or behavioral patterns are updated across all infrastructure components within industry accepted timeframes?	Yes		COBIT 4.1 DS5.9	45 CFR 164.308 (a)(5)(ii)(B)	A.10.4.1	NIST SP800-53 R3 SA-7 NIST SP800-53	NIST SP800-53 R3 SA-7 NIST SP800-53	PCI-DSS v2.0 5.1 PCI-DSS v2.0	SIG v6.0:G.7	GAPP Ref 8.2.2
IS	Information Security	Incident	IS-22	IS-22.1	Do you have a documented security incident response plan?	Yes		COBIT 4.1 DS5.6	45 CFR 164.308	Clause 4.3.3	NIST SP800-53	NIST SP800-53	PCI-DSS v2.0	AUP v5.0 J.1	GAPP Ref 1.2.4
IS	Information Security		IS-22	IS-22.2	Do you integrate customized tenant requirements into your security incident response plans?	No	We currently do not have customized tenant requirements; however, we would be happy to discuss your specific needs.	COBIT 4.1 DS5.6	45 CFR 164.308 (a)(1)(i) 45 CFR 164.308 (a)(6)(i)	Clause 4.3.3 A.13.1.1 A.13.2.1	NIST SP800-53 R3 IR-1 NIST SP800-53 R3 IR-2	NIST SP800-53 R3 IR-1 NIST SP800-53 R3 IR-2	PCI-DSS v2.0 12.9 PCI-DSS v2.0 12.9.1	AUP v5.0 J.1 SIG v6.0: J.1.1, J.1.2	GAPP Ref 1.2.4 GAPP Ref 1.2.7 GAPP Ref 7.1.2 GAPP Ref 7.2.2
IS	Information Security		IS-22	IS-22.3	Do you publish a roles and responsibilities document specifying what you vs. your tenants are responsible for during security incidents?	Yes		COBIT 4.1 DS5.6	45 CFR 164.308 (a)(1)(i) 45 CFR 164.308	Clause 4.3.3 A.13.1.1 A.13.2.1	NIST SP800-53 R3 IR-1 NIST SP800-53	NIST SP800-53 R3 IR-1 NIST SP800-53	PCI-DSS v2.0 12.9 PCI-DSS v2.0	AUP v5.0 J.1 SIG v6.0: J.1.1, J.1.2	GAPP Ref 1.2.4 GAPP Ref 1.2.7 GAPP Ref 7.1.2
IS	Information Security	Incident Reporting	IS-23	IS-23.1	Does your security information and event management (SIEM) system merge data sources (app logs, firewall logs, IDS logs, physical access logs, etc.) for granular analysis and alerting?	Yes		COBIT 4.1 DS5.6	45 CFR 164.312 (a)(5)(ii) 16 CFR 318.3	Clause 4.3.3 Clause 5.2.2 A.6.1.3	NIST SP800-53 R3 IR-2 NIST SP800-53		PCI-DSS v2.0 12.5.2 PCI-DSS v2.0	AUP v5.0 J.1 AUP v5.0 E.1 SIG v6.0: J.1.1,	GAPP Ref 1.2.7 GAPP Ref 1.2.10
IS	Information Security		IS-23	IS-23.2	Does your logging and monitoring framework allow isolation of an incident to specific tenants?	Yes		COBIT 4.1 DS5.6	45 CFR 164.312 (a)(5)(ii)	Clause 4.3.3 Clause 5.2.2	NIST SP800-53 R3 IR-2		PCI-DSS v2.0 12.5.2	AUP v5.0 J.1 AUP v5.0 E.1	GAPP Ref 1.2.7 GAPP Ref
IS	Information Security	Incident Response Legal Preparation	IS-24	IS-24.1	Does your incident response plan comply with industry standards for legally admissible chain-of-custody management processes & controls?	Yes	This control will likely move to the Legal domain in v2.0.	COBIT 4.1 DS5.6	45 CFR 164.308 (a)(5)(ii)	Clause 4.3.3 Clause 5.2.2 A.8.2.2	NIST SP800-53 R3 AU-6 NIST SP800-53			AUP v5.0 J.1 AUP v5.0 E.1 SIG v6.0: J.1.1,	GAPP Ref 1.2.7
IS	Information Security		IS-24	IS-24.2	Does your incident response capability include the use of legally admissible forensic data collection and analysis techniques?	Yes		COBIT 4.1 DS5.6	45 CFR 164.308 (a)(5)(ii)	Clause 4.3.3 Clause 5.2.2	NIST SP800-53 R3 AU-6			AUP v5.0 J.1 AUP v5.0 E.1	GAPP Ref 1.2.7
IS	Information Security		IS-24	IS-24.3	Are you capable of supporting litigation holds (freeze of data from a specific point in time) for a specific tenant without freezing other tenant data?	Yes		COBIT 4.1 DS5.6	45 CFR 164.308 (a)(5)(ii)	Clause 4.3.3 Clause 5.2.2 A.8.2.2	NIST SP800-53 R3 AU-6 NIST SP800-53			AUP v5.0 J.1 AUP v5.0 E.1 SIG v6.0: J.1.1,	GAPP Ref 1.2.7
IS	Information Security		IS-24	IS-24.4	Do you enforce and attest to tenant data separation when producing data in response to legal subpoenas?	Yes		COBIT 4.1 DS5.6	45 CFR 164.308 (a)(5)(ii)	Clause 4.3.3 Clause 5.2.2	NIST SP800-53 R3 AU-6			AUP v5.0 J.1 AUP v5.0 E.1	GAPP Ref 1.2.7
IS	Information Security	Incident Response Metrics	IS-25	IS-25.1	Do you monitor and quantify the types, volumes, and impacts on all information security incidents?	Yes		COBIT 4.1 DS 4.9	45 CFR 164.308 (a)(1)(ii)(D)	A.13.2.2	NIST SP800-53 R3 IR-4	NIST SP800-53 R3 IR-4	PCI DSS v2.0 12.9.6	SIG v6.0: J.1.2,	GAPP Ref 1.2.7 GAPP Ref
IS	Information Security		IS-25	IS-25.2	Will you share statistical information security incident data with your tenants upon request?	Yes		COBIT 4.1 DS 4.9	45 CFR 164.308 (a)(1)(ii)(D)	A.13.2.2	NIST SP800-53 R3 IR-4	NIST SP800-53 R3 IR-4	PCI DSS v2.0 12.9.6	SIG v6.0: J.1.2,	GAPP Ref 1.2.7 GAPP Ref
IS	Information Security	Acceptable Use	IS-26	IS-26.1	Do you provide documentation regarding how you may utilize or access tenant data and/or metadata?	Yes		COBIT 4.1 DS 5.3	45 CFR 164.310 (b)	A.7.1.3	NIST SP800-53 R3 AC-8	NIST SP800-53 R3 AC-8	PCI-DSS v2.0 12.3.5	AUP v5.0 B.3. SIG v6.0: B.1.7,	GAPP Ref 8.1.0
IS	Information Security		IS-26	IS-26.2	Do you collect or create metadata about tenant data usage through the use of inspection technologies (search engines, etc.)?	Yes		COBIT 4.1 DS 5.3	45 CFR 164.310 (b)	A.7.1.3	NIST SP800-53 R3 AC-8	NIST SP800-53 R3 AC-8	PCI-DSS v2.0 12.3.5	AUP v5.0 B.3. SIG v6.0: B.1.7,	GAPP Ref 8.1.0
IS	Information Security		IS-26	IS-26.3	Do you allow tenants to opt-out of having their data/metadata accessed via inspection technologies?	Yes		COBIT 4.1 DS 5.3	45 CFR 164.310 (b)	A.7.1.3	NIST SP800-53 R3 AC-8	NIST SP800-53 R3 AC-8	PCI-DSS v2.0 12.3.5	AUP v5.0 B.3. SIG v6.0: B.1.7,	GAPP Ref 8.1.0
IS	Information Security	Asset Returns	IS-27	IS-27.1	Are systems in place to monitor for privacy breaches and notify tenants expeditiously if a privacy event may have impacted their data?	Yes			45 CFR 164.308 (a)(3)(ii)(C)	A.7.1.1 A.7.1.2 A.8.3.2	NIST SP800-53 R3 PS-4	NIST SP800-53 R3 PS-4		AUP v5.0 D.1 SIG v6.0: E.6.4	GAPP Ref 5.2.3 GAPP Ref 7.2.2 GAPP Ref 8.2.1
IS	Information Security		IS-27	IS-27.2	Is your Privacy Policy aligned with industry standards?	Yes			45 CFR 164.308	A.7.1.1	NIST SP800-53	NIST SP800-53		AUP v5.0 D.1	GAPP Ref 5.2.3
IS	Information Security	eCommerce Transactions	IS-28	IS-28.1	Do you provide open encryption methodologies (3.4ES, AES, etc.) to tenants in order for them to protect their data if it is required to traverse public networks? (ex. the Internet)	Yes		COBIT 4.1 DS 5.10 5.11	45 CFR 164.312(e)(1) 45 CFR	A.7.2.1 A.10.6.1 A.10.6.2	NIST SP800-53 R3 AC-14 NIST SP800-53		PCI-DSS v2.0 2.1.1 PCI-DSS v2.0		GAPP Ref 3.2.4 GAPP Ref 4.2.3 GAPP Ref 7.1.2
IS	Information Security		IS-28	IS-28.2	Do you utilize open encryption methodologies any time your infrastructure components need to communicate to each other over public networks (ex. Internet-based replication of data from one environment to another)?	Yes		COBIT 4.1 DS 5.10 5.11	45 CFR 164.312(e)(1) 45 CFR 164.312(e)(2)(i)	A.7.2.1 A.10.6.1 A.10.6.2 A.10.9.1	NIST SP800-53 R3 AC-14 NIST SP800-53 R3 AC-21		PCI-DSS v2.0 2.1.1 PCI-DSS v2.0 4.1		GAPP Ref 3.2.4 GAPP Ref 4.2.3 GAPP Ref 7.1.2 GAPP Ref 7.2.1
IS	Information Security	Audit Tools Access	IS-29	IS-29.1	Do you restrict, log, and monitor access to your information security management systems? (Ex. Hypervisors, firewalls, vulnerability scanners, network sniffers, APIs, etc.)	Yes		COBIT 4.1 DS 5.7		A.15.3.2	NIST SP800-53 R3 AU-9 NIST SP800-53 R3 AU-11 NIST SP800-53 R3 AU-14	NIST SP800-53 R3 AU-9 NIST SP800-53 R3 AU-9 (2) NIST SP800-53 R3 AU-11 NIST SP800-53 R3 AU-14	PCI DSS v2.0 10.5.5		GAPP Ref 8.2.1

IS	Information Security	Diagnostic / Configuration Ports Access	IS-30	IS-30.1	Do you utilize dedicated secure networks to provide management access to your cloud service infrastructure?	No	All management is on our private network and is not externally accessible (without the appropriate software and credentials).	COBIT 4.1 DS5.7		A.10.6.1 A.11.1.1 A.11.4.4 A.11.5.4	NIST SP800-53 R3 CM-7 NIST SP800-53 R3 MA-3 NIST SP800-53 R3 MA-4 NIST SP800-53 R3 MA-5	NIST SP800-53 R3 CM-7 NIST SP800-53 R3 CM-7 (1) NIST SP800-53 R3 MA-3 NIST SP800-53 R3 MA-3 (1) NIST SP800-53 R3 MA-3 (2) NIST SP800-53 R3 MA-3 (3) NIST SP800-53 R3 MA-4 NIST SP800-53 R3 MA-4 (1) NIST SP800-53 R3 MA-4 (2) NIST SP800-53 R3 MA-5	PCI-DSS v2.0 9.1.2	SIG v6.0: H1.1, H1.2, G.9.15	
IS	Information Security	Network / Infrastructure	IS-31	IS-31.1	Do you collect capacity and utilization data for all relevant components of your cloud service offering?	Yes		COBIT 4.1 DS5.10		A.6.2.3 A.10.6.2	NIST SP800-53 R3 SC-20	NIST SP800-53 R3 SC-20		AUP v5.0 C.2 SIG v6.0:C.2.6,	GAPP Ref 8.2.2 GAPP Ref 8.2.5
IS	Information Security		IS-31	IS-31.2	Do you provide tenants with capacity planning and utilization reports?	No	We would generate these on an as-needed basis.	COBIT 4.1 DS5.10		A.6.2.3 A.10.6.2	NIST SP800-53 R3 SC-20	NIST SP800-53 R3 SC-20		AUP v5.0 C.2 SIG v6.0:C.2.6,	GAPP Ref 8.2.2 GAPP Ref 8.2.5
IS	Information Security	Portable / Mobile Devices	IS-32	IS-32.1	Are Policies and procedures established and measures implemented to strictly limit access to sensitive data from portable and mobile devices, such as laptops, cell phones, and personal digital assistants (PDAs), which are generally higher-risk than non-portable devices (e.g., desktop computers at the provider organization's facilities)?	Yes		COBIT 4.1 DS5.11 COBIT 4.1 DS5.5	45 CFR 164.310 (d)(1)	A.7.2.1 A.10.7.1 A.10.7.2 A.10.8.3 A.11.7.1 A.11.7.2 A.15.1.4	NIST SP800-53 R3 AC-17 NIST SP800-53 R3 AC-18 NIST SP800-53 R3 AC-19 NIST SP800-53 R3 MP-2 NIST SP800-53 R3 MP-4 NIST SP800-53 R3 MP-6		PCI DSS v2.0 9.7 PCI DSS v2.0 9.7.2 PCI DSS v2.0 9.8 PCI DSS v2.0 9.9 PCI DSS v2.0 11.1 PCI DSS v2.0 12.3	SIG v6.0:G.11, G12, G.20.13, G.20.14	GAPP Ref 1.2.6 GAPP Ref 3.2.4 GAPP Ref 8.2.6
IS	Information Security	Source Code Access Restriction	IS-33	IS-33.1	Are controls in place to prevent unauthorized access to your application, program or object source code, and assure it is restricted to authorized personnel only?	Yes				Clause 4.3.3 A.12.4.3 A.15.1.3	NIST SP800-53 R3 CM-5 NIST SP800-53	NIST SP800-53 R3 CM-5 NIST SP800-53	PCI-DSS v2.0 6.4.1 PCI-DSS v2.0	SIG v6.0: I.2.7.2, I.2.9, I.2.10, I.2.15,	GAPP Ref 1.2.6 GAPP Ref 6.2.1
IS	Information Security		IS-33	IS-33.2	Are controls in place to prevent unauthorized access to tenant application, program or object source code, and assure it is restricted to authorized personnel only?	Yes				Clause 4.3.3 A.12.4.3 A.15.1.3	NIST SP800-53 R3 CM-5 NIST SP800-53	NIST SP800-53 R3 CM-5 NIST SP800-53	PCI-DSS v2.0 6.4.1 PCI-DSS v2.0	SIG v6.0: I.2.7.2, I.2.9, I.2.10, I.2.15,	GAPP Ref 1.2.6 GAPP Ref 6.2.1
IS	Information Security	Utility Programs Access	IS-34	IS-34.1	Are utilities that can significantly manage virtualized partitions (ex. shutdown, clone, etc.) appropriately restricted and monitored?	Yes		COBIT 4.1 DS5.7		A.11.4.1 A 11.4.4	NIST SP800-53 R3 AC-5	NIST SP800-53 R3 AC-5	PCI DSS v2.0 7.1.2	SIG v6.0:H.2.16	
IS	Information Security		IS-34	IS-34.2	Do you have a capability to detect attacks which target the virtual infrastructure directly (ex. shimming, Blue Pill, Hyper Jumping, etc.)?	No	We are working with our partners to develop a solution for these attacks. All machines are only accessible and managed from internal staff to reduce risk.	COBIT 4.1 DS5.7		A.11.4.1 A 11.4.4 A.11.5.4	NIST SP800-53 R3 AC-5 NIST SP800-53 R3 AC-6 NIST SP800-53	NIST SP800-53 R3 AC-5 NIST SP800-53 R3 AC-6 NIST SP800-53	PCI DSS v2.0 7.1.2	SIG v6.0:H.2.16	
IS	Information Security		IS-34	IS-34.3	Are attacks which target the virtual infrastructure prevented with technical controls?	No	We are working with our partners to develop a solution for these attacks. All machines are only accessible and managed from internal staff to reduce risk.	COBIT 4.1 DS5.7		A.11.4.1 A 11.4.4 A.11.5.4	NIST SP800-53 R3 AC-5 NIST SP800-53 R3 AC-6 NIST SP800-53	NIST SP800-53 R3 AC-5 NIST SP800-53 R3 AC-6 NIST SP800-53	PCI DSS v2.0 7.1.2	SIG v6.0:H.2.16	
LG	Legal														
LG	Legal	Nondisclosure Agreements	LG-01	LG-01.1	Are requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details identified, documented and reviewed at planned intervals?	Yes				ISO/IEC 27001:2005 Annex A.6.1.5	NIST SP800-53 R3 PL-4 NIST SP800-53 R3 PS-6 NIST SP800-53 R3 SA-9	NIST SP800-53 R3 PL-4 NIST SP800-53 R3 PS-6 NIST SP800-53 R3 SA-9 NIST SP800-53 R3 SA-9 (1)	PCI DSS v2.0 12.8.2 PCI DSS v2.0 12.8.3 PCI DSS v2.0 12.8.4	SIG v6.0:C.2.5	GAPP Ref 1.2.5
LG	Legal	Third Party Agreements	LG-02	LG-02.1	Do you select and monitor outsourced providers in compliance with laws in the country where the data is processed and stored and transmitted?	Yes		COBIT 4.1 DS5.11		A.6.2.3 A10.2.1 A.10.8.2	NIST SP800-53 R3 CA-3 NIST SP800-53	NIST SP800-53 R3 CA-3 NIST SP800-53	PCI DSS v2.0 2.4 PCI DSS v2.0 12.8.2	AUP v5.0 C.2 SIG v6.0: C.2.4, C.2.6, G.4.1,	GAPP Ref 1.2.5
LG	Legal		LG-02	LG-02.2	Do you select and monitor outsourced providers in compliance with laws in the country where the data originates?	Yes		COBIT 4.1 DS5.11		A.6.2.3 A10.2.1	NIST SP800-53 R3 CA-3	NIST SP800-53 R3 CA-3	PCI DSS v2.0 2.4 PCI DSS v2.0	AUP v5.0 C.2 SIG v6.0: C.2.4,	GAPP Ref 1.2.5
LG	Legal		LG-02	LG-02.3	Does legal counsel review all third party agreements?	Yes		COBIT 4.1 DS5.11		A.6.2.3	NIST SP800-53	NIST SP800-53	PCI DSS v2.0 2.4	AUP v5.0 C.2	GAPP Ref 1.2.5
OP	Operations														

OP	Operations Management	Policy	OP-01	OP-01.1	Are policies and procedures established and made available for all personnel to adequately support services operations roles?	Yes		COBIT 4.1 DS13.1		Clause 5.1 A 8.1.1 A.8.2.1 A 8.2.2 A.10.1.1			PCI DSS v2.0 12.1 PCI DSS v2.0 12.2 PCI DSS v2.0 12.3 PCI DSS v2.0 12.4	SIG v6.0: G.1.1	GAPP Ref 8.2.1
OP	Operations Management	Documentation	OP-02	OP-02.1	Are information system documentation (e.g., administrator and user guides, architecture diagrams, etc.) made available to authorized personnel to ensure Configuring, installing, and operating the information system?	Yes		COBIT 4.1 DS 9, DS 13.1		Clause 4.3.3 A.10.7.4	NIST SP800-53 R3 CP-9 NIST SP800-53 R3 CP-10 NIST SP800-53 R3 SA-5 NIST SP800-53 R3 SA-10 NIST SP800-53 R3 SA-11		PCI DSS v2.0 12.1 PCI DSS v2.0 12.2 PCI DSS v2.0 12.3 PCI DSS v2.0 12.4	SIG v6.0: G.1.1	GAPP Ref 1.2.6
OP	Operations Management	Capacity / Resource Planning	OP-03	OP-03.1	Do you provide documentation regarding what levels of system (network, storage, memory, I/O, etc.) oversubscription you maintain and under what circumstances/scenarios?	Yes		COBIT 4.1 DS 3		A.10.3.1	NIST SP800-53 R3 SA-4	NIST SP800-53 R3 SA-4 NIST SP800-53		SIG v6.0:G.5	GAPP Ref 1.2.4
OP	Operations Management		OP-03	OP-03.2	Do you restrict use of the memory oversubscription capabilities present in the hypervisor?	Yes		COBIT 4.1 DS 3		A.10.3.1	NIST SP800-53 R3 SA-4	NIST SP800-53 R3 SA-4		SIG v6.0:G.5	GAPP Ref 1.2.4
OP	Operations Management	Equipment Maintenance	OP-04	OP-04.1	If using virtual infrastructure, does your cloud solution include hardware independent restore and recovery capabilities?	Yes		COBIT 4.1 A13.3	45 CFR 164.310 (a)(2)(iv)	A.9.2.4	NIST SP800-53 R3 MA-2			SIG v6.0:F.2.19	GAPP Ref 5.2.3 GAPP Ref 8.2.2
OP	Operations Management		OP-04	OP-04.2	If using virtual infrastructure, do you provide tenants with a capability to restore a Virtual Machine to a previous state in time?	Yes		COBIT 4.1 A13.3	45 CFR 164.310 (a)(2)(iv)	A.9.2.4	NIST SP800-53 R3 MA-2			SIG v6.0:F.2.19	GAPP Ref 5.2.3 GAPP Ref 8.2.2
OP	Operations Management		OP-04	OP-04.3	If using virtual infrastructure, do you allow virtual machine images to be downloaded and ported to a new cloud provider?	No	Our virtual machines are proprietary and on a private network. If this request is required, we may discuss options outside the normal scope of an engagement to allow the port to another third party provider.	COBIT 4.1 A13.3	45 CFR 164.310 (a)(2)(iv)	A.9.2.4	NIST SP800-53 R3 MA-2 NIST SP800-53 R3 MA-3 NIST SP800-53 R3 MA-4 NIST SP800-53			SIG v6.0:F.2.19	GAPP Ref 5.2.3 GAPP Ref 8.2.2 GAPP Ref 8.2.3 GAPP Ref 8.2.4 GAPP Ref 8.2.5 GAPP Ref 8.2.6 GAPP Ref 8.2.7
OP	Operations Management		OP-04	OP-04.4	If using virtual infrastructure, are machine images made available to the customer in a way that would allow the customer to replicate those images in their own off-site storage location?	No	However, we will allow copies of systems to be maintained in escrow. Again, this is not a typical request and we are happy to discuss options outside the scope of this document.	COBIT 4.1 A13.3	45 CFR 164.310 (a)(2)(iv)	A.9.2.4	NIST SP800-53 R3 MA-2 NIST SP800-53 R3 MA-3 NIST SP800-53 R3 MA-4 NIST SP800-53 R3 MA-5			SIG v6.0:F.2.19	GAPP Ref 5.2.3 GAPP Ref 8.2.2 GAPP Ref 8.2.3 GAPP Ref 8.2.4 GAPP Ref 8.2.5 GAPP Ref 8.2.6 GAPP Ref 8.2.7
OP	Operations Management		OP-04	OP-04.5	Does your cloud solution include software / provider independent restore and recovery capabilities?	No	We (as part of our service agreement) provide restore and recovery services as part of the solution.	COBIT 4.1 A13.3	45 CFR 164.310 (a)(2)(iv)	A.9.2.4	NIST SP800-53 R3 MA-2 NIST SP800-53 R3 MA-3			SIG v6.0:F.2.19	GAPP Ref 5.2.3 GAPP Ref 8.2.2 GAPP Ref 8.2.3 GAPP Ref 8.2.4
RI	Risk Management														
RI	Risk Management	Program	RI-01	RI-01.1	Is your organization insured by a 3rd party for losses?	Yes		COBIT 4.1 PO 9.1	45 CFR 164.308 (a)(8) 45 CFR	Clause 4.2.1 c) through g) Clause 4.2.2 b)	NIST SP800-53 R3 AC-4 NIST SP800-53	NIST SP800-53 R3 AC-4 NIST SP800-53	PCI DSS v2.0 12.1.2	AUP v5.0 L.2 AUP v5.0 L.2 SIG v6.0: A.1, L.1	GAPP Ref 1.2.4 GAPP Ref 1.2.4
RI	Risk Management		RI-01	RI-01.2	Do your organization's service level agreements provide tenant remuneration for losses they may incur due to outages or losses experienced within your infrastructure?	Yes		COBIT 4.1 PO 9.1	45 CFR 164.308 (a)(8) 45 CFR	Clause 4.2.1 c) through g) Clause 4.2.2 b)	NIST SP800-53 R3 AC-4 NIST SP800-53	NIST SP800-53 R3 AC-4 NIST SP800-53	PCI DSS v2.0 12.1.2	AUP v5.0 L.2 AUP v5.0 L.2 SIG v6.0: A.1, L.1	GAPP Ref 1.2.4 GAPP Ref 1.2.4
RI	Risk Management	Assessments	RI-02	RI-02.1	Are formal risk assessments aligned with the enterprise-wide framework and performed at least annually, or at planned intervals, determining the likelihood and impact of all identified risks, using qualitative and quantitative methods?	Yes		COBIT 4.1 PO 9.4	45 CFR 164.308 (a)(1)(ii)(A)	Clause 4.2.1 c) through g) Clause 4.2.3 d) Clause 5.1 f)	NIST SP800-53 R3 PL-5 NIST SP800-53 R3 RA-2	NIST SP800-53 R3 PL-5 NIST SP800-53 R3 RA-2	PCI DSS v2.0 12.1.2	AUP v5.0 I.1 AUP v5.0 I.4 SIG v6.0: C.2.1, I.4.1, I.5,	GAPP Ref 1.2.4 GAPP Ref 1.2.5
RI	Risk Management		RI-02	RI-02.2	Is the likelihood and impact associated with inherent and residual risk determined independently, considering all risk categories (e.g., audit results, threat and vulnerability analysis, and regulatory compliance)?	Yes		COBIT 4.1 PO 9.4	45 CFR 164.308 (a)(1)(ii)(A)	Clause 4.2.1 c) through g) Clause 4.2.3 d) Clause 5.1 f)	NIST SP800-53 R3 PL-5 NIST SP800-53 R3 RA-2	NIST SP800-53 R3 PL-5 NIST SP800-53 R3 RA-2	PCI DSS v2.0 12.1.2	AUP v5.0 I.1 AUP v5.0 I.4 SIG v6.0: C.2.1, I.4.1, I.5,	GAPP Ref 1.2.4 GAPP Ref 1.2.5
RI	Risk Management	Mitigation / Acceptance	RI-03	RI-03.1	Are risks mitigated to acceptable levels based on company-established criteria in accordance with reasonable resolution time frames?	Yes		COBIT 4.1 PO 9.5	45 CFR 164.308 (a)(1)(ii)(B)	Clause 4.2.1 c) through g) Clause 4.2.2 b) Clause 4.3.1 Clause 5.1 f) Clause 7.3 A.6.2.1 A.12.5.2 A.12.6.1 A.15.1.1 A.15.2.1 A.15.2.2	NIST SP800-53 R3 CA-5 NIST SP800-53 R3 CM-4	NIST SP800-53 R3 CA-5 NIST SP800-53 R3 CM-4		AUP v5.0I.4 AUP v5.0 L.2 SIG v6.0: I.3, L.9, L.10	
			RI-03	RI-03.2	Is remediation conducted at acceptable levels based on company-established criteria in accordance with reasonable time frames?	Yes									

RI	Risk Management	Business / Policy Change Impacts	RI-04	RI-04.1	Do risk assessment results include updates to security policies, procedures, standards and controls to ensure they remain relevant and effective?	Yes		COBIT 4.1 PO 9.6		Clause 4.2.3 Clause 4.2.4 Clause 4.3.1 Clause 5	NIST SP800-53 R3 CP-2 NIST SP800-53 R3 RA-2	NIST SP800-53 R3 CP-2 NIST SP800-53 R3 CP-2 (1)	PCI DSS v2.0 12.1.3	AUP v5.0 B.2 AUP v5.0 G.21 AUP v5.0 L.2 SIG v6.0: B.1.1	
RI	Risk Management	Third Party Access	RI-05	RI-05.1	Do you provide multi-failure disaster recovery capability?	Yes		COBIT 4.1 DS 2.3		A.6.2.1 A.8.3.3	NIST SP800-53 R3 CA-3	NIST SP800-53 R3 CA-3	PCI DSS v2.0 12.8.1	AUP v5.0 B.1 AUP v5.0 H.2	GAPP Ref 7.1.1 GAPP Ref 7.1.2
			RI-05	RI-05.2	Do you monitor service continuity with upstream providers in the event of provider failure?	Yes		COBIT 4.1 DS 2.3		A.6.2.1 A.8.3.3	NIST SP800-53 R3 CA-3	NIST SP800-53 R3 CA-3	PCI DSS v2.0 12.8.1	AUP v5.0 B.1 AUP v5.0 H.2	GAPP Ref 7.1.1 GAPP Ref 7.1.2
			RI-05	RI-05.3	Do you have more than one provider for each service you depend on?	Yes		COBIT 4.1 DS 2.3		A.6.2.1 A.8.3.3	NIST SP800-53 R3 CA-3	NIST SP800-53 R3 CA-3	PCI DSS v2.0 12.8.1	AUP v5.0 B.1 AUP v5.0 H.2	GAPP Ref 7.1.1 GAPP Ref 7.1.2
			RI-05	RI-05.4	Do you provide access to operational redundancy and continuity summaries which include the services on which you depend?	Yes		COBIT 4.1 DS 2.3		A.6.2.1 A.8.3.3 A.11.1.1 A.11.2.1	NIST SP800-53 R3 CA-3 NIST SP800-53 R3 MA-4	NIST SP800-53 R3 CA-3 NIST SP800-53 R3 MA-4	PCI DSS v2.0 12.8.1 PCI DSS v2.0 12.8.2	AUP v5.0 B.1 AUP v5.0 H.2 SIG v6.0: B.1.1, B.1.2, D.1.1,	GAPP Ref 7.1.1 GAPP Ref 7.1.2 GAPP Ref 7.2.1 GAPP Ref 7.2.2
			RI-05	RI-05.5	Do you provide the tenant the ability to declare a disaster?	Yes	However, the term, "disaster" needs to be defined and process and procedure discussed.	COBIT 4.1 DS 2.3		A.6.2.1 A.8.3.3 A.11.1.1 A.11.2.1	NIST SP800-53 R3 CA-3 NIST SP800-53 R3 MA-4	NIST SP800-53 R3 CA-3 NIST SP800-53 R3 MA-4	PCI DSS v2.0 12.8.1 PCI DSS v2.0 12.8.2	AUP v5.0 B.1 AUP v5.0 H.2 SIG v6.0: B.1.1, B.1.2, D.1.1,	GAPP Ref 7.1.1 GAPP Ref 7.1.2 GAPP Ref 7.2.1 GAPP Ref 7.2.2
			RI-05	RI-05.6	Do you provided a tenant triggered failover option?	No	This option is not available for the offered solution.	COBIT 4.1 DS 2.3		A.6.2.1 A.8.3.3 A.11.1.1	NIST SP800-53 R3 CA-3 NIST SP800-53	NIST SP800-53 R3 CA-3 NIST SP800-53	PCI DSS v2.0 12.8.1 PCI DSS v2.0	AUP v5.0 B.1 AUP v5.0 H.2 SIG v6.0: B.1.1.	GAPP Ref 7.1.1 GAPP Ref 7.1.2 GAPP Ref 7.2.1
			RI-05	RI-05.7	Do you share your business continuity and redundancy plans with your tenants?	Yes		COBIT 4.1 DS 2.3		A.6.2.1 A.8.3.3	NIST SP800-53 R3 CA-3	NIST SP800-53 R3 CA-3	PCI DSS v2.0 12.8.1	AUP v5.0 B.1 AUP v5.0 H.2	GAPP Ref 7.1.1 GAPP Ref 7.1.2
RM	Release														
RM	Release Management	New Development / Acquisition	RM-01	RM-01.1	Are policies and procedures established for management authorization for development or acquisition of new applications, systems, databases, infrastructure, services, operations, and facilities?	Yes		COBIT 4.1 A12, & 16.1		A.6.1.4 A.6.2.1 A.12.1.1 A.12.4.1 A.12.4.2 A.12.4.3 A.12.5.5 A.15.1.3 A.15.1.4	NIST SP800-53 R3 CA-1 NIST SP800-53 R3 CM-1 NIST SP800-53 R3 CM-9 NIST SP800-53 R3 PL-1 NIST SP800-53 R3 PL-2 NIST SP800-53 R3 SA-1 NIST SP800-53 R3 SA-3 NIST SP800-53 R3 SA-4		PCI DSS v2.0 6.3.2	AUP v5.0 I.2 SIG v6.0: I.1.1, I.1.2, I.2. 7.2, I.2.8, I.2.9, I.2.10, I.2.13, I.2.14, I.2.15, I.2.18, I.2.22.6, L.5,	GAPP Ref 1.2.6
RM	Release Management	Production Changes	RM-02	RM-02.1	Do you provide tenants with documentation which describes your production change management procedures and their roles/rights/responsibilities within it?	Yes		COBIT 4.1 A16.1, A17.6	45 CFR 164.308 (a)(5)(ii)(C) 45 CFR 164.312 (b)	A.10.1.4 A.12.5.1 A.12.5.2			PCI DSS v2.0 1.1.1 PCI DSS v2.0 6.3.2 PCI DSS v2.0 6.4 PCI DSS v2.0 6.1	SIG v6.0: I.2.17, I.2.20, I.2.22	GAPP Ref 1.2.6
RM	Release Management	Quality Testing	RM-03	RM-03.1	Do you provide your tenants with documentation which describes your quality assurance process?	Yes		COBIT 4.1 PO 8.1		A.6.1.3 A.10.1.1 A.10.1.4 A.10.3.2 A.12.1.1 A.12.2.1 A.12.2.2 A.12.2.3 A.12.2.4 A.12.4.1 A.12.4.2 A.12.4.3 A.12.5.1 A.12.5.2 A.12.5.3 A.12.6.1 A.13.1.2 A.15.2.1 A.15.2.2	NIST SP800-53 R3 CM-1 NIST SP800-53 R3 CM-2 NIST SP800-53 R3 SA-3 NIST SP800-53 R3 SA-4 NIST SP800-53 R3 SA-5 NIST SP800-53 R3 SA-8 NIST SP800-53 R3 SA-10 NIST SP800-53 R3 SA-11 NIST SP800-53 R3 SA-13		PCI DSS v2.0 1.1.1 PCI DSS v2.0 6.1 PCI DSS v2.0 6.4	C.1.7, G.1, G.6, I.1, I.4.5, I.2.18, , I.22.1, I.22.3, I.22.6, I.2.23, I.2.22.2, I.2.22.4, I.2.22.7. I.2.22.8, I.2.22.9, I.2.22.10, I.2.22.11, I.2.22.12, I.2.22.13, I.2.22.14,I.2.20, I.2.17, I.2.7.1, I.3, I.2.10, L.9	GAPP Ref 9.1.0 GAPP Ref 9.1.1 GAPP Ref 9.2.1 GAPP Ref 9.2.2
RM	Release Management	Outsourced Development	RM-04	RM-04.1	Do you have controls in place to ensure that standards of quality are being met for all software development?	Yes				A.6.1.8 A.6.2.1	NIST SP800-53 R3 SA-4		PCI DSS v2.0 3.6.7		
RM	Release Management		RM-04	RM-04.2	Do you have controls in place to detect source code security defects for any outsourced software development activities?	Yes				A.6.1.8 A.6.2.1	NIST SP800-53 R3 SA-4		PCI DSS v2.0 3.6.7		

RM	Release Management	Unauthorized Software Installations	RM-05	RM-05.1	Do you have controls in place to restrict and monitor the installation of unauthorized software onto your systems?	Yes				A.10.1.3 A.10.4.1 A.11.5.4 A.11.6.1 A.12.4.1 A.12.5.3				AUP v5.0 G.1 AUP v5.0 I.2 SIG v6.0: G.2.13, G.20.2,G.20.4, G.20.5, G.7, G.7.1, G.12.11, H.2.16, I.2.22.1, I.2.22.3, I.2.22.6, I.2.23,	GAPP Ref 3.2.4 GAPP Ref 8.2.2
RS	Resiliency														
RS	Resiliency	Management Program	RS-03	RS-03.1	Are Policy, process and procedures defining business continuity and disaster recovery in place to minimize the impact of a realized risk event and properly communicated to tenants?	Yes		COBIT 4.1 PO 9.1 PO 9.2 DS 4.2	45 CFR 164.308 (a)(7)(i) (New) 45 CFR 164.308 (a)(7)(ii)(C)	Clause 4.3.2 A.14.1.1 A 14.1.4	NIST SP800-53 R3 CP-1 NIST SP800-53 R3 CP-2	NIST SP800-53 R3 CP-1 NIST SP800-53 R3 CP-2 NIST SP800-53 R3 CP-2 (1) NIST SP800-53 R3 CP-2 (2)	PCI DSS v2.0 12.9.1	SIG v6.0: K.1.2.9, K.1.2.10, K.3.1	
RS	Resiliency	Impact Analysis	RS-02	RS-02.1	Do you provide tenants with ongoing visibility and reporting into your operational Service Level Agreement (SLA) performance?	Yes			45 CFR 164.308 (a)(7)(ii)(E)	ISO/IEC 27001:2005	NIST SP800-53 R3 RA-3	NIST SP800-53 R3 RA-3		SIG v6.0:K.2	
RS	Resiliency		RS-02	RS-02.2	Do you make standards-based information security metrics (CSA, CAMM, etc.) available to your tenants?	Yes	We use industry best practices but do not specifically subscribe to a particular standard.		45 CFR 164.308 (a)(7)(ii)(E)	ISO/IEC 27001:2005 A.14.1.2	NIST SP800-53 R3 RA-3	NIST SP800-53 R3 RA-3		SIG v6.0:K.2	
RS	Resiliency		RS-02	RS-02.3	Do you provide customers with ongoing visibility and reporting into your SLA performance?	Yes			45 CFR 164.308 (a)(7)(ii)(E)	ISO/IEC 27001:2005	NIST SP800-53 R3 RA-3	NIST SP800-53 R3 RA-3		SIG v6.0:K.2	
RS	Resiliency	Business Continuity Planning	RS-03	RS-03.1	Do you provide tenants with geographically resilient hosting options?	Yes			45 CFR 164.308 (a)(7)(i) 45 CFR 164.308 (a)(7)(ii)(B) 45 CFR 164.308 (a)(7)(ii)(C) 45 CFR 164.308	Clause 5.1 A.6.1.2 A.14.1.3 A.14.1.4	NIST SP800-53 R3 CP-1 NIST SP800-53 R3 CP-2 NIST SP800-53 R3 CP-3 NIST SP800-53		PCI DSS v2.0 12.9.1 PCI DSS v2.0 12.9.3 PCI DSS v2.0 12.9.4	SIG v6.0: K.1.2.3. K.1.2.4, K.1.2.5, K.1.2.6, K.1.2.7, K.1.2.11, K.1.2.13, K.1.2.15,	
RS	Resiliency		RS-03	RS-03.2	Do you provide tenants with infrastructure service failover capability to other providers?	No	We do not currently offer this request as part of a standard solution, but would be happy to discuss options on locating a DC solution that meets your needs.		45 CFR 164.308 (a)(7)(i) 45 CFR 164.308 (a)(7)(ii)(B) 45 CFR 164.308 (a)(7)(ii)(C)	Clause 5.1 A.6.1.2 A.14.1.3 A.14.1.4	NIST SP800-53 R3 CP-1 NIST SP800-53 R3 CP-2 NIST SP800-53 R3 CP-3		PCI DSS v2.0 12.9.1 PCI DSS v2.0 12.9.3 PCI DSS v2.0 12.9.4	SIG v6.0: K.1.2.3. K.1.2.4, K.1.2.5, K.1.2.6, K.1.2.7, K.1.2.11, K.1.2.13,	
RS	Resiliency	Business Continuity Testing	RS-04	RS-04.1	Are business continuity plans subject to test at planned intervals or upon significant organizational or environmental changes to ensure continuing effectiveness?	Yes			45 CFR 164.308 (a)(7)(ii)(D)	A.14.1.5	NIST SP800-53 R3 CP-2 NIST SP800-53 R3 CP-3 NIST SP800-53 R3 CP-4	NIST SP800-53 R3 CP-2 NIST SP800-53 R3 CP-2 (1) NIST SP800-53 R3 CP-2 (2) NIST SP800-53 R3 CP-3 NIST SP800-53 R3 CP-4 NIST SP800-53 R3 CP-4 (1)	PCI DSS v2.0 12.9.2	SIG v6.0: K.1.3, K.1.4.3, K.1.4.6, K.1.4.7, K.1.4.8, K.1.4.9, K.1.4.10, K.1.4.11, K.1.4.12	
RS	Resiliency	Environmental Risks	RS-05	RS-05.1	Is physical protection against damage from natural causes and disasters as well as deliberate attacks anticipated, designed and countermeasures applied?	Yes			45 CFR 164.308 (a)(7)(i) 45 CFR 164.310(a)(2)(ii) (New)	A.9.1.4 A.9.2.1	NIST SP800-53 R3 PE-1 NIST SP800-53 R3 PE-13 NIST SP800-53 R3 PE-14 NIST SP800-53 R3 PE-15 NIST SP800-53 R3 PE-18	NIST SP800-53 R3 PE-1 NIST SP800-53 R3 PE-13 NIST SP800-53 R3 PE-13 (1) NIST SP800-53 R3 PE-13 (2) NIST SP800-53 R3 PE-13 (3) NIST SP800-53 R3 PE-14 NIST SP800-53 R3 PE-14 (1) NIST SP800-53 R3 PE-15 NIST SP800-53 R3 PE-18		AUP v5.0 F.1 SIG v6.0: F.2.9, F.1.2.21, F.5.1, F.1.5.2, F.2.1, F.2.7, F.2.8,	GAPP Ref 8.2.4

RS	Resiliency	Equipment Location	RS-06	RS-06.1	Are any of your datacenters located in places which have a high probability/occurrence of high-impact environmental risks (floods, tornadoes, earthquakes, hurricanes, etc.)?	Yes	We have data centers around the globe, some of which may be subjected, albeit a low probability, to environmental risks.		45 CFR 164.310 (c)	A.9.2.1	NIST SP800-53 R3 PE-1 NIST SP800-53 R3 PE-5 NIST SP800-53 R3 PE-14 NIST SP800-53 R3 PE-15 NIST SP800-53 R3 PE-18	NIST SP800-53 R3 PE-1 NIST SP800-53 R3 PE-5 NIST SP800-53 R3 PE-14 NIST SP800-53 R3 PE-14 (1) NIST SP800-53 R3 PE-15 NIST SP800-53 R3 PE-18	PCI DSS v2.0 9.1.3 PCI DSS v2.0 9.5 PCI DSS v2.0 9.6 PCI DSS v2.0 9.9 PCI DSS v2.0 9.9.1	AUP v5.0 F.1 SIG v6.0: F.2.9, F.1.2.21, F.5.1, F.1.5.2, F.2.1, F.2.7, F.2.8,	
RS	Resiliency	Equipment Power Failures	RS-07	RS-07.1	Are Security mechanisms and redundancies implemented to protect equipment from utility service outages (e.g., power failures, network disruptions, etc.)?	Yes				A.9.2.2 A.9.2.3 A 9.2.4	NIST SP800-53 R3 CP-8 NIST SP800-53 R3 PE-1 NIST SP800-53 R3 PE-9 NIST SP800-53 R3 PE-10 NIST SP800-53 R3 PE-11 NIST SP800-53 R3 PE-12 NIST SP800-53 R3 PE-13 NIST SP800-53 R3 PE-14			AUP v5.0 F.1 SIG v6.0: F.1.6, F.1.6.1, F.1.6.2, F.1.9.2, F.2.10, F.2.11, F.2.12,	
RS	Resiliency	Power / Telecommunications	RS-08	RS-08.1	Do you provide tenants with documentation showing the transport route of their data between your systems?	Yes				A.9.2.2 A.9.2.3	NIST SP800-53 R3 PE-1 NIST SP800-53 R3 PE-1	NIST SP800-53 R3 PE-1 NIST SP800-53 R3 PE-1		AUP v5.0 F.1 SIG v6.0: F.1.6,	
RS	Resiliency		RS-08	RS-08.2	Can Tenants define how their data is transported and through which legal jurisdiction?	Yes	We can accomodate this request if required, but by default, this is not a standard option of service.			A.9.2.2 A.9.2.3	NIST SP800-53 R3 PE-1 NIST SP800-53	NIST SP800-53 R3 PE-1 NIST SP800-53		AUP v5.0 F.1 SIG v6.0: F.1.6, F.1.6.1, F.1.6.2,	
SA	Security														
SA	Security Architecture	Customer Access Requirements	SA-01	SA-01.1	Are all identified security, contractual and regulatory requirements for customer access contractually addressed and remediated prior to granting customers access to data, assets and Information systems?	Yes				A.6.2.1 A.6.2.2 A.11.1.1	NIST SP800-53 R3 CA-1 NIST SP800-53 R3 CA-2 NIST SP800-53 R3 CA-5 NIST SP800-53 R3 CA-6	NIST SP800-53 R3 CA-1 NIST SP800-53 R3 CA-2 NIST SP800-53 R3 CA-2 (1) NIST SP800-53 R3 CA-5 NIST SP800-53 R3 CA-6		SIG v6.0: C.2.1, C.2.3, C.2.4, C.2.6.1, H.1	GAPP Ref 1.2.2 GAPP Ref 1.2.6 GAPP Ref 6.2.1 GAPP Ref 6.2.2
SA	Security Architecture	User ID Credentials	SA-02	SA-02.1	Do you support use of, or integration with, existing customer-based Single Sign On (SSO) solutions to your service?	Yes	We have partnered with Ping Identity and use their PingFederate solution for SSO solutions.	COBIT 4.1 DS5.3 COBIT 4.1 DS5.4	45 CFR 164.308(a)(5)(ii)(c) (New) 45 CFR 164.308	A.8.3.3 A.11.1.1 A.11.2.1 A.11.2.3			PCI DSS v2.0 8.1 PCI DSS v2.0 8.2, PCI DSS v2.0 8.3	AUP v5.0 B.1 AUP v5.0 H.5 SIG v6.0: E.6.2, E.6.3, H.1.1,	
SA	Security Architecture		SA-02	SA-02.2	Do you use open standards to delegate authentication capabilities to your tenants?	Yes		COBIT 4.1 DS5.3 COBIT 4.1 DS5.4	45 CFR 164.308(a)(5)(ii)	A.8.3.3 A.11.1.1			PCI DSS v2.0 8.1 PCI DSS v2.0	AUP v5.0 B.1 AUP v5.0 H.5	
SA	Security Architecture		SA-02	SA-02.3	Do you support identity federation standards (SAML, SPML, WS-Federation, etc.) as a means of authenticating/authorizing users?	Yes		COBIT 4.1 DS5.3 COBIT 4.1 DS5.4	45 CFR 164.308(a)(5)(ii)	A.8.3.3 A.11.1.1			PCI DSS v2.0 8.1 PCI DSS v2.0	AUP v5.0 B.1 AUP v5.0 H.5	
SA	Security Architecture		SA-02	SA-02.4	Do you have a Policy Enforcement Point capability (ex. XACML) to enforce regional legal and policy constraints on user access?	No	Roles and Responsibilities are attached to the user after they are authenticated via SSO (SAML assertion). Policies are defined prior to user authentication and are administrated by tenant administrators.	COBIT 4.1 DS5.3 COBIT 4.1 DS5.4	45 CFR 164.308(a)(5)(ii)(c) (New) 45 CFR 164.308 (a)(5)(ii)(D) 45 CFR 164.312 (a)(2)(i) 45 CFR 164.312	A.8.3.3 A.11.1.1 A.11.2.1 A.11.2.3 A.11.2.4 A.11.5.5			PCI DSS v2.0 8.1 PCI DSS v2.0 8.2, PCI DSS v2.0 8.3 PCI DSS v2.0 8.4 PCI DSS v2.0 8.5 PCI DSS v2.0 10.1	AUP v5.0 B.1 AUP v5.0 H.5 SIG v6.0: E.6.2, E.6.3, H.1.1, H.1.2, H.2, H.3.2, H.4, H.4.1, H.4.5, H.4.8	
SA	Security Architecture		SA-02	SA-02.5	Do you have an identity management system in place which enables both role-based and context-based entitlement to data (enables classification of data for a tenant)?	Yes	Tenant Administrators may use templates to populate role-based access to functions within the application.	COBIT 4.1 DS5.3 COBIT 4.1 DS5.4	45 CFR 164.308(a)(5)(ii)(c) (New) 45 CFR 164.308	A.8.3.3 A.11.1.1 A.11.2.1 A.11.2.3			PCI DSS v2.0 8.1 PCI DSS v2.0 8.2, PCI DSS v2.0 8.3	AUP v5.0 B.1 AUP v5.0 H.5 SIG v6.0: E.6.2, E.6.3, H.1.1,	
SA	Security Architecture		SA-02	SA-02.6	Do you provide tenants with strong (multifactor) authentication options (digital certs, tokens, biometric, etc..) for user access?	No	We have a partner that provides two-factor authentication; however, this feature has not been implemented as part of our security architecture.	COBIT 4.1 DS5.3 COBIT 4.1 DS5.4	45 CFR 164.308(a)(5)(ii)(c) (New) 45 CFR 164.308 (a)(5)(ii)(D)	A.8.3.3 A.11.1.1 A.11.2.1 A.11.2.3 A.11.2.4			PCI DSS v2.0 8.1 PCI DSS v2.0 8.2, PCI DSS v2.0 8.3 PCI DSS v2.0 8.4	AUP v5.0 B.1 AUP v5.0 H.5 SIG v6.0: E.6.2, E.6.3, H.1.1, H.1.2, H.2,	
SA	Security Architecture		SA-02	SA-02.7	Do you allow tenants to use third party identity assurance services?	Yes	We would work together to design the security architecture and discuss your needs and who / where these services are located.	COBIT 4.1 DS5.3 COBIT 4.1 DS5.4	45 CFR 164.308(a)(5)(ii)(c) (New) 45 CFR 164.308 (a)(5)(ii)(D)	A.8.3.3 A.11.1.1 A.11.2.1 A.11.2.3 A.11.2.4			PCI DSS v2.0 8.1 PCI DSS v2.0 8.2, PCI DSS v2.0 8.3 PCI DSS v2.0 8.4	AUP v5.0 B.1 AUP v5.0 H.5 SIG v6.0: E.6.2, E.6.3, H.1.1, H.1.2, H.2,	

SA	Security Architecture	Data Security / Integrity	SA-03	SA-03.1	Is your Data Security Architecture designed using an industry standard? (ex. CDSA, MULITSAFE, CSA Trusted Cloud Architectural Standard, FedRAMP CAESARS)	Yes	We use best practices in the industry but do not subscribe to a single industry standard.	COBIT 4.1 DS5.11		A.10.8.1 A.10.8.2 A.11.1.1 A.11.6.1 A.11.4.6	NIST SP800-53 R3 AC-1 NIST SP800-53 R3 AC-4 NIST SP800-53	NIST SP800-53 R3 AC-1 NIST SP800-53 R3 AC-4 NIST SP800-53	PCI DSS v2.0 2.3 PCI DSS v2.0 3.4.1, PCI DSS v2.0 4.1 PCI DSS v2.0	AUP v5.0 B.1 SIG v6.0: G.8.2.0.2, G.8.2.0.3, G.12.1, G.12.4,	GAPP Ref 1.1.0 GAPP Ref 1.2.2 GAPP Ref 1.2.6 GAPP Ref 4.2.3 GAPP Ref 5.2.1
SA	Security Architecture	Application Security	SA-04	SA-04.1	Do you utilize industry standards (Build Security in Maturity Model [BSIMM] Benchmarks, Open Group ACS Trusted Technology Provider Framework, NIST, etc.) to build-in security for your Systems/Software Development Lifecycle (SDLC)?	Yes		COBIT 4.1 AI2.4	45 CFR 164.312(e)(2)(i)	A.11.5.6 A.11.6.1 A.12.2.1 A.12.2.2			PCI DSS v2.0 6.5	AUP v5.0 I.4 SIG v6.0: G.16.3, I.3	GAPP Ref 1.2.6
SA	Security Architecture		SA-04	SA-04.2	Do you utilize an automated source-code analysis tool to detect code security defects prior to production?	Yes		COBIT 4.1 AI2.4	45 CFR 164.312(e)(2)(i)	A.11.5.6 A.11.6.1			PCI DSS v2.0 6.5	AUP v5.0 I.4 SIG v6.0:	GAPP Ref 1.2.6
SA	Security Architecture		SA-04	SA-04.3	Do you verify that all of your software suppliers adhere to industry standards for Systems/Software Development Lifecycle (SDLC) security?	Yes		COBIT 4.1 AI2.4	45 CFR 164.312(e)(2)(i)	A.11.5.6 A.11.6.1 A.12.2.1			PCI DSS v2.0 6.5	AUP v5.0 I.4 SIG v6.0: G.16.3, I.3	GAPP Ref 1.2.6
SA	Security Architecture	Data Integrity	SA-05	SA-05.1	Are data input and output integrity routines (i.e., reconciliation and edit checks) implemented for application interfaces and databases to prevent manual or systematic processing errors or corruption of data?	Yes			45 CFR 164.312 (c)(1) (New) 45 CFR 164.312 (c)(2)(New)	A.10.9.2 A.10.9.3 A.12.2.1 A.12.2.2	NIST SP800-53 R3 SI-10 NIST SP800-53 R3 SI-11		PCI DSS v2.0 6.3.1 PCI DSS v2.0 6.3.2	AUP v5.0 I.4 SIG v6.0: G.16.3, I.3	GAPP Ref 1.2.6
SA	Security Architecture	Production / Nonproduction	SA-06	SA-06.1	For your SaaS or PaaS offering, do you provide tenants with separate environments for production and test processes?	Yes		COBIT 4.1 DS5.7		A.10.1.4 A.10.3.2	NIST SP800-53 R3 SC-2	NIST SP800-53 R3 SC-2	PCI DSS v2.0 6.4.1	AUP v5.0 B.1 SIG v6.0:	GAPP Ref 1.2.6
SA	Security Architecture		SA-06	SA-06.2	For your IaaS offering, do you provide tenants with guidance on how to create suitable production and test environments?	No	This does not apply to Perfect Commerce's offering.	COBIT 4.1 DS5.7		A.10.1.4 A.10.3.2	NIST SP800-53 R3 SC-2	NIST SP800-53 R3 SC-2	PCI DSS v2.0 6.4.1	AUP v5.0 B.1 SIG v6.0:	GAPP Ref 1.2.6
SA	Security Architecture	Remote User Multifactor Authentication	SA-07	SA-07.1	Is multi-factor authentication required for all remote user access?	No				A.11.1.1 A.11.4.1 A.11.4.2 A.11.4.6 A.11.7.1	NIST SP800-53 R3 AC-17 NIST SP800-53 R3 AC-20 NIST SP800-53		PCI DSS v2.0 8.3	AUP v5.0 B.1 SIG v6.0: H.1.1, G.9.13, G.9.20, G.9.21,	GAPP Ref 8.2.2
SA	Security Architecture	Network Security	SA-08	SA-08.1	For your IaaS offering, do you provide customers with guidance on how to create a layered security architecture equivalence using your virtualized solution?	No	This does not apply to Perfect Commerce's offering.			A.10.6.1 A.10.6.2 A.10.9.1 A.10.10.2 A.11.4.1 A.11.4.5 A.11.4.6 A.11.4.7 A.15.1.4	NIST SP800-53 R3 SC-7		PCI DSS v2.0 1.1 PCI DSS v2.0 1.1.2 PCI DSS v2.0 1.1.3 PCI DSS v2.0 1.1.5 PCI DSS v2.0 1.1.6 PCI DSS v2.0 1.2 PCI DSS v2.0 1.2.1 PCI DSS v2.0 2.2.2, PCI DSS v2.0 2.2.3		GAPP Ref 8.2.5
SA	Security Architecture	Segmentation	SA-09	SA-09.1	Are system and network environments logically separated to ensure Business and customer security requirements?	Yes		COBIT 4.1 DS5.10	45 CFR 164.308 (a)(4)(ii)(A)	A.11.4.5 A.11.6.1	NIST SP800-53 R3 AC-4		PCI DSS v2.0 1.1 PCI DSS v2.0 1.2	AUP v5.0 G.17 SIG v6.0: G.9.2,	
SA	Security Architecture		SA-09	SA-09.2	Are system and network environments logically separated to ensure compliance with legislative, regulatory, and contractual requirements?	Yes		COBIT 4.1 DS5.10	45 CFR 164.308 (a)(4)(ii)(A)	A.11.4.5 A.11.6.1 A.11.6.2	NIST SP800-53 R3 AC-4 NIST SP800-53		PCI DSS v2.0 1.1 PCI DSS v2.0 1.2 PCI DSS v2.0	AUP v5.0 G.17 SIG v6.0: G.9.2, G.9.3, G.9.13	
SA	Security Architecture		SA-09	SA-09.3	Are system and network environments logically separated to ensure separation of production and non-production environments?	Yes		COBIT 4.1 DS5.10	45 CFR 164.308 (a)(4)(ii)(A)	A.11.4.5 A.11.6.1	NIST SP800-53 R3 AC-4		PCI DSS v2.0 1.1 PCI DSS v2.0 1.2	AUP v5.0 G.17 SIG v6.0: G.9.2,	
SA	Security Architecture		SA-09	SA-09.4	Are system and network environments logically separated to ensure protection and isolation of sensitive data?	Yes		COBIT 4.1 DS5.10	45 CFR 164.308 (a)(4)(ii)(A)	A.11.4.5 A.11.6.1	NIST SP800-53 R3 AC-4		PCI DSS v2.0 1.1 PCI DSS v2.0 1.2	AUP v5.0 G.17 SIG v6.0: G.9.2,	
SA	Security Architecture	Wireless Security	SA-10	SA-10.1	Are policies and procedures established and mechanisms implemented to protect network environment peremeter and configured to restrict unauthorized traffic?	Yes		COBIT 4.1 DS5.5 COBIT 4.1 DS5.7 COBIT 4.1 DS5.8	45 CFR 164.312 (e)(1)(2)(ii) 45 CFR	A.7.1.1 A.7.1.2 A.7.1.3	NIST SP800-53 R3 AC-1 NIST SP800-53		PCI DSS v2.0 1.2.3 PCI DSS v2.0		GAPP Ref 8.2.5
SA	Security Architecture		SA-10	SA-10.2	Are policies and procedures established and mechanisms implemented to ensure proper security settings enabled with strong encryption for authentication and transmission, replacing vendor default settings? (e.g., encryption keys, passwords, SNMP community strings, etc.)	Yes		COBIT 4.1 DS5.5 COBIT 4.1 DS5.7 COBIT 4.1 DS5.8 COBIT 4.1 DS5.10	45 CFR 164.312 (e)(1)(2)(ii) 45 CFR 164.308(a)(5)(ii)(D) (New)	A.7.1.1 A.7.1.2 A.7.1.3 A.9.2.1 A.9.2.4	NIST SP800-53 R3 AC-1 NIST SP800-53 R3 AC-18 NIST SP800-53		PCI DSS v2.0 1.2.3 PCI DSS v2.0 2.1.1 PCI DSS v2.0 4.1		GAPP Ref 8.2.5
SA	Security Architecture		SA-10	SA-10.3	Are policies and procedures established and mechanisms implemented to protect network environments and detect the presence of unauthorized (rogue) network devices for a timely disconnect from the network?	Yes		COBIT 4.1 DS5.5 COBIT 4.1 DS5.7 COBIT 4.1 DS5.8 COBIT 4.1 DS5.10	45 CFR 164.312 (e)(1)(2)(ii) 45 CFR 164.308(a)(5)(ii	A.7.1.1 A.7.1.2 A.7.1.3 A.9.2.1	NIST SP800-53 R3 AC-1 NIST SP800-53 R3 AC-18		PCI DSS v2.0 1.2.3 PCI DSS v2.0 2.1.1		GAPP Ref 8.2.5
SA	Security Architecture	Shared Networks	SA-11	SA-11.1	Is access to systems with shared network infrastructure restricted to authorized personnel in accordance with security policies, procedures and standards. Networks shared with externalentities shall have a documented plan detailing the compensating controls used to separate network traffic between organizations?	Yes			45 CFR 164.312 (a)(1) (New)	A.10.8.1 A.11.1.1 A.11.6.2 A.11.4.6	NIST SP800-53 R3 PE-4 NIST SP800-53 R3 SC-4 NIST SP800-53		PCI DSS v2.0 1.3.5 PCI DSS v2.0 2.4	AUP v5.0 B.1 SIG v6.0: D.1.1, E.1, F.1.1, H.1.1,	GAPP Ref 8.2.5

SA	Security Architecture	Clock Synchronization	SA-12	SA-12.1	Do you utilize a synchronized time-service protocol (ex. NTP) to ensure all systems have a common time reference?	Yes		COBIT 4.1 DS5.7		A.10.10.1 A.10.10.6	NIST SP800-53 R3 AU-1 NIST SP800-53 R3 AU-8	NIST SP800-53 R3 AU-1 NIST SP800-53 R3 AU-8 NIST SP800-53 R3 AU-8 (1)	PCI DSS v2.0 10.4	AUP v5.0 G.7 AUP v5.0 G.8 SIG v6.0: G.13, G.14.8, G.15.5, G.16.8, G.17.6, G.18.3, G.19.2.6, G.19.3.1,	
SA	Security Architecture	Equipment Identification	SA-13	SA-13.1	Is automated equipment identification used as a method of connection authentication to validate connection authentication integrity based on known equipment location?	No	This is completed manually.	COBIT 4.1 DS5.7		A.11.4.3	NIST SP800-53 R3 IA-3 NIST SP800-53 R3 IA-4	NIST SP800-53 R3 IA-3 NIST SP800-53 R3 IA-4 NIST SP800-53 R3 IA-4 (4)		AUP v5.0 D.1 SIG v6.0: D.1.1, D.1.3	
SA	Security Architecture	Audit Logging / Intrusion Detection	SA-14	SA-14.1	Are file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis and response to incidents?	Yes		COBIT 4.1 DS5.5 COBIT 4.1 DS5.6 COBIT 4.1 DS9.2	45 CFR 164.308 (a)(1)(ii)(D) 45 CFR 164.312	A.10.10.1 A.10.10.2 A.10.10.3			PCI DSS v2.0 10.1 PCI DSS v2.0 10.2		GAPP Ref 8.2.1 GAPP Ref 8.2.2
SA	Security Architecture		SA-14	SA-14.2	Is Physical and logical user access to audit logs restricted to authorized personnel?	Yes		COBIT 4.1 DS5.5 COBIT 4.1 DS5.6	45 CFR 164.308 (a)(1)(ii)(D)	A.10.10.1 A.10.10.2			PCI DSS v2.0 10.1 PCI DSS		GAPP Ref 8.2.1 GAPP Ref 8.2.2
SA	Security Architecture		SA-14	SA-14.3	Can you provide evidence that due diligence mapping of regulations and standards to your controls/architecture/processes has been done?	Yes		COBIT 4.1 DS5.5 COBIT 4.1 DS5.6 COBIT 4.1 DS9.2	45 CFR 164.308 (a)(1)(ii)(D) 45 CFR 164.312 (b)	A.10.10.1 A.10.10.2 A.10.10.3 A.10.10.4			PCI DSS v2.0 10.1 PCI DSS v2.0 10.2 PCI DSS		GAPP Ref 8.2.1 GAPP Ref 8.2.2
SA	Security Architecture	Mobile Code	SA-15	SA-15.1	Is mobile code authorized before its installation and use and the code configuration checked to ensure that the authorized mobile code operates according to a clearly defined security policy?	Yes				A.10.4.2 A.12.2.2	NIST SP800-53 R3 SC-18	NIST SP800-53 R3 SC-18 NIST SP800-53 R3 SC-18 (4)		SIG v6.0:G.20.12, I.2.5	
SA	Security Architecture		SA-15	SA-15.2	Is all unauthorized mobile code prevented from executing?	Yes				A.10.4.2	NIST SP800-53	NIST SP800-53		SIG	

CONSENSUS ASSESSMENT INITIATIVE QUESTIONNAIRE (CAIQ) V.1.1 GUIDING DOCUMENT PRINCIPLES

INTENT OF THIS TAB: To assist reviewers/users of document to understand both the intent and

GUIDING PRINCIPLES:

- Questionnaire is organized using CSA 13 governing & operating domains divided into "control areas" within CSA's Control Matrix structure

- Questions are to assist both cloud providers in general principles of cloud security and clients in vetting cloud providers on the security of their offering and company security profile

- CAIQ not intended to duplicate or replace existing industry security assessments but to contain questions unique or critical to the cloud computing model in each control area

- Each question should be able to be answered yes or no

- If a question can't be answered yes or no then it was separated into two or more questions to allow yes or no answers.

- Questions are intended to foster further detailed questions to provider by client specific to client's cloud security needs. This was done to limit number of questions to make the assessment feasible and since each client may have unique follow-on questions or may not be concerned with all "follow-on

Cloud Controls Matrix (CCM) R1.1

Control Area	Control ID	Control Specification	Control Revisions V1.1	Cloud Service Delivery Model Applicability			Scope Applicability		Compliance Mapping							
				SaaS	PaaS	IaaS	Service Provider	Tenant	COBIT 4.1	HIPAA / HITECH Act	ISO/IEC 27001:2005	NIST SP800-53	FedRAMP	PCI DSS v2.0	BITS Shared Assessments AUP v5.0 / SIG v6.0	GAPP (Aug 2009)
Compliance - Audit Planning	CO-01	Audit plans, activities and operational action items focusing on data duplication, access, and data boundary limitations shall be designed to minimize the risk of business process disruption. Audit activities must be planned and agreed upon in advance by stakeholders.	No Change	X	X	X	X		COBIT 4.1 ME 2.1, ME 2.2 PO 9.5 PO 9.6	45 CFR 164.312(b)	Clause 4.2.2 e) Clause 4.2.3b Clause 5.1 g Clause 8 A.15.3.1	NIST SP800-53 R3 CA-2 NIST SP800-53 R3 CA-7 NIST SP800-53 R3 PL-6	NIST SP800-53 R3 CA-2 NIST SP800-53 R3 CA-2 (1) NIST SP800-53 R3 CA-7 NIST SP800-53 R3 CA-7 (2) NIST SP800-53 R3 PL-6	PCI DSS v2.0 2.1.2.b	SIG v6.0: L.2, L.3, L.7, L.9, L.11	GAPP Ref 10.2.5
Compliance - Independent Audits	CO-02	Independent reviews and assessments shall be performed at least annually, or at planned intervals, to ensure the organization is compliant with policies, procedures, standards and applicable regulatory requirements (i.e., internal/external audits, certifications, vulnerability and penetration testing)	No Change	X	X	X	X	X	COBIT 4.1 DS5.5, ME2.5, ME 3.1 PO 9.6	45 CFR 164.308 (a)(8) 45 CFR 164.308(a)(1)(ii)(D)	Clause 4.2.3e Clause 5.1 g Clause 5.2.1 d) Clause 6 A.6.1.8	NIST SP800-53 R3 CA-1 NIST SP800-53 R3 CA-2 NIST SP800-53 R3 CA-6 NIST SP800-53 R3 RA-5	NIST SP800-53 R3 CA-1 NIST SP800-53 R3 CA-2 NIST SP800-53 R3 CA-2 (1) NIST SP800-53 R3 CA-6 NIST SP800-53 R3 RA-5 NIST SP800-53 R3 RA-5 (1) NIST SP800-53 R3 RA-5 (2) NIST SP800-53 R3 RA-5 (3) NIST SP800-53 R3 RA-5 (8) NIST SP800-53 R3 RA-5 (5)	PCI DSS v2.0 11.2 PCI DSS v2.0 11.3 PCI DSS v2.0 6.6 PCI DSS v2.0 12.1.2.b	SIG v6.0: L.2, L.4, L.7, L.9, L.11	GAPP Ref 1.2.5 GAPP Ref 1.2.7 GAPP Ref 4.2.1 GAPP Ref 8.2.7 GAPP Ref 10.2.3 GAPP Ref 10.2.5
Compliance - Third Party Audits	CO-03	Third party service providers shall demonstrate compliance with information security and confidentiality, service definitions and delivery level agreements included in third party contracts. Third party reports, records and services shall undergo audit and review, at planned intervals, to govern and maintain compliance with the service delivery agreements.	No Change	X	X	X	X		COBIT 4.1 ME 2.6, DS 2.1, DS 2.4	45 CFR 164.308(b)(1) (New) 45 CFR 164.308 (b)(4)	A.6.2.3 A.10.2.1 A.10.2.2 A.10.6.2	NIST SP800-53 R3 CA-3 NIST SP800-53 R3 SA-9 NIST SP800-53 R3 SA-12 NIST SP800-53 R3 SC-7	NIST SP800-53 R3 CA-3 NIST SP800-53 R3 SA-9 NIST SP800-53 R3 SA-9 (1) NIST SP800-53 R3 SA-12 NIST SP800-53 R3 SC-7 NIST SP800-53 R3 SC-7 (1) NIST SP800-53 R3 SC-7 (2) NIST SP800-53 R3 SC-7 (3) NIST SP800-53 R3 SC-7 (4) NIST SP800-53 R3 SC-7 (5) NIST SP800-53 R3 SC-7 (7) NIST SP800-53 R3 SC-7 (8) NIST SP800-53 R3 SC-7 (12) NIST SP800-53 R3 SC-7 (13) NIST SP800-53 R3 SC-7 (18)	PCI DSS v2.0 2.4 PCI DSS v2.0 12.8.2 PCI DSS v2.0 12.8.3 PCI DSS v2.0 12.8.4 Appendix A	AUP v5.0 C.2 SIG v6.0: C.2.4, C.2.6, G.4.1, G.4.2, L.2, L.4, L.7, L.11	GAPP Ref 1.2.11 GAPP Ref 4.2.3 GAPP Ref 7.2.4 GAPP Ref 10.2.3 GAPP Ref 10.2.4
Compliance - Contact / Authority Maintenance	CO-04	Liaisons and points of contact with local authorities shall be maintained in accordance with business and customer requirements and compliance with legislative, regulatory, and contractual requirements. Data, objects, applications, infrastructure and hardware may be assigned legislative domain and jurisdiction to facilitate proper compliance points of contact.	No Change	X	X	X	X	X	COBIT 4.1 ME 3.1		A.6.1.6 A.6.1.7	NIST SP800-53 R3 AT-5 NIST SP800-53 R3 IR-6 NIST SP800-53 R3 SI-5	NIST SP800-53 R3 AT-5 NIST SP800-53 R3 IR-6 NIST SP800-53 R3 IR-6 (1) NIST SP800-53 R3 SI-5	PCI DSS v2 11.1.a PCI PCI DSS v2 12.5.3 PCI DSS v2 12.9	SIG v6.0: L1	GAPP Ref 1.2.7 GAPP Ref 10.1.1 GAPP Ref 10.2.4
Compliance - Information System Regulatory Mapping	CO-05	Statutory, regulatory, and contractual requirements shall be defined for all elements of the information system. The organization's approach to meet known requirements, and adapt to new mandates shall be explicitly defined, documented, and kept up to date for each information system element in the organization. Information system elements may include data, objects, applications, infrastructure and hardware. Each element may be assigned a legislative domain and jurisdiction to facilitate proper compliance mapping.	No Change	X	X	X	X	X	COBIT 4.1 ME 3.1		ISO/IEC 27001:2005 Clause 4.2.1 b) 2) Clause 4.2.1 c) 1) Clause 4.2.1 g) Clause 4.2.3 d) 6) Clause 4.3.3 Clause 5.2.1 a - f Clause 7.3 c) 4) A.7.2.1 A.15.1.1 A.15.1.3 A.15.1.4 A.15.1.6	NIST SP800-53 R3 AC-1 NIST SP800-53 R3 AT-1 NIST SP800-53 R3 AU-1 NIST SP800-53 R3 CA-1 NIST SP800-53 R3 CM-1 NIST SP800-53 R3 CP-1 NIST SP800-53 R3 IA-1 NIST SP800-53 R3 IA-7 NIST SP800-53 R3 IR-1 NIST SP800-53 R3 MA-1 NIST SP800-53 R3 MP-1 NIST SP800-53 R3 PE-1 NIST SP800-53 R3 PL-1 NIST SP800-53 R3 PM-1 NIST SP800-53 R3 PS-1 NIST SP800-53 R3 RA-1 NIST SP800-53 R3 RA-2 NIST SP800-53 R3 SA-1 NIST SP800-53 R3 SA-6 NIST SP800-53 R3 SC-1 NIST SP800-53 R3 SC-13 NIST SP800-53 R3 SI-1	NIST SP800-53 R3 AC-1 NIST SP800-53 R3 AT-1 NIST SP800-53 R3 AU-1 NIST SP800-53 R3 CA-1 NIST SP800-53 R3 CM-1 NIST SP800-53 R3 CP-1 NIST SP800-53 R3 IA-1 NIST SP800-53 R3 IA-7 NIST SP800-53 R3 IR-1 NIST SP800-53 R3 MA-1 NIST SP800-53 R3 MP-1 NIST SP800-53 R3 PE-1 NIST SP800-53 R3 PL-1 NIST SP800-53 R3 PM-1 NIST SP800-53 R3 PS-1 NIST SP800-53 R3 RA-1 NIST SP800-53 R3 RA-2 NIST SP800-53 R3 SA-1 NIST SP800-53 R3 SA-6 NIST SP800-53 R3 SC-1 NIST SP800-53 R3 SC-13 NIST SP800-53 R3 SC-13 (1) NIST SP800-53 R3 SI-1	PCI DSS v2.0 3.1.1 PCI DSS v2.0 3.1	SIG v6.0: L.1, L.2, L.4, L.7, L.9	GAPP Ref 1.2.2 GAPP Ref 1.2.4 GAPP Ref 1.2.9 GAPP Ref 1.2.11 GAPP Ref 3.2.4 GAPP Ref 5.2.1
Compliance - Intellectual Property	CO-06	Policy, process and procedure shall be established and implemented to safeguard intellectual property and the use of proprietary software within the legislative jurisdiction and contractual constraints governing the organization.	No Change	X	X	X	X	X			Clause 4.2.1 A.6.1.5 A.7.1.3 A.10.8.2 A.12.4.3 A.15.1.2	NIST SP800-53 R3 SA-6 NIST SP800-53 R3 SA-7 NIST SP800-53 R3 PM-5	NIST SP800-53 R3 SA-6 NIST SP800-53 R3 SA-7 NIST SP800-53 R3 PM-5		SIG v6.0: L.4	N/A
Data Governance - Ownership / Stewardship	DG-01	All data shall be designated with stewardship with assigned responsibilities defined, documented and communicated.	No Change	X	X	X	X		COBIT 4.1 DS5.1, PO 2.3	45 CFR 164.308 (a)(2)	A.6.1.3 A.7.1.2 A.15.1.4	NIST SP800-53 R3 CA-2 NIST SP800-53 R3 PM-5 NIST SP800-53 R3 PS-2 NIST SP800-53 R3 RA-2 NIST SP800-53 R3 SA-2	NIST SP800-53 R3 CA-2 NIST SP800-53 R3 CA-2 (1) NIST SP800-53 R3 PM-5 NIST SP800-53 R3 PS-2 NIST SP800-53 R3 RA-2 NIST SP800-53 R3 SA-2		SIG v6.0: C.2.5.1, C.2.5.2, D.1.3, L.7	GAPP Ref 6.2.1
Data Governance - Classification	DG-02	Data, and objects containing data, shall be assigned a classification based on data type, jurisdiction of origin, jurisdiction domiciled, context, legal constraints, contractual constraints, value, sensitivity, criticality to the organization and third party obligation for retention and prevention of unauthorized disclosure or misuse.	No Change	X	X	X	X	X	COBIT 4.1 PO 2.3, DS 11.6		A.7.2.1	NIST SP800-53 R3 RA-2 NIST SP800-53 R3 AC-4	NIST SP800-53 R3 RA-2 NIST SP800-53 R3 AC-4	PCI DSS v2.0 9.7.1 PCI DSS v2.0 9.10 PCI DSS v2.0 12.3	SIG v6.0: D.1.3, D.2.2	GAPP Ref 1.2.3 GAPP Ref 1.2.6 GAPP Ref 4.1.2 GAPP Ref 8.2.1 GAPP Ref 8.2.5 GAPP Ref 8.2.6
Data Governance - Handling / Labeling / Security Policy	DG-03	Policies and procedures shall be established for labeling, handling and security of data and objects which contain data. Mechanisms for label inheritance shall be implemented for objects that acts as aggregate containers for data.	No Change	X	X	X	X	X	COBIT 4.1 PO 2.3, DS 11.6		A.7.2.2 A.10.7.1 A.10.7.3 A.10.8.1	NIST SP800-53 R3 AC-16 NIST SP800-53 R3 MP-1 NIST SP800-53 R3 MP-3 NIST SP800-53 R3 PE-16 NIST SP800-53 R3 SI-12 NIST SP800-53 R3 SC-9	NIST SP800-53 R3 AC-16 NIST SP800-53 R3 MP-1 NIST SP800-53 R3 MP-3 NIST SP800-53 R3 PE-16 NIST SP800-53 R3 SI-12 NIST SP800-53 R3 SC-9 NIST SP800-53 R3 SC-9 (1)	PCI DSS v2.0 9.5 PCI DSS v2.0 9.6 PCI DSS v2.0 9.7.1 PCI DSS v2.0 9.7.2 PCI DSS v2.0 9.10	AUP v5.0 G.13 SIG v6.0: D.2.2	GAPP Ref 1.1.2 GAPP Ref 5.1.0 GAPP Ref 7.1.2 GAPP Ref 8.1.0 GAPP Ref 8.2.5 GAPP Ref 8.2.8

Copyright © 2010, Cloud Security Alliance

Cloud Controls Matrix (CCM) R1.1

Control Area	Control ID	Control Specification	Control Revisions v1.1	Cloud Service Delivery Model Applicability			Scope Applicability		Compliance Mapping							
				SaaS	PaaS	IaaS	Service Provider	Tenant	COBIT 4.1	HIPAA/HITECH Act	ISO/IEC 27001-2005	NIST SP800-53	FedRAMP	PCI DSS v2.0	BITS Shared Assessments AUP v5.0 / SIG v6.0	GAPP Aug 2009
Data Governance - Retention Policy	DG-04	Policies and procedures for data retention and storage shall be established and backup or redundancy mechanisms implemented to ensure compliance with regulatory, statutory, contractual or business requirements. Testing the recovery of disk or tape backups must be implemented at planned intervals.	Policies and procedures for data retention and storage shall be established and backup or redundancy mechanisms implemented to ensure compliance with regulatory, statutory, contractual or business requirements. Testing the recovery of backups must be implemented at planned intervals. Removed the specific reference to tape and disk backups as there are other media types.	X	X	X	X	X	COBIT 4.1 DS 4.1, DS 4.2, DS 4.5, DS 4.9, DS 11.6	45 CFR 164.308 (a)(7)(ii)(A) 45 CFR 164.310 (d)(2)(iv) 45 CFR 164.306(a)(3)(ii)(C) (New) 45 CFR 164.310(d)(2)(i) (New)	Clause 4.3.3 A.10.5.1 A.10.7.3	NIST SP800-53 R3 CP-2 NIST SP800-53 R3 CP-6 NIST SP800-53 R3 CP-7 NIST SP800-53 R3 CP-8 NIST SP800-53 R3 CP-9 NIST SP800-53 R3 SI-12 NIST SP800-53 R3 AU-11	NIST SP800-53 R3 CP-2 NIST SP800-53 R3 CP-6 (1) NIST SP800-53 R3 CP-6 (2) NIST SP800-53 R3 CP-6 NIST SP800-53 R3 CP-6 (1) NIST SP800-53 R3 CP-6 (3) NIST SP800-53 R3 CP-7 NIST SP800-53 R3 CP-7 (1) NIST SP800-53 R3 CP-7 (2) NIST SP800-53 R3 CP-7 (3) NIST SP800-53 R3 CP-7 (5) NIST SP800-53 R3 CP-8 NIST SP800-53 R3 CP-8 (1) NIST SP800-53 R3 CP-8 (2) NIST SP800-53 R3 CP-9 NIST SP800-53 R3 CP-9 (1) NIST SP800-53 R3 CP-9 (3) NIST SP800-53 R3 SI-12 NIST SP800-53 R3 AU-11	PCI DSS v2.0 9.1 PCI DSS v2.0 9.5.1 PCI DSS v2.0 9.5.1.1 PCI DSS v2.0 9.5.1.2 PCI DSS v2.0 9.9.1 PCI DSS v2.0 9.9.5 PCI DSS v2.0 9.9.6 PCI DSS v2.0 10.7	SIG v6.0: D.2.2.8	GAPP Ref 5.1.0 GAPP Ref 5.1.1 GAPP Ref 5.2.2 GAPP Ref 5.2.6
Data Governance - Secure Disposal	DG-05	Policies and procedures shall be established and mechanisms implemented for the secure disposal and complete removal of data from all storage media, ensuring data is not recoverable by any computer forensic means.	No Change	X	X	X	X		COBIT 4.1 DS 11.4	45 CFR 164.310 (d)(2)(i) 45 CFR 164.310 (d)(2)(ii)	A.9.2.6 A.10.7.2	NIST SP800-53 R3 MP-6 NIST SP800-53 R3 PE-1	NIST SP800-53 R3 MP-6 NIST SP800-53 R3 MP-6 (4) NIST SP800-53 R3 PE-1	PCI DSS v2.0 3.1.1 PCI DSS v2.0 9.10 PCI DSS v2.0 9.10.1 PCI DSS v2.0 9.10.2 PCI DSS v2.0 3.1	SIG v6.0: D.2.2.10, D.2.2.11, D.3.2.14,	GAPP Ref 5.1.0 GAPP Ref 5.2.3
Data Governance - Non-Production Data	DG-06	Production data shall not be replicated or used in non-production environments.	No Change	X	X	X	X			45 CFR 164.308(a)(4)(ii)(B)	A.7.1.3 A.10.1.4 A.12.4.2 A.12.5.1	NIST SP800-53 R3 SA-11 NIST SP800-53 R3 CM-04	NIST SP800-53 R3 SA-11 NIST SP800-53 R3 SA-11 (1) NIST SP800-53 R3 CM-04	PCI DSS v2.0 6.4.3	SIG v6.0: I.2.16	GAPP Ref 1.2.6
Data Governance - Information Leakage	DG-07	Security mechanisms shall be implemented to prevent data leakage.	No Change	X	X	X	X		COBIT 4.1 DS 11.6		A.10.6.2 A.12.5.4	NIST SP800-53 R3 AC-2 NIST SP800-53 R3 AC-3 NIST SP800-53 R3 AC-4 NIST SP800-53 R3 AC-6 NIST SP800-53 R3 AC-11 NIST SP800-53 R3 AU-13 NIST SP800-53 R3 PE-19 NIST SP800-53 R3 SC-28 NIST SP800-53 R3 SA-6 NIST SP800-53 R3 SI-7	NIST SP800-53 R3 AC-2 NIST SP800-53 R3 AC-2 (1) NIST SP800-53 R3 AC-2 (2) NIST SP800-53 R3 AC-2 (3) NIST SP800-53 R3 AC-2 (4) NIST SP800-53 R3 AC-2 (7) NIST SP800-53 R3 AC-3 NIST SP800-53 R3 AC-3 (3) NIST SP800-53 R3 AC-4 NIST SP800-53 R3 AC-6 NIST SP800-53 R3 AC-6 (1) NIST SP800-53 R3 AC-6 (2) NIST SP800-53 R3 AC-11 NIST SP800-53 R3 AC-11 (1) NIST SP800-53 R3 AU-13 NIST SP800-53 R3 PE-19 NIST SP800-53 R3 SC-28 NIST SP800-53 R3 SC-28 (1) NIST SP800-53 R3 SA-6 NIST SP800-53 R3 SI-7 NIST SP800-53 R3 SI-7 (1)	PCI DSS v2.0 1.2 PCI DSS v2.0 6.5.5 PCI DSS v2.0 11.1 PCI DSS v2.0 11.2 PCI DSS v2.0 11.3 PCI DSS v2.0 11.4 PCI DSS v2.0 A.1	SIG v6.0: I.2.16	GAPP Ref 7.2.1 GAPP Ref 8.1.0 GAPP Ref 8.1.1 GAPP Ref 8.2.1 GAPP Ref 8.2.2 GAPP Ref 8.2.5 GAPP Ref 8.2.6
Data Governance - Risk Assessments	DG-08	Risk assessments associated with data governance requirements shall be conducted at planned intervals considering the following: • Awareness of where sensitive data is stored and transmitted across applications, databases, servers and network infrastructure • Compliance with defined retention periods and end-of-life disposal requirements • Data classification and protection from unauthorized use, access, loss, destruction, and falsification	No Change	X	X	X	X	X	COBIT 4.1 PO 9.1, PO 9.2, PO 9.4, DS 5.7	45 CFR 164.308(a)(1)(ii)(A) (New) 45 CFR 164.308(a)(8) (New)	Clause 4.2.1 c) & g) Clause 4.2.3 d) Clause 4.3.1 & 4.3.3 Clause 7.2 & 7.3 A.7.2 A.15.1.1 A.15.1.3 A.15.1.4	NIST SP800-53 R3 CA-3 NIST SP800-53 R3 RA-2 NIST SP800-53 R3 RA-3 NIST SP800-53 R3 MP-8 NIST SP800-53 R3 PM-9 NIST SP800-53 R3 SI-12	NIST SP800-53 R3 CA-3 NIST SP800-53 R3 RA-2 NIST SP800-53 R3 RA-3 NIST SP800-53 R3 MP-8 NIST SP800-53 R3 PM-9 NIST SP800-53 R3 SI-12	PCI DSS v2.0 12.1 PCI DSS v2.0 12.1.2	SIG v6.0: L.4, L.5, L.6, L.7	GAPP Ref 1.2.4 GAPP Ref 8.2.1
Facility Security - Policy	FS-01	Policies and procedures shall be established for maintaining a safe and secure working environment in offices, rooms, facilities and secure areas.	No Change	X	X	X	X	X	COBIT 4.1 DS5.7, DS 12.1, DS 12.4 DS 4.9	45 CFR 164.310 (a)(1) 46 CFR 164.310 (a)(2)(ii) 46 CFR 164.306(a)(3)(ii)(A) (New) 46 CFR 164.310 (a)(2)(iii) (New)	A.5.1.1 A.9.1.3 A.9.1.5	NIST SP800-53 R3 CA-2 NIST SP800-53 R3 PE-1 NIST SP800-53 R3 PE-6 NIST SP800-53 R3 PE-7 NIST SP800-53 R3 PE-8	NIST SP800-53 R3 CA-2 NIST SP800-53 R3 CA-2 (1) NIST SP800-53 R3 PE-1 NIST SP800-53 R3 PE-6 NIST SP800-53 R3 PE-6 (1) NIST SP800-53 R3 PE-7 NIST SP800-53 R3 PE-7 (1) NIST SP800-53 R3 PE-8	PCI DSS v2.0 9.1 PCI DSS v2.0 9.2 PCI DSS v2.0 9.3 PCI DSS v2.0 9.4	AUP v5.0 F.2 SIG v6.0: F.1.1, F.1.2 F.1.3, F.1.4, F.1.5, F.1.5, F.1.7, F.1.8, F.1.9, F.2.1, F.2.2, F.2.3, F.2.4, F.2.5, F2.6, F.2.7, F.2.8, F.2.9, F.2.10, F.2.11, F.2.12, F.2.13, F.2.14, F.2.15, F.2.16, F.2.17, F.2.18,F.2.19, F.2.20	GAPP Ref 8.1.0 GAPP Ref 8.1.1 GAPP Ref 8.2.1
Facility Security - User Access	FS-02	Physical access to information assets and functions by users and support personnel shall be restricted.	No Change				X	X		45 CFR 164.310(a)(1) (New) 45 CFR 164.310(a)(2)(ii) (New) 45 CFR 164.310(b) (New) 45 CFR 164.310 (c) (New)	A.9.1.1 A.9.1.2	NIST SP800-53 R3 PE-2 NIST SP800-53 R3 PE-3 NIST SP800-53 R3 PE-4 NIST SP800-53 R3 PE-5 NIST SP800-53 R3 PE-6	NIST SP800-53 R3 PE-2 NIST SP800-53 R3 PE-2 (1) NIST SP800-53 R3 PE-3 NIST SP800-53 R3 PE-4 NIST SP800-53 R3 PE-5 NIST SP800-53 R3 PE-6 NIST SP800-53 R3 PE-6 (1)	PCI DSS v2.0 9.1	AUP v5.0 H.6 SIG v6.0: F.1.2.3, F.1.2.4, F.1.2.5, F.1.2.6, F.1.2.8, F.1.2. 9, F.1.2.10, F.1.2.11, F.1.2.12, F.1.2.13, F.1.2.14, F.1.2.15, F.1.2.24, F.1.4.2, F1.4.6, F.1.4.7, F.1.7, F.1.8, F.2.13, F.2.14, F.2.15, F.2.16, F.2.17, F.2.18	GAPP Ref 8.2.1 GAPP Ref 8.2.2 GAPP Ref 8.2.3
Facility Security - Controlled Access Points	FS-03	Physical security perimeters (fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks and security patrols) shall be implemented to safeguard sensitive data and information systems.	No Change	X	X	X	X		COBIT 4.1 DS 12.3		A.9.1.1	NIST SP800-53 R3 PE-2 NIST SP800-53 R3 PE-3 NIST SP800-53 R3 PE-6 NIST SP800-53 R3 PE-18	NIST SP800-53 R3 PE-2 NIST SP800-53 R3 PE-2 (1) NIST SP800-53 R3 PE-3 NIST SP800-53 R3 PE-6 NIST SP800-53 R3 PE-6 (1) NIST SP800-53 R3 PE-18	PCI DSS v2.0 9.1	AUP v5.0 F.2 SIG v6.0: F.1.2.3, F.1.2.4, F.1.2.5, F.1.2.6, F.1.2.8, F.1.2. 9, F.1.2.10, F.1.2.11, F.1.2.12, F.1.2.13, F.1.2.14, F.1.2.15, F.1.2.24, F.1.3, F.1.4.2, F1.4.6, F.1.4.7, F.1.6, F.1.7,F.1.8, F.2.13, F.2.14, F.2.15, F.2.16, F.2.17, F.2.18	GAPP Ref 8.2.3

Copyright © 2010, Cloud Security Alliance

Cloud Controls Matrix (CCM) R1.1

Control Area	Control ID	Control Specification	Control Revisions v1.1	Cloud Service Delivery Model Applicability			Scope Applicability		Compliance Mapping							
				SaaS	PaaS	IaaS	Service Provider	Tenant	COBIT 4.1	HIPAA / HITECH Act	ISO/IEC 27001-2005	NIST SP800-53	FedRAMP	PCI DSS v2.0	BITS Shared Assessments AUP v5.0 / SIG v6.0	GAPP (May 2009)
Facility Security - Secure Area Authorization	FS-04	Ingress and egress to secure areas shall be constrained and monitored by physical access control mechanisms to ensure that only authorized personnel are allowed access.	Physical controls and alteration mechanisms shall be designed to address the requirements of legislative, quality and risk results shared with tenants	X	X	X	X		DS 12.3, DS 12.3		A.9.1.1 A.9.1.3	NIST SP800-53 R3 PE-2 NIST SP800-53 R3 PE-3 NIST SP800-53 R3 PE-6 NIST SP800-53 R3 PE-7 NIST SP800-53 R3 PE-8 NIST SP800-53 R3 PE-16	NIST SP800-53 R3 PE-2 NIST SP800-53 R3 PE-3 (1) NIST SP800-53 R3 PE-3 NIST SP800-53 R3 PE-6 NIST SP800-53 R3 PE-6 (1) NIST SP800-53 R3 PE-7 NIST SP800-53 R3 PE-7 (1) NIST SP800-53 R3 PE-8 NIST SP800-53 R3 PE-16	PCI DSS v2.0 9.1 PCI DSS v2.0 9.1.1 PCI DSS v2.0 9.1.2 PCI DSS v2.0 9.1.3 PCI DSS v2.0 9.3	AUP v5.0 F.2 SIG v6.0: F.1.2.3, F.1.2.4, F.1.2.5, F.1.2.6, F.1.2.8, F.1.2.9, F.1.2.10, F.1.2.11, F.1.2.12, F.1.2.13, F.1.2.14, F.1.2.15, F.1.2.24, F.1.3, F.1.4.2, F1.4.6, F.1.4.7, F.1.6, F.1.7,F.1.8, F.2.13, F.2.14, F.2.15, F.2.16, F.2.17, F.2.18	GAPP Ref 8.2.3
Facility Security - Unauthorized Persons Entry	FS-05	Ingress and egress points such as service areas and other points where unauthorized personnel may enter the premises shall be monitored, controlled and, if possible, isolated from data storage and processing facilities to percent unauthorized data corruption, compromise and loss.	No Change	X	X	X	X		COBIT 4.1 DS 12.3		A.9.1.6	NIST SP800-53 R3 PE-7 NIST SP800-53 R3 PE-16 NIST SP800-53 R3 PE-18	NIST SP800-53 R3 PE-7 NIST SP800-53 R3 PE-7 (1) NIST SP800-53 R3 PE-16 NIST SP800-53 R3 PE-18		AUP v5.0 F.2 SIG v6.0: F.1.2.3, F.1.2.4, F.1.2.5, F.1.2.6, F.1.2.8, F.1.2. 9, F.1.2.10, F.1.2.11, F.1.2.12, F.1.2.13, F.1.2.14, F.1.2.15, F.1.2.24, F.1.3, F.1.4.2, F1.4.6, F.1.4.7, F.1.6, F.1.7,F.1.8, F.2.13, F.2.14, F.2.15, F.2.16, F.2.17, F.2.18	GAPP Ref 8.2.3
Facility Security - Off-Site Authorization	FS-06	Authorization must be obtained prior to relocation or transfer of hardware, software or data to an offsite premises.	No Change	X	X	X	X			45 CFR 164.310 (d)(1) (New)	A.9.2.7 A.10.1.2	NIST SP800-53 R3 MA-1 NIST SP800-53 R3 MA-2 NIST SP800-53 R3 PE-16	NIST SP800-53 R3 MA-1 NIST SP800-53 R3 MA-2 NIST SP800-53 R3 MA-2 (1) NIST SP800-53 R3 PE-16	PCI DSS v2.0 9.5 PCI DSS v2.0 9.9	AUP v5.0 G.21 SIG v6.0:F.2.18	GAPP Ref 8.2.5 GAPP Ref 8.2.9
Facility Security - Off-Site Equipment	FS-07	Policies and procedures shall be established for securing and asset management for the use and secure disposal of equipment maintained and used outside the organization's premise.	Policies and procedures governing asset management shall be established for secure reprposing of equipment and resources prior to tenant assignment or jurisdictional transport.	X	X	X	X			45 CFR 164.310 (c) 45 CFR 164.310 (d)(1) (New) 45 CFR 164.310 (d)(2)(i) (New)	A.9.2.5 A.9.2.6	NIST SP800-53 R3 AC-17 NIST SP800-53 R3 MA-1 NIST SP800-53 R3 PE-1 NIST SP800-53 R3 PE-16 NIST SP800-53 R3 PE-17	NIST SP800-53 R3 AC-17 NIST SP800-53 R3 AC-17 (1) NIST SP800-53 R3 AC-17 (2) NIST SP800-53 R3 AC-17 (3) NIST SP800-53 R3 AC-17 (4) NIST SP800-53 R3 AC-17 (5) NIST SP800-53 R3 AC-17 (7) NIST SP800-53 R3 AC-17 (8) NIST SP800-53 R3 MA-1 NIST SP800-53 R3 PE-1 NIST SP800-53 R3 PE-16 NIST SP800-53 R3 PE-17	PCI DSS v2.0 9.8 PCI DSS v2.0 9.9 PCI DSS v2.0 9.10	SIG v6.0:F.2.18, F.2.19,	N/A
Facility Security - Asset Management	FS-08	A complete inventory of critical assets shall be maintained with ownership defined and documented.	No Change	X	X	X	X	X		45 CFR 164.310 (d)(2)(iii)	A.7.1.1 A.7.1.2	NIST SP800-53 R3 CM-8	NIST SP800-53 R3 CM-8 NIST SP800-53 R3 CM-8 (1) NIST SP800-53 R3 CM-8 (3) NIST SP800-53 R3 CM-8 (5)	PCI DSS v2.0 9.9.1 PCI DSS v2.0 12.3.3 PCI DSS v2.0 12.3.4	AUP v5.0 D.1 SIG v6.0: D.1.1, D.2.1. D.2.2,	N/A
Human Resources Security - Background Screening	HR-01	Pursuant to local laws, regulations, ethics and contractual constraints all employment candidates, contractors and third parties will be subject to background verification proportional to the data classification to be accessed, the business requirements and acceptable risk.	No Change	X	X	X	X	X	COBIT 4.1 PO 7.6		A.8.1.2	NIST SP800-53 R3 PS-2 NIST SP800-53 R3 PS-3	NIST SP800-53 R3 PS-2 NIST SP800-53 R3 PS-3	PCI DSS v2.0 12.7 PCI DSS v2.0 12.8.3	AUP v5.0 E.2 SIG v6.0: E.2	GAPP Ref 1.2.9
Human Resources Security - Employment Agreements	HR-02	Prior to granting individuals physical or logical access to facilities, systems or data employees, contractors, third party users and customers shall contractually agree and sign the terms and conditions of their employment or service contract, which must explicitly include the parties responsibility for information security.	Prior to granting individuals physical or logical access to facilities, systems or data employees, contractors, third party contractors and tenants shall contractually agree and sign equivalent terms and conditions regarding information security responsibilities in employment or service contract	X	X	X	X	X	COBIT DS 2.1	45 CFR 164.310(a)(1) (New) 45 CFR 164.308(a)(4)(i) (New)	A.6.1.5 A.8.1.3	NIST SP800-53 R3 PL-4 NIST SP800-53 R3 PS-6 NIST SP800-53 R3 PS-7	NIST SP800-53 R3 PL-4 NIST SP800-53 R3 PS-6 NIST SP800-53 R3 PS-7	PCI DSS v2.0 12.4 PCI DSS v2.0 12.8.2	AUP v5.0 C.1 SIG v6.0: E.3.5	GAPP Ref 1.2.9 GAPP Ref 8.2.6
Human Resources - Employment Termination	HR-03	Roles and responsibilities for following performing employment termination or change in employment procedures shall be assigned, documented and communicated.	Roles and responsibilities following employment termination or change in employment procedures must follow the terms of the master agreement with the tenant(s).	X	X	X	X	X	COBIT 4.1 PO 7.8	45 CFR 164.308 (a)(3)(ii)(C)	A.8.3.1	NIST SP800-53 R3 PS-4 NIST SP800-53 R2 PS-5	NIST SP800-53 R3 PS-4 NIST SP800-53 R3 PS-5		SIG v6.0: E.6	GAPP Ref 8.2.2 GAPP Ref 10.2.5
Information Security - Management Program	IS-01	An Information Security Management Program (ISMP) has been developed, documented, approved, and implemented that includes administrative, technical, and physical safeguards to protect assets and data from loss, misuse, unauthorized access, disclosure, alteration, and destruction. The security program should address, but not be limited to, the following areas insofar as they relate to the characteristics of the business: • Risk management • Security policy • Organization of information security • Asset management • Human resources security • Physical and environmental security • Communications and operations management • Access control • Information systems acquisition, development, and maintenance	No Change	X	X	X	X	X	COBIT 4.1 R2 DS5.2 COBIT 4.1 R2 DS5.5	45 CFR 164.308(a)(1)(i) 45 CFR 164.308(a)(1)(ii)(B) 45 CFR 164.316(b)(1)(i) 45 CFR 164.308(a)(3)(i) (New) 45 CFR 164.308(a) (New)	Clause 4.2 Clause 5 A.5.1.1 A.5.1.2 A.5.1.3 A.5.1.4 A.5.1.5 A.5.1.6 A.5.1.7 A.5.1.8	NIST SP800-53 R3 PM-1 NIST SP800-53 R3 PM-2 NIST SP800-53 R3 PM-3 NIST SP800-53 R3 PM-4 NIST SP800-53 R3 PM-5 NIST SP800-53 R3 PM-6 NIST SP800-53 R3 PM-7 NIST SP800-53 R3 PM-8 NIST SP800-53 R3 PM-9 NIST SP800-53 R3 PM-10 NIST SP800-53 R3 PM-11	NIST SP800-53 R3 PM-1 NIST SP800-53 R3 PM-2 NIST SP800-53 R3 PM-3 NIST SP800-53 R3 PM-4 NIST SP800-53 R3 PM-5 NIST SP800-53 R3 PM-6 NIST SP800-53 R3 PM-7 NIST SP800-53 R3 PM-8 NIST SP800-53 R3 PM-9 NIST SP800-53 R3 PM-10 NIST SP800-53 R3 PM-11	PCI DSS v2.0 12.1 PCI DSS v2.0 12.2	SIG v6.0: A.1, B.1	GAPP Ref 8.2.1
Information Security - Management Support / Involvement	IS-02	Executive and line management shall take formal action to support information security through clear documented direction, commitment, explicit assignment and verification of assignment execution	No Change	X	X	X	X		COBIT 4.1 DS5.1	45 CFR 164.316 (b)(2)(ii) 45 CFR 164.316 (b)(2)(iii)	Clause 5 A.6.1.1	NIST SP800-53 R3 CM-1 NIST SP800-53 R3 PM-1 NIST SP800-53 R3 PM-11	NIST SP800-53 R3 CM-1 NIST SP800-53 R3 PM-1 NIST SP800-53 R3 PM-11	PCI DSS v2.0 12.5	SIG v6.0: C.1	GAPP Ref 8.2.1

Copyright © 2010, Cloud Security Alliance

Cloud Controls Matrix (CCM) R1.1

Control Area	Control ID	Control Specification	Control Relevance v1.1	Cloud Service Delivery Model Applicability			Scope Applicability		Compliance Mapping							
				SaaS	PaaS	IaaS	Service Provider	Tenant	COBIT 4.1	HIPAA / HITECH Act	ISO/IEC 27001:2005	NIST SP800-53	FedRAMP	PCI DSS v2.0	BITS Shared Assessments AUP v5.0 / SIG v6.0	GAPP (Aug 2009)
Information Security - Policy	IS-03	Management shall approve a formal information security policy document which shall be communicated and published to employees, contractors and other relevant external parties. The Information Security Policy shall establish the direction of the organization and align to best practices, regulatory, federal/state and international laws where applicable. The information security policy shall be supported by a strategic plan and a security program with well defined roles and responsibilities for senior leadership and other roles.	No Change	X	X	X	X	X	COBIT 4.1 DS5.2	45 CFR 164.316 (a) 45 CFR 164.316 (b)(1)(i) 45 CFR 164.316 (b)(2)(ii) 45 CFR 164.308(a)(2) (New)	Clause 4.2.1 Clause 5 A.5.1.1 A.6.2.3	NIST SP800-53 R3 AC-1 NIST SP800-53 R3 AT-1 NIST SP800-53 R3 AU-1 NIST SP800-53 R3 CA-1 NIST SP800-53 R3 CM-1 NIST SP800-53 R3 IA-1 NIST SP800-53 R3 IR-1 NIST SP800-53 R3 MA-1 NIST SP800-53 R3 MP-1 NIST SP800-53 R3 MP-1 NIST SP800-53 R3 PE-1 NIST SP800-53 R3 PL-1 NIST SP800-53 R3 PS-1 NIST SP800-53 R3 SA-1 NIST SP800-53 R3 SC-1 NIST SP800-53 R3 SI-1	NIST SP800-53 R3 AC-1 NIST SP800-53 R3 AT-1 NIST SP800-53 R3 AU-1 NIST SP800-53 R3 CA-1 NIST SP800-53 R3 CM-1 NIST SP800-53 R3 IA-1 NIST SP800-53 R3 IR-1 NIST SP800-53 R3 MA-1 NIST SP800-53 R3 MP-1 NIST SP800-53 R3 MP-1 NIST SP800-53 R3 PE-1 NIST SP800-53 R3 PL-1 NIST SP800-53 R3 PS-1 NIST SP800-53 R3 SA-1 NIST SP800-53 R3 SC-1 NIST SP800-53 R3 SI-1	PCI DSS v2.0 12.1 PCI DSS v2.0 12.2	SIG v6.0 B.1	GAPP Ref 8.1.0 GAPP Ref 8.1.1
Information Security - Baseline Requirements	IS-04	Baseline security requirements shall be established and applied to the design and implementation of (developed or purchased) applications, databases, systems, and network infrastructure and information processing that comply with policies, standards and applicable regulatory requirements. Compliance with security baseline requirements must be assessed at least annually or upon significant changes.	No Change	X	X	X	X		COBIT 4.1 AI2.1 COBIT 4.1 AI2.2 COBIT 4.1 AI3.3 COBIT 4.1 DS2.3 COBIT 4.1 DS11.6		A.12.1.1 A.15.2.2	NIST SP800-53 R3 CM-2 NIST SP800-53 R3 SA-2 NIST SP800-53 R3 SA-4	NIST SP800-53 R3 CM-2 NIST SP800-53 R3 CM-2 (1) NIST SP800-53 R3 CM-2 (3) NIST SP800-53 R3 CM-2 (5) NIST SP800-53 R3 SA-2 NIST SP800-53 R3 SA-4 NIST SP800-53 R3 SA-4 (1) NIST SP800-53 R3 SA-4 (4) NIST SP800-53 R3 SA-4 (7)	PCI DSS v1.2 1.1 PCI DSS v1.2 1.1.1 PCI DSS v1.2 1.1.2 PCI DSS v1.2 1.1.3 PCI DSS v1.2 1.1.4 PCI DSS v1.2 1.1.5 PCI DSS v1.2 1.1.6 PCI DSS v1.2 2.2 PCI DSS v1.2 2.2.1 PCI DSS v1.2 2.2.2 PCI DSS v1.2 2.2.3 PCI DSS v1.2 2.2.4	AUP v5.0 L.2 SIG v6.0: L.2, L.5, L.7 L.8, L.9, L.10	GAPP Ref 1.2.6 GAPP Ref 8.2.1 GAPP Ref 8.2.7
Information Security - Policy Reviews	IS-05	Management shall review the information security policy at planned intervals or as a result of changes to the organization to ensure its continuing effectiveness and accuracy.	Security policy changes with material operational impact must require formal notification of subcontractors, tenants, supporting service tiers and employees of the impact and ramifications.	X	X	X	X	X	COBIT 4.1 DS 5.2 DS 5.4	45 CFR 164.316 (b)(2)(iii) 45 CFR 164.306(e) (New)	Clause 4.2.3 f) A.5.1.2	NIST SP800-53 R3 AC-1 NIST SP800-53 R3 AT-1 NIST SP800-53 R3 AU-1 NIST SP800-53 R3 CA-1 NIST SP800-53 R3 CM-1 NIST SP800-53 R3 CP-1 NIST SP800-53 R3 IA-1 NIST SP800-53 R3 IA-5 NIST SP800-53 R3 IR-1 NIST SP800-53 R3 MA-1 NIST SP800-53 R3 MP-1 NIST SP800-53 R3 PE-1 NIST SP800-53 R3 PL-1 NIST SP800-53 R3 PM-1 NIST SP800-53 R3 PS-1 NIST SP800-53 R3 RA-1 NIST SP800-53 R3 SA-1 NIST SP800-53 R3 SC-1 NIST SP800-53 R3 SI-1	NIST SP800-53 R3 AC-1 NIST SP800-53 R3 AT-1 NIST SP800-53 R3 AU-1 NIST SP800-53 R3 CA-1 NIST SP800-53 R3 CM-1 NIST SP800-53 R3 CP-1 NIST SP800-53 R3 IA-1 NIST SP800-53 R3 IA-5 NIST SP800-53 R3 IA-5 (1) NIST SP800-53 R3 IA-5 (2) NIST SP800-53 R3 IA-5 (3) NIST SP800-53 R3 IA-5 (6) NIST SP800-53 R3 IA-5 (7) NIST SP800-53 R3 IR-1 NIST SP800-53 R3 MA-1 NIST SP800-53 R3 MP-1 NIST SP800-53 R3 PE-1 NIST SP800-53 R3 PL-1 NIST SP800-53 R3 PM-1 NIST SP800-53 R3 PS-1 NIST SP800-53 R3 RA-1 NIST SP800-53 R3 SA-1 NIST SP800-53 R3 SC-1 NIST SP800-53 R3 SI-1	PCI DSS v2.0 12.1.3	AUP v5.0 B.2 SIG v6.0: B.1.33, B.1.34,	GAPP Ref 1.2.1 GAPP Ref 8.2.7 GAPP Ref 10.2.3
Information Security - Policy Enforcement	IS-06	A formal disciplinary or sanction policy shall be established for employees who have violated security policies and procedures. Employees shall be made aware of what action might be taken in the event of a violation and stated as such in the policies and procedures.	No Change	X	X	X	X	X	COBIT 4.1 PO 7.7	45 CFR 164.308 (a)(1)(ii)(C)	A.8.2.3	NIST SP800-53 R3 PL-4 NIST SP800-53 R3 PS-1 NIST SP800-53 R3 PS-8	NIST SP800-53 R3 PL-4 NIST SP800-53 R3 PS-1 NIST SP800-53 R3 PS-8		SIG v6.0:B.1.6	GAPP Ref 10.2.4
Information Security - User Access Policy	IS-07	User access policies and procedures shall be documented, approved and implemented for granting and revoking normal and privileged access to applications, databases, and server and network infrastructure in accordance with business, security, compliance and service level agreement (SLA) requirements.	No Change	X	X	X	X		COBIT 4.1 DS 5.4	45 CFR 164.308 (a)(3)(i) 45 CFR 164.312 (a)(1) 45 CFR 164.312 (a)(2)(ii) 45 CFR 164.308(a)(4)(ii)(B) (New) 45 CFR 164.308(a)(4)(ii)(c) (New)	A.11.1.1 A.11.2.1 A.11.2.4 A.11.4.1 A.11.5.2 A.11.6.1	NIST SP800-53 R3 AC-1 NIST SP800-53 R3 IA-1	NIST SP800-53 R3 AC-1 NIST SP800-53 R3 IA-1	PCI DSS v2.0 3.5.1 PCI DSS v2.0 8.5.1 PCI DSS v2.0 12.5.4	AUP v5.0 B.1 SIG v6.0: B.1.8, B.1.21, B.1.28, E.5.2, H.1.1, K.1.4.5,	GAPP Ref 8.1.0
Information Security - User Access Restriction / Authorization	IS-08	Normal and privileged user access to applications, systems, databases, network configurations, and sensitive data and functions shall be restricted and approved by management prior to access granted.	No Change	X	X	X	X	X	COBIT 4.1 DS5.4	45 CFR 164.308 (a)(3)(i) 45 CFR 164.308 (a)(3)(ii)(A) 45 CFR 164.308 (a)(4)(i) 45 CFR 164.308 (a)(4)(ii)(B) 45 CFR 164.308 (a)(4)(ii)(C) 45 CFR 164.312 (a)(1)	A.11.2.1 A.11.2.2 A.11.4.1 A.11.4.2 A.11.6.1	NIST SP800-53 R3 AC-3 NIST SP800-53 R3 AC-5 NIST SP800-53 R3 AC-6 NIST SP800-53 R3 IA-2 NIST SP800-53 R3 IA-4 NIST SP800-53 R3 IA-5 NIST SP800-53 R3 IA-8 NIST SP800-53 R3 MA-5 NIST SP800-53 R3 PS-6 NIST SP800-53 R3 SA-7 NIST SP800-53 R3 SI-9	NIST SP800-53 R3 AC-3 NIST SP800-53 R3 AC-3 (3) NIST SP800-53 R3 AC-5 NIST SP800-53 R3 AC-6 NIST SP800-53 R3 AC-6 (1) NIST SP800-53 R3 AC-6 (2) NIST SP800-53 R3 IA-2 NIST SP800-53 R3 IA-2 (1) NIST SP800-53 R3 IA-2 (2) NIST SP800-53 R3 IA-2 (3) NIST SP800-53 R3 IA-2 (8) NIST SP800-53 R3 IA-4 NIST SP800-53 R3 IA-4 (4) NIST SP800-53 R3 IA-5 NIST SP800-53 R3 IA-5 (1) NIST SP800-53 R3 IA-5 (2) NIST SP800-53 R3 IA-5 (3) NIST SP800-53 R3 IA-5 (6) NIST SP800-53 R3 IA-5 (7) NIST SP800-53 R3 IA-8 NIST SP800-53 R3 MA-5 NIST SP800-53 R3 PS-6 NIST SP800-53 R3 SA-7 NIST SP800-53 R3 SI-9	PCI DSS v2.0 7.1 PCI DSS v2.0 7.1.1 PCI DSS v2.0 7.1.2 PCI DSS v2.0 7.1.3 PCI DSS v2.0 7.2.1 PCI DSS v2.0 7.2.2 PCI DSS v2.0 8.5.1 PCI DSS v2.0 12.5.4	SIG v6.0: H.2.4, H.2.5,	GAPP Ref 8.2.2
Information Security - User Access Revocation	IS-09	Timely deprovisioning, revocation or modification of user access to the organizations systems, information assets and data shall be implemented upon any change in status of employees, contractors, customers, business partners or third parties. Any change in status is intended to include termination of employment, contract or agreement, change of employment or transfer within the organization.	No Change	X	X	X	X		COBIT 4.1 DS 5.4	45 CFR 164.308(a)(3)(ii)(C)	ISO/IEC 27001:2005 A.8.3.3 A.11.1.1 A.11.2.1 A.11.2.2	NIST SP800-53 R3 AC-2 NIST SP800-53 R3 PS-4 NIST SP800-53 R3 PS-5	NIST SP800-53 R3 AC-2 NIST SP800-53 R3 AC-2 (1) NIST SP800-53 R3 AC-2 (2) NIST SP800-53 R3 AC-2 (3) NIST SP800-53 R3 AC-2 (4) NIST SP800-53 R3 AC-2 (7) NIST SP800-53 R3 PS-4 NIST SP800-53 R3 PS-5	PCI DSS v2.0 8.5.4 PCI DSS v2.0 8.5.5	AUP v5.0 H.2 SIG v6.0: E.6.2, E.6.3	GAPP Ref 8.2.1

Copyright © 2010, Cloud Security Alliance

Cloud Controls Matrix (CCM) R1.1

Control Area	Control ID	Control Specification	Control Posture v1.1	Cloud Service Delivery Model Applicability			Scope Applicability		Compliance Mapping							
				SaaS	PaaS	IaaS	Service Provider	Tenant	COBIT 4.1	HIPAA / HITECH Act	ISO/IEC 27001-2005	NIST SP800-53	FedRAMP	PCI DSS v2.0	BITS Shared Assessments AUP v5.0 / SIG v6.0	GAPP (Aug 2009)
Information Security - User Access Review	IS-10	All levels of user access shall be reviewed by management at planned intervals and documented. For access violations identified, remediation must follow documented access control policies and procedures.	Periodic attestation of entitlement rights for all system users is required. Attestation for entitlement rights should extend to users in supporting service lines SaaS, SaaS, PaaS, IOaaS, . 3. Automated or manual notification shall be implemented for identified violations.	X	X	X	X	X	COBIT 4.1 DS5.3 COBIT 4.1 DS5.4	45 CFR 164.308 (a)(3)(ii)(B) 45 CFR 164.308 (a)(4)(ii)(C)	A.11.2.4	NIST SP800-53 R3 AC-2 NIST SP800-53 R3 AU-6 NIST SP800-53 R3 PM-10 NIST SP800-53 R3 PS-6 NIST SP800-53 R3 PS-7	NIST SP800-53 R3 AC-2 NIST SP800-53 R3 AC-2 (1) NIST SP800-53 R3 AC-2 (2) NIST SP800-53 R3 AC-2 (3) NIST SP800-53 R3 AC-2 (4) NIST SP800-53 R3 AC-2 (7) NIST SP800-53 R3 AU-6 NIST SP800-53 R3 AU-6 (1) NIST SP800-53 R3 AU-6 (3) NIST SP800-53 R3 PM-10 NIST SP800-53 R3 PS-6 NIST SP800-53 R3 PS-7		SIG v6.0:H.2.6, H.2.7, H.2.8,	GAPP Ref 8.2.1 GAPP Ref 8.2.7
Information Security - Training / Awareness	IS-11	A security awareness training program shall be established for all contractors, third party users and employees of the organization and mandated when appropriate. All individuals with access to organizational data shall receive appropriate awareness training and regular updates in organizational procedures, process and policies, relating to their function relative to the organization.	A security awareness training program that addresses multi-tenant, nationality and cloud delivery model SOD and conflicts of interest shall be established for all contractors, third party users, tenants and employees of the organization. All individuals with access to tenant data shall receive appropriate awareness training and regular updates in organizational procedures, process and policies, relating to their function relative to the organization.	X	X	X	X	X	COBIT 4.1 PO 7.4	45 CFR 164.308 (a)(5)(i) 45 CFR 164.308 (a)(5)(ii)(A)	Clause 5.2.2 A.8.2.2	NIST SP800-53 R3 AT-1 NIST SP800-53 R3 AT-2 NIST SP800-53 R3 AT-3 NIST SP800-53 R3 AT-4	NIST SP800-53 R3 AT-1 NIST SP800-53 R3 AT-2 NIST SP800-53 R3 AT-3 NIST SP800-53 R3 AT-4	PCI DSS v2.0 12.6 PCI DSS v2.0 12.6.1 PCI DSS v2.0 12.6.2	AUP v5.0 E.1 SIG v6.0:E.4	GAPP Ref 1.2.10 GAPP Ref 8.2.1
Information Security - Industry Knowledge / Benchmarking	IS-12	Industry security knowledge and benchmarking through networking, specialist security forums, and professional associations shall be maintained.	No Change	X	X	X	X	X			A.6.1.7	NIST SP800-53 R3 AT-5 NIST SP800-53 R3 SI-5	NIST SP800-53 R3 AT-5 NIST SP800-53 R3 SI-5		SIG v6.0:C.1.8	N/A
Information Security - Roles / Responsibilities	IS-13	Roles and responsibilities of contractors, employees and third party users shall be documented as they relate to information assets and security.	No Change	X	X	X	X	X	COBIT 4.1 DS5.1		Clause 5.1 c) A.6.1.2 A.6.1.3 A.8.1.1	NIST SP800-53 R3 AT-3 NIST SP800-53 R3 PL-4 NIST SP800-53 R3 PM-10 NIST SP800-53 R3 PS-1 NIST SP800-53 R3 PS-6 NIST SP800-53 R3 PS-7	NIST SP800-53 R3 AT-3 NIST SP800-53 R3 PL-4 NIST SP800-53 R3 PM-10 NIST SP800-53 R3 PS-1 NIST SP800-53 R3 PS-6 NIST SP800-53 R3 PS-7		AUP v5.0 B.1 SIG v6.0: B.1.5, D.1.1, D.1.3.3, E.1, F.1.1, H.1.1, K.1.2	GAPP Ref 1.2.9 GAPP Ref 8.2.1
Information Security - Management Oversight	IS-14	Managers are responsible for maintaining awareness of and complying with security policies, procedures and standards that are relevant to their area of responsibility.	No Change	X	X	X	X	X	COBIT 4.1 DS5.3 COBIT 4.1 DS5.4 COBIT 4.1 DS5.5		Clause 5.2.2 A.8.2.1 A.8.2.2 A.11.2.4 A.15.2.1	NIST SP800-53 R3 AT-2 NIST SP800-53 R3 AT-3 NIST SP800-53 R3 CA-1 NIST SP800-53 R3 CA-5 NIST SP800-53 R3 CA-6 NIST SP800-53 R3 CA-7 NIST SP800-53 R3 PM-10	NIST SP800-53 R3 AT-2 NIST SP800-53 R3 AT-3 NIST SP800-53 R3 CA-1 NIST SP800-53 R3 CA-5 NIST SP800-53 R3 CA-6 NIST SP800-53 R3 CA-7 NIST SP800-53 R3 CA-7 (2) NIST SP800-53 R3 PM-10	PCI DSS v2.0 12.6.1 PCI DSS v2.0 12.6.2	AUP v5.0 E.1 SIG v6.0: E.4	GAPP Ref 1.1.2 GAPP Ref 8.2.1
Information Security - Segregation of Duties	IS-15	Policies, process and procedures shall be implemented to enforce and assure proper segregation of duties. In those events where user-role conflict of interest constraint exist, technical controls shall be in place to mitigate any risks arising from unauthorized or unintentional modification or misuse of the organization's information assets.	No Change	X	X	X	X		COBIT 4.1 DS 5.4	45 CFR 164.308 (a)(1)(i)(C) 45 CFR 164.308 (a)(3)(i)(A) 45 CFR 164.308(a)(4)(ii)(A) (New) 45 CFR 164.308 (a)(5)(ii)(C) 45 CFR 164.312 (c)	A.10.1.3	NIST SP800-53 R3 AC-1 NIST SP800-53 R3 AC-2 NIST SP800-53 R3 AC-5 NIST SP800-53 R3 AC-6 NIST SP800-53 R3 AU-1 NIST SP800-53 R3 AU-6 NIST SP800-53 R3 SI-1 NIST SP800-53 R3 SI-4	NIST SP800-53 R3 AC-1 NIST SP800-53 R3 AC-2 NIST SP800-53 R3 AC-2 (1) NIST SP800-53 R3 AC-2 (2) NIST SP800-53 R3 AC-2 (3) NIST SP800-53 R3 AC-2 (4) NIST SP800-53 R3 AC-2 (7) NIST SP800-53 R3 AC-5 NIST SP800-53 R3 AC-6 NIST SP800-53 R3 AC-6 (1) NIST SP800-53 R3 AC-6 (2) NIST SP800-53 R3 AU-1 NIST SP800-53 R3 AU-6 NIST SP800-53 R3 AU-6 (1) NIST SP800-53 R3 AU-6 (3) NIST SP800-53 R3 SI-1 NIST SP800-53 R3 SI-4 NIST SP800-53 R3 SI-4 (2) NIST SP800-53 R3 SI-4 (4) NIST SP800-53 R3 SI-4 (5) NIST SP800-53 R3 SI-4 (6)	PCI DSS v2.0 6.4.2	SIG v6.0:G.2.13, G.3, G.20.1, G.20.2, G.20.5	GAPP Ref 8.2.2
Information Security - User Responsibility	IS-16	Users shall be made aware of their responsibilities for: • Maintaining awareness and compliance with published security policies, procedures, standards and applicable regulatory requirements • Maintaining a safe and secure working environment • Leaving unattended equipment in a secure manner	No Change	X	X	X	X	X	COBIT 4.1 PO 4.6	45 CFR 164.308 (a)(5)(ii)(D)	Clause 5.2.2 A.8.2.2 A.11.3.1 A.11.3.2	NIST SP800-53 R3 AT-2 NIST SP800-53 R3 AT-3 NIST SP800-53 R3 AT-4 NIST SP800-53 R3 PL-4	NIST SP800-53 R3 AT-2 NIST SP800-53 R3 AT-3 NIST SP800-53 R3 AT-4 NIST SP800-53 R3 PL-4	PCI DSS v2.0 5.5.7 PCI DSS v2.0 12.6.1	AUP v5.0 E.1 SIG v6.0: E.4	GAPP Ref 1.2.10 GAPP Ref 8.2.1
Information Security - Workspace	IS-17	Policies and procedures shall be established for clearing visible documents containing sensitive data when a workspace is unattended and enforcement of workstation session logout for a period of inactivity.	Policies and procedures shall be established for proper data management within the provider environment. Policies and procedures must resolve conflicts of interests and include a tamper audit function, that trips a tamper audit to the customer if the integrity of the tenant data has potentially been compromised. (access not authorized by tenant or data loss)	X	X	X	X	X			Clause 5.2.2 A.8.2.2 A.9.1.5 A.11.3.1 A.11.3.2 A.11.3.3	NIST SP800-53 R3 AC-11 NIST SP800-53 R3 MP-2 NIST SP800-53 R3 MP-3 NIST SP800-53 R3 MP-4	NIST SP800-53 R3 AC-11 NIST SP800-53 R3 AC-11 (1) NIST SP800-53 R3 MP-2 NIST SP800-53 R3 MP-2 (1) NIST SP800-53 R3 MP-3 NIST SP800-53 R3 MP-4 NIST SP800-53 R3 MP-4 (1)		AUP v5.0 E.1 SIG v6.0: E.4	GAPP Ref 8.2.3

Copyright © 2010, Cloud Security Alliance

Control Area	Control ID	Control Specification	Control Revisions v1.3	Cloud Service Delivery Model Applicability			Scope Applicability		Compliance Mapping							
				SaaS	PaaS	IaaS	Service Provider	Tenant	COBIT 4.1	HIPAA / HITECH Act	ISO/IEC 27001:2005	NIST SP800-53	FedRAMP	PCI DSS v2.0	2013 Shared Assessments AUP v5.0 / SIG v6.0	GAPP (Aug 2009)
Information Security - Encryption	IS-18	Policies and procedures shall be established and mechanisms implemented for encrypting sensitive data in storage (e.g., file servers, databases, and end-user workstations) and data in transmission (e.g., system interfaces, over public networks, and electronic messaging).	No Change	X	X	X	X		COBIT 4.1 DS5.8 COBIT 4.1 DS5.10 COBIT 4.1 DS5.11	45 CFR 164.312 (a)(2)(iv) 45 CFR 164.312 (e)(2) 45 CFR 164.312 (e)(2)(ii)	A.10.8.3 A.10.8.4 A.12.3.1 A.15.1.3 A.15.1.4	NIST SP800-53 R3 AC-18 NIST SP800-53 R3 IA-3 NIST SP800-53 R3 IA-7 NIST SP800-53 R3 SC-7 NIST SP800-53 R3 SC-8 NIST SP800-53 R3 SC-9 NIST SP800-53 R3 SC-13 NIST SP800-53 R3 SC-18 NIST SP800-53 R3 SC-23 NIST SP800-53 R3 SI-8	NIST SP800-53 R3 AC-18 NIST SP800-53 R3 AC-18 (1) NIST SP800-53 R3 AC-18 (2) NIST SP800-53 R3 AC-18 (3) NIST SP800-53 R3 AC-18 (4) NIST SP800-53 R3 AC-18 (5) NIST SP800-53 R3 IA-3 NIST SP800-53 R3 IA-7 NIST SP800-53 R3 SC-7 NIST SP800-53 R3 SC-7 (1) NIST SP800-53 R3 SC-7 (2) NIST SP800-53 R3 SC-7 (3) NIST SP800-53 R3 SC-7 (4) NIST SP800-53 R3 SC-7 (5) NIST SP800-53 R3 SC-7 (7) NIST SP800-53 R3 SC-7 (8) NIST SP800-53 R3 SC-7 (12) NIST SP800-53 R3 SC-7 (13) NIST SP800-53 R3 SC-7 (18) NIST SP800-53 R3 SC-8 NIST SP800-53 R3 SC-8 (1) NIST SP800-53 R3 SC-9 NIST SP800-53 R3 SC-9 (1) NIST SP800-53 R3 SC-13 NIST SP800-53 R3 SC-13 (1) NIST SP800-53 R3 SC-16 NIST SP800-53 R3 SC-23 NIST SP800-53 R3 SI-8	PCI-DSS v2.0 2.1.1 PCI-DSS v2.0 3.4 PCI-DSS v2.0 3.4.1 PCI-DSS v2.0 4.1 PCI-DSS v2.0 4.1.1<PCI-DSS v2.0 4.1.1 PCI DSS v2.0 4.2	AUP v5.0 G.8 AUP v5.0 G.15 AUP v5.0 J.1 SIG v6.0: 3.10.4, G.11.1, G.11.2, G.12.1, G.12.3, G.12.4, G.12.10, G.14.18, G.14.19, G.15.2, G.16.10, G.16.15, G.17.16, G.17.17, G.18.13, G.18.14, G.19.1.1, G.20.14	GAPP Ref 8.2.1 GAPP Ref 8.2.5 GAPP Ref 8.2.6
Information Security - Encryption Key Management	IS-19	Policies and procedures shall be established and mechanisms implemented for effective key management to support encryption of data in storage and in transmission.	No Change	X	X	X	X		COBIT 4.1 DS5.8	45 CFR 164.312 (a)(2)(iv) 45 CFR 164.312(e)(1) (New)	Clause 4.3.3 A.10.7.3 A.12.3.2 A.15.1.6	NIST SP800-53 R3 SC-12 NIST SP800-53 R3 SC-13 NIST SP800-53 R3 SC-17 NIST SP800-53 R3 SC-28	NIST SP800-53 R3 SC-12 NIST SP800-53 R3 SC-12 (2) NIST SP800-53 R3 SC-12 (6) NIST SP800-53 R3 SC-13 NIST SP800-53 R3 SC-13 (1) NIST SP800-53 R3 SC-17 NIST SP800-53 R3 SC-28 NIST SP800-53 R3 SC-28 (1)	PCI-DSS v2.0 3.4.1 PCI-DSS v2.0 3.5 PCI-DSS v2.0 3.5.1 PCI-DSS v2.0 3.5.2 PCI-DSS v2.0 3.6 PCI-DSS v2.0 3.6.1 PCI-DSS v2.0 3.6.2 PCI-DSS v2.0 3.6.3 PCI-DSS v2.0 3.6.4 PCI-DSS v2.0 3.6.5 PCI-DSS v2.0 3.6.6 PCI-DSS v2.0 3.6.7 PCI-DSS v2.0 3.6.8	SIG v6.0: L.6	GAPP Ref 8.1.1 GAPP Ref 8.2.1 GAPP Ref 8.2.5
Information Security - Vulnerability / Patch Management	IS-20	Policies and procedures shall be established and mechanism implemented for vulnerability and patch management, ensuring that application, system, and network device vulnerabilities are evaluated and vendor-supplied security patches applied in a timely manner taking a risk-based approach for prioritizing critical patches.	No Change	X	X	X	X		COBIT 4.1 AI6.1 COBIT 4.1 AI3.3 COBIT 4.1 DS5.9	45 CFR 164.308 (a)(1)(i)(i)(A) 45 CFR 164.308 (a)(1)(i)(i)(B) 45 CFR 164.308 (a)(5)(i)(i)(B)	A.12.5.1 A.12.5.2 A.12.6.1	NIST SP800-53 R3 CM-3 NIST SP800-53 R3 CM-4 NIST SP800-53 R3 CP-10 NIST SP800-53 R3 RA-5 NIST SP800-53 R3 SA-7 NIST SP800-53 R3 SI-1 NIST SP800-53 R3 SI-2 NIST SP800-53 R3 SI-5	NIST SP800-53 R3 CM-3 NIST SP800-53 R3 CM-3 (2) NIST SP800-53 R3 CM-4 NIST SP800-53 R3 CP-10 NIST SP800-53 R3 CP-10 (2) NIST SP800-53 R3 CP-10 (3) NIST SP800-53 R3 RA-5 NIST SP800-53 R3 RA-5 (1) NIST SP800-53 R3 RA-5 (2) NIST SP800-53 R3 RA-5 (3) NIST SP800-53 R3 RA-5 (6) NIST SP800-53 R3 RA-5 (8) NIST SP800-53 R3 SA-7 NIST SP800-53 R3 SI-1 NIST SP800-53 R3 SI-2 NIST SP800-53 R3 SI-2 (2) NIST SP800-53 R3 SI-5	PCI-DSS v2.0 2.2 PCI-DSS v2.0 5.1 PCI-DSS v2.0 6.2 PCI-DSS v2.0 6.3.2 PCI-DSS v2.0 6.4.5 PCI-DSS v2.0 6.5.X PCI-DSS v2.0 6.6 PCI-DSS v2.0 11.2 PCI-DSS v2.0 11.2.1 PCI-DSS v2.0 11.2.2 PCI-DSS v2.0 11.2.3	AUP v5.0 I.4 SIG v6.0: G.15.2, I.3	GAPP Ref 1.2.5 GAPP Ref 8.2.7
Information Security - Anti-Virus / Malicious Software	IS-21	Ensure that all antivirus programs are capable of detecting, removing, and protecting against all known types of malicious or unauthorized software with antivirus signature updates at least every 12 hours.	No Change	X	X	X	X	X	COBIT 4.1 DS5.9	45 CFR 164.308 (a)(5)(ii)(B)	A.10.4.1	NIST SP800-53 R3 SA-7 NIST SP800-53 R3 SC-5 NIST SP800-53 R3 SI-3 NIST SP800-53 R3 SI-5 NIST SP800-53 R3 SI-7 NIST SP800-53 R3 SI-8	NIST SP800-53 R3 SA-7 NIST SP800-53 R3 SC-5 NIST SP800-53 R3 SI-3 NIST SP800-53 R3 SI-3 (1) NIST SP800-53 R3 SI-3 (2) NIST SP800-53 R3 SI-3 (3) NIST SP800-53 R3 SI-5 NIST SP800-53 R3 SI-7 NIST SP800-53 R3 SI-7 (1) NIST SP800-53 R3 SI-8	PCI-DSS v2.0 5.1 PCI-DSS v2.0 5.1.1 PCI-DSS v2.0 5.2	SIG v6.0: G.7	GAPP Ref 8.2.2
Information Security - Incident Management	IS-22	Policy, process and procedures shall be established to triage security related events and ensure timely and thorough incident management.	No Change	X	X	X	X	X	COBIT 4.1 DS5.6	45 CFR 164.308 (a)(1)(ii) 45 CFR 164.308 (a)(6)(ii)	Clause 4.3.3 A.13.1.1 A.13.2.1	NIST SP800-53 R3 IR-1 NIST SP800-53 R3 IR-2 NIST SP800-53 R3 IR-3 NIST SP800-53 R3 IR-4 NIST SP800-53 R3 IR-5 NIST SP800-53 R3 IR-7 NIST SP800-53 R3 IR-8	NIST SP800-53 R3 IR-1 NIST SP800-53 R3 IR-2 NIST SP800-53 R3 IR-3 NIST SP800-53 R3 IR-4 NIST SP800-53 R3 IR-4 (1) NIST SP800-53 R3 IR-5 NIST SP800-53 R3 IR-7 NIST SP800-53 R3 IR-7 (1) NIST SP800-53 R3 IR-7 (2) NIST SP800-53 R3 IR-8	PCI-DSS v2.0 12.9 PCI-DSS v2.0 12.9.1 PCI-DSS v2.0 12.9.2 PCI-DSS v2.0 12.9.3 PCI-DSS v2.0 12.9.4 PCI-DSS v2.0 12.9.5 PCI-DSS v2.0 12.9.6	AUP v5.0 J.1 SIG v6.0: J.1.1, J.1.2	GAPP Ref 1.2.4 GAPP Ref 1.2.7 GAPP Ref 7.1.2 GAPP Ref 7.2.2 GAPP Ref 7.2.4 GAPP Ref 10.2.1 GAPP Ref 10.2.4
Information Security - Incident Reporting	IS-23	Contractors, employees and third party users shall be made aware of their responsibility to report all information security events in a timely manner. Information security events shall be reported through predefined communications channels in a prompt and expedient manner in compliance with statutory, regulatory and contractual requirements.	No Change	X	X	X	X	X	COBIT 4.1 DS5.6	45 CFR 164.312 (a)(6)(ii) 16 CFR 318.3 (a) (New) 16 CFR 318.5 (a) (New) 45 CFR 160.410 (a)(1) (New)	Clause 4.3.3 Clause 5.2.2 A.6.1.3 A.8.2.1 A.8.2.2 A.13.1.1 A.13.1.2 A.13.2.1	NIST SP800-53 R3 IR-2 NIST SP800-53 R3 IR-6 NIST SP800-53 R3 IR-7 NIST SP800-53 R3 SI-4 NIST SP800-53 R3 SI-5	NIST SP800-53 R3 IR-2 NIST SP800-53 R3 IR-6 NIST SP800-53 R3 IR-6 (1) NIST SP800-53 R3 IR-7 NIST SP800-53 R3 IR-7 (1) NIST SP800-53 R3 IR-7 (2) NIST SP800-53 R3 SI-4 NIST SP800-53 R3 SI-4 (2) NIST SP800-53 R3 SI-4 (4) NIST SP800-53 R3 SI-4 (5) NIST SP800-53 R3 SI-4 (6) NIST SP800-53 R3 SI-5	PCI-DSS v2.0 12.5.2 PCI-DSS v2.0 12.5.3	AUP v5.0 J.1 AUP v5.0 E.1 SIG v6.0: J.1.1, E.4	GAPP Ref 1.2.7 GAPP Ref 1.2.10 GAPP Ref 7.1.2 GAPP Ref 7.2.2 GAPP Ref 7.2.4 GAPP Ref 10.2.4
Information Security - Incident Response Legal Preparation	IS-24	In the event a follow-up action concerning a person or organization after an information security incident requires legal action proper forensic procedures including chain of custody shall be required for collection, retention, and presentation of evidence to support potential legal action subject to the relevant jurisdiction.	No Change	X	X	X	X	X	COBIT 4.1 DS5.6	45 CFR 164.308 (a)(6)(ii)	Clause 4.3.3 Clause 5.2.2 A.8.2.2 A.8.2.3 A.13.2.3 A.15.1.3	NIST SP800-53 R3 AU-6 NIST SP800-53 R3 AU-7 NIST SP800-53 R3 AU-9 NIST SP800-53 R3 AU-11 NIST SP800-53 R3 IR-5 NIST SP800-53 R3 IR-7 NIST SP800-53 R3 IR-8	NIST SP800-53 R3 AU-6 NIST SP800-53 R3 AU-6 (1) NIST SP800-53 R3 AU-6 (3) NIST SP800-53 R3 AU-7 NIST SP800-53 R3 AU-7 (1) NIST SP800-53 R3 AU-9 NIST SP800-53 R3 AU-9 (2) NIST SP800-53 R3 AU-11 NIST SP800-53 R3 IR-5 NIST SP800-53 R3 IR-7 NIST SP800-53 R3 IR-7 (1) NIST SP800-53 R3 IR-7 (2) NIST SP800-53 R3 IR-8		AUP v5.0 J.1 AUP v5.0 E.1 SIG v6.0: J.1.1, J.1.2, E.4	GAPP Ref 1.2.7
Information Security - Incident Response Metrics	IS-25	Mechanisms shall be put in place to monitor and quantify the types, volumes, and costs of information security incidents.	No Change	X	X	X	X	X	COBIT 4.1 DS 4.9	45 CFR 164.308 (a)(1)(ii)(D)	A.13.2.2	NIST SP800-53 R3 IR-4 NIST SP800-53 R3 IR-5 NIST SP800-53 R3 IR-8	NIST SP800-53 R3 IR-4 NIST SP800-53 R3 IR-4 (1) NIST SP800-53 R3 IR-5 NIST SP800-53 R3 IR-8	PCI DSS v2.0 12.9.5	SIG v6.0: J.1.2,	GAPP Ref 1.2.7 GAPP Ref 1.2.10

Copyright © 2010, Cloud Security Alliance

Control Area	Control ID	Control Specification	Control Specification (+1)	Cloud Service Delivery Model Applicability: SaaS	PaaS	IaaS	Supply Relationship: Service Provider	Tenant	Compliance Regime: COBIT 4.1	HIPAA / HITECH Act	ISO/IEC 27001:2005	NIST SP800-53	FedRAMP	PCI DSS v2.0	BITS Shared Assessments AUP v5.0 / SIG v6.0	GAPP (Aug 2009)
Information Security - Acceptable Use	IS-26	Policies and procedures shall be established for the acceptable use of information assets.	Policies and procedures shall be established for the acceptable use of information assets. The policies shall address acceptable data mining functionality and Traffic pattern analysis. And shall inform the tenant who is getting access to the data service output.	X	X	X	X	X	COBIT 4.1 DS 5.3	45 CFR 164.312 (b)	A.7.1.3	NIST SP800-53 R3 AC-8 NIST SP800-53 R3 AC-20 NIST SP800-53 R3 PL-4	NIST SP800-53 R3 AC-8 NIST SP800-53 R3 AC-20 NIST SP800-53 R3 AC-20 (1) NIST SP800-53 R3 AC-20 (2) NIST SP800-53 R3 PL-4	PCI-DSS v2.0 12.3.8	AUP v5.0 D.3 SIG v6.0: D 5.7, D.1.3.3, E.3.2, E.3.5.1, E.3.5.2	GAPP Ref 8.1.0
Information Security - Asset Returns	IS-27	Employees, contractors and third party users must return all assets owned by the organization within a defined and documented time frame once the employment, contract or agreement has been terminated.	Controls shall be put in place to insure privacy and automate tenant breach formal notification upon the compromise of a tenant's system(s).	X	X	X	X	X		45 CFR 164.308 (a)(3)(ii)(C)	A.7.1.1 A.7.1.2 A.8.3.2	NIST SP800-53 R3 PS-4	NIST SP800-53 R3 PS-4		AUP v5.0 D.1 SIG v6.0: E.6.4	GAPP Ref 5.2.3 GAPP Ref 7.2.2 GAPP Ref 8.2.1 GAPP Ref 8.2.6
Information Security - eCommerce Transactions	IS-28	Electronic commerce (e-commerce) related data traversing public networks shall be appropriately classified and protected from fraudulent activity, unauthorized disclosure or modification in such a manner to prevent contract dispute and compromise of data.	No Change	X	X	X	X	X	COBIT 4.1 DS 5.10 5.11	45 CFR 164.312(e)(1) 45 CFR 164.312(e)(2)(i)	A.7.2.1 A.10.6.1 A.10.6.2 A.10.9.1 A.10.9.2 A.15.1.4	NIST SP800-53 R3 AC-14 NIST SP800-53 R3 AC-21 NIST SP800-53 R3 AC-22 NIST SP800-53 R3 IA-8 NIST SP800-53 R3 AU-10 NIST SP800-53 R3 SC-4 NIST SP800-53 R3 SC-8 NIST SP800-53 R3 SC-9	NIST SP800-53 R3 AC-14 NIST SP800-53 R3 AC-14 (1) NIST SP800-53 R3 AC-21 NIST SP800-53 R3 AC-22 NIST SP800-53 R3 IA-8 NIST SP800-53 R3 AU-10 NIST SP800-53 R3 AU-10 (5) NIST SP800-53 R3 SC-4 NIST SP800-53 R3 SC-8 NIST SP800-53 R3 SC-8 (1) NIST SP800-53 R3 SC-9 NIST SP800-53 R3 SC-9 (1)	PCI-DSS v2.0 2.1.1 PCI-DSS v2.0 4.1 PCI-DSS v2.0 4.1.1 PCI DSS v2.0 4.2	AUP v5.0 G.4 AUP v5.0 G.11 AUP v5.0G.16 AUP v5.0 G.18 AUP v5.0 I.3 AUP v5.0 I.4 SIG v6.0:G.18.1.1, G.18.1.2, G.18.1.3, G.10.8, G.9.11, G.14, G.15.1	GAPP Ref 3.2.4 GAPP Ref 4.2.3 GAPP Ref 7.1.2 GAPP Ref 7.2.1 GAPP Ref 7.2.2 GAPP Ref 8.2.1 GAPP Ref 8.2.6
Information Security - Audit Tools Access	IS-29	Access to, and use of, audit tools that interact with the organizations information systems shall be appropriately segmented and restricted to prevent compromise and misuse of log data.	No Change	X	X	X	X		COBIT 4.1 DS 5.7		A.15.3.2	NIST SP800-53 R3 AU-9 NIST SP800-53 R3 AU-11 NIST SP800-53 R3 AU-14	NIST SP800-53 R3 AU-9 NIST SP800-53 R3 AU-9 (2) NIST SP800-53 R3 AU-11 NIST SP800-53 R3 AU-14	PCI DSS v2.0 10.5.5		GAPP Ref 8.2.1
Information Security - Diagnostic / Configuration Ports Access	IS-30	User access to diagnostic and configuration ports shall be restricted to authorized individuals and applications.	No Change	X	X	X	X	X	COBIT 4.1 DS5.7		A.10.6.1 A.11.1.1 A.11.4.4 A.11.5.4	NIST SP800-53 R3 CM-7 NIST SP800-53 R3 MA-3 NIST SP800-53 R3 MA-4 NIST SP800-53 R3 MA-5	NIST SP800-53 R3 CM-7 NIST SP800-53 R3 CM-7 (1) NIST SP800-53 R3 MA-3 NIST SP800-53 R3 MA-3 (1) NIST SP800-53 R3 MA-3 (2) NIST SP800-53 R3 MA-3 (3) NIST SP800-53 R3 MA-4 NIST SP800-53 R3 MA-4 (1) NIST SP800-53 R3 MA-4 (2) NIST SP800-53 R3 MA-5	PCI-DSS v2.0 9.1.2	SIG v6.0: H1.1, H1.2, G.9.15	N/A
Information Security - Network / Infrastructure Services	IS-31	Network and infrastructure service level agreements (in-house or outsourced) shall clearly document security controls, capacity and service levels, and business or customer requirements.	No Change	X	X	X	X	X	COBIT 4.1 DS5.10		A.6.2.3 A.10.6.2	NIST SP800-53 R3 SC-20 NIST SP800-53 R3 SC-21 NIST SP800-53 R3 SC-22 NIST SP800-53 R3 SC-23 NIST SP800-53 R3 SC-24	NIST SP800-53 R3 SC-20 NIST SP800-53 R3 SC-20 (1) NIST SP800-53 R3 SC-21 NIST SP800-53 R3 SC-22 NIST SP800-53 R3 SC-23		AUP v5.0 C.2 SIG v6.0:C.2.6, G.9.9	GAPP Ref 8.2.2 GAPP Ref 8.2.5
Information Security - Portable / Mobile Devices	IS-32	Policies and procedures shall be established and measures implemented to strictly limit access to sensitive data from portable and mobile devices, such as laptops, cell phones, and personal digital assistants (PDAs), which are generally higher-risk than non-portable devices (e.g., desktop computers at the organization's facilities).	No Change	X	X	X	X	X	COBIT 4.1 DS5.11 COBIT 4.1 DS5.5	45 CFR 164.310 (d)(1)	A.7.2.1 A.10.7.1 A.10.7.2 A.10.8.3 A.11.7.1 A.11.7.2 A.15.1.4	NIST SP800-53 R3 AC-17 NIST SP800-53 R3 AC-18 NIST SP800-53 R3 AC-19 NIST SP800-53 R3 MP-2 NIST SP800-53 R3 MP-4 NIST SP800-53 R3 MP-6	NIST SP800-53 R3 AC-17 NIST SP800-53 R3 AC-17 (1) NIST SP800-53 R3 AC-17 (2) NIST SP800-53 R3 AC-17 (3) NIST SP800-53 R3 AC-17 (4) NIST SP800-53 R3 AC-17 (5) NIST SP800-53 R3 AC-17 (7) NIST SP800-53 R3 AC-17 (8) NIST SP800-53 R3 AC-18 NIST SP800-53 R3 AC-18 (1) NIST SP800-53 R3 AC-18 (2) NIST SP800-53 R3 AC-18 (3) NIST SP800-53 R3 AC-18 (4) NIST SP800-53 R3 AC-18 (5) NIST SP800-53 R3 AC-19 NIST SP800-53 R3 AC-19 (1) NIST SP800-53 R3 AC-19 (2) NIST SP800-53 R3 AC-19 (3) NIST SP800-53 R3 MP-2 NIST SP800-53 R3 MP-2 (1) NIST SP800-53 R3 MP-4 NIST SP800-53 R3 MP-4 (1) NIST SP800-53 R3 MP-6 NIST SP800-53 R3 MP-6 (4)	PCI DSS v2.0 9.7 PCI DSS v2.0 9.7.2 PCI DSS v2.0 9.8 PCI DSS v2.0 9.9 PCI DSS v2.0 11.1 PCI DSS v2.0 12.3	SIG v6.0:G.11, G12, G.20.13, G.20.14	GAPP Ref 1.2.6 GAPP Ref 3.2.4 GAPP Ref 8.2.6
Information Security - Source Code Access Restriction	IS-33	Access to application, program or object source code shall be restricted to authorized personnel on a need to know basis. Records shall be maintained regarding the individual granted access, reason for access and version of source code exposed.	Access to application, program or object source code shall be restricted to authorized personnel based on cloud delivery model (PaaS) on a need to know basis.	X	X	X	X				Clause 4.3.3 A.12.4.3 A.15.1.3	NIST SP800-53 R3 CM-5 NIST SP800-53 R3 CM-6	NIST SP800-53 R3 CM-5 NIST SP800-53 R3 CM-5 (1) NIST SP800-53 R3 CM-5 (5) NIST SP800-53 R3 CM-6 NIST SP800-53 R3 CM-6 (1) NIST SP800-53 R3 CM-6 (3)	PCI-DSS v2.0 6.4.1 PCI-DSS v2.0 6.4.2	SIG v6.0 : I.2.7.2, I.2.9, I.2.10, I.2.15,	GAPP Ref 1.2.6 GAPP Ref 8.2.1
Information Security - Utility Programs Access	IS-34	Utility programs capable of potentially overriding system, object, network, virtual machine and application controls shall be restricted.	Utility programs and privileged management accounts capable of potentially overriding system, object, network, virtual machine and application controls shall be restricted. Utilities that utilities that can shut down virtualized partitions shall be disallowed. Attacks that target the virtual infrastructure (Shimming, Blue Pill, Hyperjacking, etc.) shall be identified and remediated with technical and procedural controls.	X	X	X	X	X	COBIT 4.1 DS5.7		A.11.4.1 A.11.4.4 A.11.5.4	NIST SP800-53 R3 AC-5 NIST SP800-53 R3 AC-6 NIST SP800-53 R3 CM-7 NIST SP800-53 R3 SC-3 NIST SP800-53 R3 SC-19	NIST SP800-53 R3 AC-5 NIST SP800-53 R3 AC-6 NIST SP800-53 R3 AC-6 (1) NIST SP800-53 R3 AC-6 (2) NIST SP800-53 R3 CM-7 NIST SP800-53 R3 CM-7 (1) NIST SP800-53 R3 SC-3 NIST SP800-53 R3 SC-19	PCI DSS v2.0 7.1.2	SIG v6.0:I.2.16	N/A
Legal - Non-Disclosure Agreements	LG-01	Requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details shall be identified, documented and reviewed at planned intervals.	No Change	X	X	X	X	X			ISO/IEC 27001:2005 Annex A.6.1.5	NIST SP800-53 R3 PL-4 NIST SP800-53 R3 PS-6 NIST SP800-53 R3 SA-9	NIST SP800-53 R3 PL-4 NIST SP800-53 R3 PS-6 NIST SP800-53 R3 SA-9 NIST SP800-53 R3 SA-9 (1)	PCI DSS v2.0 12.8.2 PCI DSS v2.0 12.8.3 PCI DSS v2.0 12.8.4	SIG v6.0:C.2.5	GAPP Ref 1.2.5

Copyright © 2010, Cloud Security Alliance

Control Area	Control ID	Control Specification	Control Revisions v1.1	Cloud Service Delivery Model Applicability			Scope Applicability		Compliance Mapping							
				SaaS	PaaS	IaaS	Service Provider	Tenant	COBIT 4.1	HIPAA / HITECH Act	ISO/IEC 27001-2005	NIST SP800-53	FedRAMP	PCI DSS v2.0	PCI Data Security Standard AUP v5.0 / PCI DSS v2.0	GAPP (Aug 2009)
Legal - Third Party Agreements	LG-03	Third party agreements that directly, or indirectly, impact the organization's information assets or data are required to include explicit coverage of all relevant security requirements. This includes agreements involving processing, accessing, communicating, hosting or managing the organization's information assets, or adding or terminating services or products to existing information. Assess agreement's provisions shall include security (e.g., encryption, access controls, and leakage prevention) and integrity controls for data exchanged to prevent improper disclosure, alteration or destruction.	No Change	X	X	X	X	X	COBIT 4.1 DS5.11	45 CFR 164.308 (a)(4)(i)(B) 45 CFR 164.308 (b)(1) 45 CFR 164.308 (b)(2)(i) 45 CFR 164.308 (b)(2)(ii) 45 CFR 164.308 (b)(2)(iii) 45 CFR 164.308 (b)(3) 45 CFR 164.308 (b)(4) 45 CFR 164.312(e)(2)(i) (New) 45 CFR 164.312 (b)(1) (New) 45 CFR 164.312(b)(2)(i) (New) 45 CFR 164.314 (a)(1)(i) 45 CFR 164.314 (a)(1)(ii)(A) 45 CFR 164.314 (a)(2)(i) 45 CFR 164.314 (a)(2)(i)(A) 45 CFR 164.314 (a)(2)(i)(B) 45 CFR 164.314 (a)(2)(i)(C) 45 CFR 164.314 (a)(2)(i)(D) 45 CFR 164.314 (a)(2)(ii)(A) 45 CFR 164.314 (a)(2)(ii)(A)(1) 45 CFR 164.314 (a)(2)(ii)(A)(2) 45 CFR 164.314 (a)(2)(ii)(B) 45 CFR 164.314 (a)(2)(ii)(C) 45 CFR 164.314 (a)(2)(iii) 45 CFR 164.314 (b)(2) 45 CFR 164.314 (b)(2)(i) 45 CFR 164.314 (b)(2)(ii) 45 CFR 164.314 (b)(2)(iii) 45 CFR 164.314 (b)(2)(iv)	A.6.2.3 A.10.2.1 A.11.6.2 A.11.4.6 A.11.6.1 A.12.3.1 A.12.5.4	NIST SP800-53 R3 CA-3 NIST SP800-53 R3 MP-5 NIST SP800-53 R3 PS-7 NIST SP800-53 R3 SA-9 NIST SP800-53 R3 SA-12 NIST SP800-53 R3 SA-6	NIST SP800-53 R3 CA-3 NIST SP800-53 R3 MP-5 NIST SP800-53 R3 MP-5 (2) NIST SP800-53 R3 MP-5 (4) NIST SP800-53 R3 PS-7 NIST SP800-53 R3 SA-6 NIST SP800-53 R3 SA-7 NIST SP800-53 R3 SA-9 NIST SP800-53 R3 SA-9 (1)	PCI DSS v2.0 12.8 PCI DSS v2.0 12.8.2	AUP v5.0 C.2 SIG v6.0: C.2.4, C.2.6, G.4.7, G.10.9	GAPP Ref 1.2.9
Operations Management - Policy	OP-01	Policies and procedures shall be established and made available for all personnel to adequately support services operations role.	No Change	X	X	X	X		COBIT 4.1 DS13.1		Clause 5.1 A 8.1.1 A.8.2.1 A 9.2.2 A.10.1.1	NIST SP800-53 R3 CM-2 NIST SP800-53 R3 CM-3 NIST SP800-53 R3 CM-4 NIST SP800-53 R3 CM-5 NIST SP800-53 R3 CM-6 NIST SP800-53 R3 CM-9 NIST SP800-53 R3 MA-4 NIST SP800-53 R3 SA-3 NIST SP800-53 R3 SA-4 NIST SP800-53 R3 SA-5 NIST SP800-53 R3 SA-8 NIST SP800-53 R3 SA-10 NIST SP800-53 R3 SA-11 NIST SP800-53 R3 SA-12	NIST SP800-53 R3 CM-2 NIST SP800-53 R3 CM-2 (1) NIST SP800-53 R3 CM-2 (3) NIST SP800-53 R3 CM-2 (5) NIST SP800-53 R3 CM-3 NIST SP800-53 R3 CM-3 (2) NIST SP800-53 R3 CM-4 NIST SP800-53 R3 CM-5 NIST SP800-53 R3 CM-5 (1) NIST SP800-53 R3 CM-5 (5) NIST SP800-53 R3 CM-6 NIST SP800-53 R3 CM-6 (1) NIST SP800-53 R3 CM-6 (3) NIST SP800-53 R3 CM-9 NIST SP800-53 R3 MA-4 NIST SP800-53 R3 MA-4 (1) NIST SP800-53 R3 MA-4 (2) NIST SP800-53 R3 SA-3 NIST SP800-53 R3 SA-4 NIST SP800-53 R3 SA-4 (1) NIST SP800-53 R3 SA-4 (4) NIST SP800-53 R3 SA-4 (7) NIST SP800-53 R3 SA-5 NIST SP800-53 R3 SA-5 (1) NIST SP800-53 R3 SA-5 (3) NIST SP800-53 R3 SA-8 NIST SP800-53 R3 SA-10 NIST SP800-53 R3 SA-11 NIST SP800-53 R3 SA-11 (1) NIST SP800-53 R3 SA-12	PCI DSS v2.0 12.1 PCI DSS v2.0 12.2 PCI DSS v2.0 12.3 PCI DSS v2.0 12.4	SIG v6.0: G.1.1	GAPP Ref 8.2.1
Operations Management - Documentation	OP-02	Information system documentation (e.g., administrator and user guides, architecture diagrams, etc.) shall be made available to authorized personnel to ensure the following: • Configuring, installing, and operating the information system • Effectively using the system's security features	No Change	X	X	X	X		COBIT 4.1 DS 9, DS 13.1		Clause 4.3.3 A.10.7.4	NIST SP800-53 R3 CP-9 NIST SP800-53 R3 CP-10 NIST SP800-53 R3 SA-5 NIST SP800-53 R3 SA-10 NIST SP800-53 R3 SA-11	NIST SP800-53 R3 CP-9 NIST SP800-53 R3 CP-9 (1) NIST SP800-53 R3 CP-9 (3) NIST SP800-53 R3 CP-10 NIST SP800-53 R3 CP-10 (2) NIST SP800-53 R3 CP-10 (3) NIST SP800-53 R3 SA-5 NIST SP800-53 R3 SA-5 (1) NIST SP800-53 R3 SA-5 (3) NIST SP800-53 R3 SA-10 NIST SP800-53 R3 SA-11 NIST SP800-53 R3 SA-11 (1)	PCI DSS v2.0 12.1 PCI DSS v2.0 12.2 PCI DSS v2.0 12.3 PCI DSS v2.0 12.4	SIG v6.0: G.1.1	GAPP Ref 1.2.6
Operations Management - Capacity / Resource Planning	OP-03	The availability, quality, and adequate capacity and resources shall be planned, prepared, and measured to deliver the required system performance in accordance with regulatory, contractual and business requirements. Projections of future capacity requirements shall be made to mitigate the risk of system overload.	No Change	X	X	X	X	X	COBIT 4.1 DS 3		A.10.3.1	NIST SP800-53 R3 SA-4	NIST SP800-53 R3 SA-4 NIST SP800-53 R3 SA-4 (1) NIST SP800-53 R3 SA-4 (4) NIST SP800-53 R3 SA-4 (7)		SIG v6.0:G.5	GAPP Ref 1.2.4
Operations Management - Equipment Maintenance	OP-04	Policies and procedures shall be established for equipment maintenance ensuring continuity and availability of operations.	No Change	X	X	X	X		COBIT 4.1 AI3.3	45 CFR 164.310 (a)(2)(iv)	A.9.2.4	NIST SP800-53 R3 MA-2 NIST SP800-53 R3 MA-3 NIST SP800-53 R3 MA-4 NIST SP800-53 R3 MA-5 NIST SP800-53 R3 MA-6	NIST SP800-53 R3 MA-2 NIST SP800-53 R3 MA-2 (1) NIST SP800-53 R3 MA-3 NIST SP800-53 R3 MA-3 (1) NIST SP800-53 R3 MA-3 (2) NIST SP800-53 R3 MA-3 (3) NIST SP800-53 R3 MA-4 NIST SP800-53 R3 MA-4 (1) NIST SP800-53 R3 MA-4 (2) NIST SP800-53 R3 MA-5 NIST SP800-53 R3 MA-6		SIG v6.0:F.2.19	GAPP Ref 5.2.3 GAPP Ref 8.2.2 GAPP Ref 8.2.3 GAPP Ref 8.2.4 GAPP Ref 8.2.5 GAPP Ref 8.2.6 GAPP Ref 8.2.7
Risk Management - Program	RI-01	Organizations shall develop and maintain an enterprise risk management framework to manage risk to an acceptable level.	Organizations shall develop and maintain a cloud oriented risk management framework to manage risk as defined in the master agreement or industry best-practices and standards.	X	X	X	X	X	COBIT 4.1 PO 9.1	45 CFR 164.308 (a)(8) 45 CFR 164.308(a)(1)(ii)(B) (New)	Clause 4.2.1 c) through g) Clause 4.2.2 b) Clause 5.1 f) Clause 7.2 & 7.3 A.6.2.1 A.12.6.1 A.14.1.2 A.15.2.1 A.15.2.2	NIST SP800-53 R3 AC-4 NIST SP800-53 R3 CA-2 NIST SP800-53 R3 CA-6 NIST SP800-53 R3 PM-9 NIST SP800-53 R3 RA-1	NIST SP800-53 R3 AC-4 NIST SP800-53 R3 CA-2 NIST SP800-53 R3 CA-2 (1) NIST SP800-53 R3 CA-6 NIST SP800-53 R3 PM-9 NIST SP800-53 R3 RA-1	PCI DSS v2.0 12.1.2	AUP v5.0 L.2 SIG v6.0: A.1, L.1	GAPP Ref 1.2.4

Copyright © 2010, Cloud Security Alliance

Control Area	Control ID	Control Specification	Control Revisions v1.1	Cloud Service Delivery Model Applicability			Scope Applicability		Compliance Mapping							
				SaaS	PaaS	IaaS	Service Provider	Tenant	COBIT 4.1	HIPAA / HITECH Act	ISO/IEC 27001-2005	NIST SP800-53	FedRAMP	PCI DSS v2.0	BITS Shared Assessments AUP v5.0 / SIG v6.0	GAPP (Aug 2009)
Risk Management - Assessments	RI-02	Aligned with the enterprise-wide framework, formal risk assessments shall be performed at least annually, or at planned intervals, determining the likelihood and impact of all identified risks, using qualitative and quantitative methods. The likelihood and impact associated with inherent and residual risk shall be determined independently, considering all risk categories (e.g., audit results, threat and vulnerability analysis, and regulatory compliance).	No Change	X	X	X	X	X	COBIT 4.1 PO 9.4	45 CFR 164.308 (a)(1)(ii)(A)	Clause 4.2.1 c) through g) Clause 4.2.3 d) Clause 5.1 f) Clause 7.2 & 7.3 A.6.2.1 A.12.5.2 A.12.6.1 A.14.1.2 A.15.1.1 A.15.2.1 A.15.2.2	NIST SP800-53 R3 PL-5 NIST SP800-53 R3 RA-2 NIST SP800-53 R3 RA-3	NIST SP800-53 R3 PL-5 NIST SP800-53 R3 RA-2 NIST SP800-53 R3 RA-3	PCI DSS v2.0 12.1.2	AUP v5.0 L1 AUP v5.0 L4 SIG v6.0: C.2.1, I.4.1, I.5, I.15, I.18, I.13	GAPP Ref 1.2.4 GAPP Ref 1.2.5
Risk Management - Mitigation / Acceptance	RI-03	Risks shall be mitigated to an acceptable level. Acceptance levels based on risk criteria shall be established and documented in accordance with reasonable resolution time frames and executive approval.	No Change	X	X	X	X	X	COBIT 4.1 PO 9.5	45 CFR 164.308 (a)(1)(ii)(B)	Clause 4.2.1 c) through g) Clause 4.2.2 b) Clause 4.3.1 Clause 5.1 f) Clause 7.3 A.6.2.1 A.12.5.2 A.12.6.1 A.15.1.1 A.15.2.1 A.15.2.2	NIST SP800-53 R3 CA-5 NIST SP800-53 R3 CM-4	NIST SP800-53 R3 CA-5 NIST SP800-53 R3 CM-4		AUP v5.0L4 AUP v5.0 L.2 SIG v6.0: I.3, L.9, L.10	N/A
Risk Management - Business / Policy Change Impacts	RI-04	Risk assessment results shall include updates to security policies, procedures, standards and controls to ensure they remain relevant and effective.	No Change	X	X	X	X	XX	COBIT 4.1 PO 9.6		Clause 4.2.3 Clause 4.2.4 Clause 4.3.1 Clause 5 Clause 7 A.5.1.2 A.10.1.2 A.10.2.3 A.14.1.2 A.15.2.1 A.15.2.2	NIST SP800-53 R3 CP-2 NIST SP800-53 R3 RA-2 NIST SP800-53 R3 RA-3	NIST SP800-53 R3 CP-2 NIST SP800-53 R3 CP-2 (1) NIST SP800-53 R3 CP-2 (2) NIST SP800-53 R3 RA-2 NIST SP800-53 R3 RA-3	PCI DSS v2.0 12.1.3	AUP v5.0 B.2 AUP v5.0 G.21 AUP v5.0 L.2 SIG v6.0: B.1.1, B.1.2, B.1.5, B.1.7.2, G.2, I.9, L.10	N/A
Risk Management - Third Party Access	RI-05	The identification, assessment, and prioritization of risks posed by business processes requiring third party access to the organization's information systems and data shall be followed by coordinated application of resources to minimize, monitor, and measure likelihood and impact of unauthorized or inappropriate access. Compensating controls derived from the risk analysis shall be implemented prior to provisioning access.	Service Providers shall implement and communicate disaster recovery, business continuity, capacity overflow and operational redundancy plans to all dependent service tiers. Service Providers shall perform failure impact analysis studies and communicate potential service impacts and reduced capacity projections to tenants. Tenants shall be afforded access to operational redundancy and continuity summaries which shall include dependent service tier oriented impact analysis. Security mechanisms and redundancies (at a minimum of N+2 at all times) shall be implemented to protect physical and virtual machines, networks, service providers and hardware from service outages (e.g., power failures, network disruptions, etc.). Tenants shall access to a tenant triggered failover control.	X	X	X	X	X	COBIT 4.1 DS 2.3		A.6.2.1 A.9.3.3 A.11.1.1 A.11.2.1 A.11.2.4	NIST SP800-53 R3 CA-3 NIST SP800-53 R3 MA-4 NIST SP800-53 R3 RA-3	NIST SP800-53 R3 CA-3 NIST SP800-53 R3 MA-4 NIST SP800-53 R3 MA-4 (1) NIST SP800-53 R3 MA-4 (2) NIST SP800-53 R3 RA-3	PCI DSS v2.0 12.8.1 PCI DSS v2.0 12.8.2 PCI DSS v2.0 12.8.3 PCI DSS v2.0 12.8.4	AUP v5.0 B.1 AUP v5.0 H.2 SIG v6.0: B.1.1, B.1.2, D.1.1, E.1, F.1.1, H.1.1, K.1.1, E.6.2, E.6.3	GAPP Ref 7.1.1 GAPP Ref 7.1.2 GAPP Ref 7.2.1 GAPP Ref 7.2.2 GAPP Ref 7.2.3 GAPP Ref 7.2.4
Release Management - New Development / Acquisition	RM-01	Policies and procedures shall be established for management authorization for development or acquisition of new applications, systems, databases, infrastructure, services, operations, and facilities.	No Change	X	X	X	X		COBIT 4.1 A12, A 16.1		A.6.1.4 A.6.2.1 A.12.1.1 A.12.4.1 A.12.4.2 A.12.4.3 A.12.5.5 A.15.1.3 A.15.1.4	NIST SP800-53 R3 CA-1 NIST SP800-53 R3 CM-1 NIST SP800-53 R3 CM-9 NIST SP800-53 R3 PL-1 NIST SP800-53 R3 PL-2 NIST SP800-53 R3 SA-1 NIST SP800-53 R3 SA-3 NIST SP800-53 R3 SA-4	NIST SP800-53 R3 CA-1 NIST SP800-53 R3 CM-1 NIST SP800-53 R3 CM-9 NIST SP800-53 R3 PL-1 NIST SP800-53 R3 PL-2 NIST SP800-53 R3 PL-2 (2) NIST SP800-53 R3 SA-1 NIST SP800-53 R3 SA-3 NIST SP800-53 R3 SA-4 NIST SP800-53 R3 SA-4 (1) NIST SP800-53 R3 SA-4 (4) NIST SP800-53 R3 SA-4 (7)	PCI DSS v2.0 6.3.2	AUP v5.0 L2 SIG v6.0: I.1.1, I.1.2, I.2, I.7.2, I.2.8, I.2.9, I.2.10, I.2.13, I.2.14, I.2.15, I.2.18, I.2.22.6, L.5,	GAPP Ref 1.2.6
Release Management - Production Changes	RM-02	Changes to the production environment shall be documented, tested and approved prior to implementation. Production software and hardware changes may include applications, systems, databases and network devices requiring patches, service packs, and other updates and modifications.	No Change	X	X	X	X	X	COBIT 4.1 A16.1, A17.5	45 CFR 164.308 (a)(5)(ii)(C) 45 CFR 164.312 (b)	A.10.1.4 A.12.5.1 A.12.5.2	NIST SP800-53 R3 CA-1 NIST SP800-53 R3 CA-6 NIST SP800-53 R3 CA-7 NIST SP800-53 R3 CM-2 NIST SP800-53 R3 CM-3 NIST SP800-53 R3 CM-5 NIST SP800-53 R3 CM-6 NIST SP800-53 R3 CM-9 NIST SP800-53 R3 PL-2 NIST SP800-53 R3 PL-5 NIST SP800-53 R3 SI-2 NIST SP800-53 R3 SI-6 NIST SP800-53 R3 SI-7	NIST SP800-53 R3 CA-1 NIST SP800-53 R3 CA-6 NIST SP800-53 R3 CA-7 NIST SP800-53 R3 CA-7 (2) NIST SP800-53 R3 CM-2 NIST SP800-53 R3 CM-2 (1) NIST SP800-53 R3 CM-2 (3) NIST SP800-53 R3 CM-2 (5) NIST SP800-53 R3 CM-3 NIST SP800-53 R3 CM-3 (2) NIST SP800-53 R3 CM-5 NIST SP800-53 R3 CM-5 (1) NIST SP800-53 R3 CM-5 (5) NIST SP800-53 R3 CM-6 NIST SP800-53 R3 CM-6 (1) NIST SP800-53 R3 CM-6 (3) NIST SP800-53 R3 CM-9 NIST SP800-53 R3 PL-2 NIST SP800-53 R3 PL-2 (2) NIST SP800-53 R3 PL-5 NIST SP800-53 R3 SI-2 NIST SP800-53 R3 SI-2 (2) NIST SP800-53 R3 SI-6 NIST SP800-53 R3 SI-7 NIST SP800-53 R3 SI-7 (1)	PCI DSS v2.0 1.1.1 PCI DSS v2.0 6.3.2 PCI DSS v2.0 6.4 PCI DSS v2.0 6.1	SIG v6.0: I.2.17, I.2.20, I.2.22	GAPP Ref 1.2.6
Release Management - Quality Testing	RM-03	A program for the systematic monitoring and evaluation to ensure that standards of quality are being met shall be established for all software developed by the organization. Quality evaluation and acceptance criteria for information systems, upgrades, and new versions shall be established, documented and tests of the system(s) shall be carried out both during development and prior to acceptance to maintain security. Management shall have a clear oversight capacity in the quality testing process with the final product being certified as "fit for purpose" (the product should be suitable for the intended purpose) and "right first time" (mistakes should be eliminated) prior to release.	No Change	X	X	X	X		COBIT 4.1 PO 8.1		A.6.1.3 A.10.1.1 A.10.1.4 A.10.3.2 A.12.1.1 A.12.2.1 A.12.2.2 A.12.2.3 A.12.2.4 A.12.4.1 A.12.4.2 A.12.4.3 A.12.5.1 A.12.5.2 A.12.5.3 A.12.6.1 A.13.1.2 A.15.2.1 A.15.2.2	NIST SP800-53 R3 CM-1 NIST SP800-53 R3 CM-2 NIST SP800-53 R3 SA-3 NIST SP800-53 R3 SA-4 NIST SP800-53 R3 SA-5 NIST SP800-53 R3 SA-8 NIST SP800-53 R3 SA-10 NIST SP800-53 R3 SA-11 NIST SP800-53 R3 SA-13	NIST SP800-53 R3 CM-1 NIST SP800-53 R3 CM-2 NIST SP800-53 R3 CM-2 (1) NIST SP800-53 R3 CM-2 (3) NIST SP800-53 R3 CM-2 (5) NIST SP800-53 R3 SA-3 NIST SP800-53 R3 SA-4 NIST SP800-53 R3 SA-4 (1) NIST SP800-53 R3 SA-4 (4) NIST SP800-53 R3 SA-4 (7) NIST SP800-53 R3 SA-5 NIST SP800-53 R3 SA-5 (1) NIST SP800-53 R3 SA-5 (3) NIST SP800-53 R3 SA-8 NIST SP800-53 R3 SA-10 NIST SP800-53 R3 SA-11 NIST SP800-53 R3 SA-11 (1) NIST SP800-53 R3 SA-13	PCI DSS v2.0 1.1.1 PCI DSS v2.0 6.1 PCI DSS v2.0 6.4	C.1.7, G.1, G.6, I.1, I.4.5, I.2.18, , I.22.1, I.22.3, I.22.5, I.2.23, I.2.22.2, I.2.22.4, I.2.22.7, I.2.22.8, I.2.22.9, I.2.22.10, I.2.22.11, I.2.22.12, I.2.22.13, I.2.22.14 I.2.20, I.2.17, I.2.7.1, I.3, J.2.10, L.9	GAPP Ref 9.1.0 GAPP Ref 9.1.1 GAPP Ref 9.2.1 GAPP Ref 9.2.2

Copyright © 2010, Cloud Security Alliance

Control Area	Control ID	Control Specification	Control Relevance v3.1	Cloud Service Delivery Model Applicability			Scope Applicability		Compliance Mapping							
				SaaS	PaaS	IaaS	Service Provider	Tenant	COBIT 4.1	HIPAA / HITECH Act	ISO/IEC 27001:2005	NIST SP800-53	FedRAMP	PCI DSS v2.0	SCIS Model Assessments AUP v6.0 / SIG v6.0	GAPP (Aug 2009)
Release Management - Outsourced Development	RM-04	A program for the systematic monitoring and evaluation to ensure that standards of quality are being met shall be established for all outsourced software development. The development of all outsourced software shall be supervised and monitored by the organization and must include security requirements, independent security review of the outsourced environment by a certified individual, certified security training for outsourced software developers, and code reviews. Certification for the purposes of this control shall be defined as either a ISO/IEC 17024 accredited certification or a locally recognized license or certification in the legislative jurisdiction the organization outsourcing the development has chosen as its domicile.	No Change	X	X	X	X	X			A.6.1.8 A.6.2.1 A.6.2.3 A.10.1.4 A.10.2.1 A.10.3.2 A.10.3.3 A.10.3.2 A.12.1.1 A.12.5.1 A.12.5.2 A.12.5.3 A.12.6.4 A.12.6.1 A.12.6.2 A.12.5.3 A.12.5.1 A.12.5.2 A.12.5.3 A.12.5.5 A.12.5.1 A.12.5.2 A.12.5.1 A.12.5.2	NIST SP800-53 R3 SA-4 NIST SP800-53 R3 SA-5 NIST SP800-53 R3 SA-8 NIST SP800-53 R3 SA-9 NIST SP800-53 R3 SA-10 NIST SP800-53 R3 SA-11 NIST SP800-53 R3 SA-12 NIST SP800-53 R3 SA-13	NIST SP800-53 R3 SA-4 NIST SP800-53 R3 SA-4 (1) NIST SP800-53 R3 SA-4 (4) NIST SP800-53 R3 SA-4 (7) NIST SP800-53 R3 SA-5 NIST SP800-53 R3 SA-5 (1) NIST SP800-53 R3 SA-5 (3) NIST SP800-53 R3 SA-8 NIST SP800-53 R3 SA-9 NIST SP800-53 R3 SA-9 (1) NIST SP800-53 R3 SA-10 NIST SP800-53 R3 SA-11 NIST SP800-53 R3 SA-11 (1) NIST SP800-53 R3 SA-12 NIST SP800-53 R3 SA-13	PCI DSS v2.0 2.5.7 PCI DSS v2.0 6.4.5.2 PCI DSS v2.0 7.1.3 PCI DSS v2.0 8.5.1 PCI DSS v2.0 9.1 PCI DSS v2.0 9.1.2 PCI DSS v2.0 9.2b PCI DSS v2.0 9.9.1 PCI DSS v2.0 10.5.2 PCI DSS v2.0 10.5 PCI DSS v2.0 10.3.1 PCI DSS v2.0 10.3.3	AUP v6.0 D.2 AUP v6.0 I.2 AUP v5.0 I.4 AUP v5.0 I.1 SIG v6.0: I.2.4, G.4, G.6, I.1, I.4.4, I.4.5, I.2.7.2, I.2.8, I.2.9, I.2.15, I.2.16, I.2.22.5, I.2.7.1, I.2.13, I.2.14, I.2.17, I.2.20, I.2.22.2, I.2.22.4, I.2.22.7, I.2.22.8, I.2.22.9, I.2.22.10, I.2.22.11, I.2.22.12, I.2.22.13, I.2.22.14, I.3, J.1.2.10, J.7, L.5, L.10	N/A
Release Management - Unauthorized Software Installations	RM-05	Policies and procedures shall be established and mechanisms implemented to restrict the installation of unauthorized software.	No Change	X	X	X	X				A.10.1.3 A.10.6.1 A.11.5.4 A.11.6.1 A.12.6.1 A.12.5.3	NIST SP800-53 R3 CM-1 NIST SP800-53 R3 CM-2 NIST SP800-53 R3 CM-3 NIST SP800-53 R3 CM-5 NIST SP800-53 R3 CM-7 NIST SP800-53 R3 CM-8 NIST SP800-53 R3 CM-9 NIST SP800-53 R3 SA-6 NIST SP800-53 R3 SA-7 NIST SP800-53 R3 SI-1 NIST SP800-53 R3 SI-3 NIST SP800-53 R3 SI-4 NIST SP800-53 R3 SI-7	NIST SP800-53 R3 CM-1 NIST SP800-53 R3 CM-2 NIST SP800-53 R3 CM-2 (1) NIST SP800-53 R3 CM-2 (3) NIST SP800-53 R3 CM-2 (5) NIST SP800-53 R3 CM-3 NIST SP800-53 R3 CM-3 (2) NIST SP800-53 R3 CM-5 NIST SP800-53 R3 CM-5 (1) NIST SP800-53 R3 CM-5 (5) NIST SP800-53 R3 CM-7 NIST SP800-53 R3 CM-7 (1) NIST SP800-53 R3 CM-8 NIST SP800-53 R3 CM-8 (1) NIST SP800-53 R3 CM-8 (3) NIST SP800-53 R3 CM-8 (5) NIST SP800-53 R3 CM-9 NIST SP800-53 R3 SA-6 NIST SP800-53 R3 SA-7 NIST SP800-53 R3 SI-1 NIST SP800-53 R3 SI-3 NIST SP800-53 R3 SI-3 (1) NIST SP800-53 R3 SI-3 (2) NIST SP800-53 R3 SI-3 (3) NIST SP800-53 R3 SI-4 NIST SP800-53 R3 SI-4 (2) NIST SP800-53 R3 SI-4 (4) NIST SP800-53 R3 SI-4 (5) NIST SP800-53 R3 SI-4 (6) NIST SP800-53 R3 SI-7 NIST SP800-53 R3 SI-7 (1)		AUP v6.0 G.1 AUP v5.0 I.2 SIG v6.0: G.2.13, G.20.2, G.20.4, G.20.5, G.7, G.7.1, G.12.11, H.2.16, I.2.22.1, I.2.22.3, I.2.22.6, I.2.23,	GAPP Ref 3.2.4 GAPP Ref 8.2.2
Resiliency - Management Program	RS-01	Policy, process and procedures defining business continuity and disaster recovery shall be put in place to minimize the impact of a realized risk event on the organization to an acceptable level and facilitate recovery of information assets (which may be the result of, for example, natural disasters, accidents, equipment failures, and deliberate actions) through a combination of preventive and recovery controls, in accordance with regulatory, statutory, contractual, and business requirements and consistent with industry standards. This Resiliency management program shall be communicated to all organizational participants with a need to know basis prior to adoption and shall also be published, hosted, stored, recorded and disseminated to multiple facilities which must be accessible in the event of an incident.	No Change	X	X	X	X	X	COBIT 4.1 PO 9.1 PO 9.2 DS 4.2	45 CFR 164.308 (a)(7)(i) (New) 45 CFR 164.308 (a)(7)(ii)(C)	Clause 4.3.2 A.14.1.1 A 14.1.4	NIST SP800-53 R3 CP-1 NIST SP800-53 R3 CP-2	NIST SP800-53 R3 CP-1 NIST SP800-53 R3 CP-2 NIST SP800-53 R3 CP-2 (1) NIST SP800-53 R3 CP-2 (2)	PCI DSS v2.0 12.9.1	SIG v6.0: K.1.2.9, K.1.2.10, K.3.1	N/A
Resiliency - Impact Analysis	RS-02	There shall be a defined and documented method for determining the impact of any disruption to the organization which must incorporate the following: • Identify critical products and services • Identify all dependencies, including processes, applications, business partners and third party service providers • Understand threats to critical products and services • Determine impacts resulting from planned or unplanned disruptions and how these vary over time • Establish the maximum tolerable period for disruption • Establish priorities for recovery • Establish recovery time objectives for resumption of critical products and services within their maximum tolerable period of disruption • Estimate the resources required for resumption	No Change	X	X	X	X	X		45 CFR 164.308 (a)(7)(ii)(E)	ISO/IEC 27001:2005 A.14.1.2 A 14.1.4	NIST SP800-53 R3 RA-3	NIST SP800-53 R3 RA-3		SIG v6.0:K.2	N/A

Copyright © 2010, Cloud Security Alliance

Control Area	Control ID	Control Specification	Control Revision v1.1	Cloud Service Delivery Model Applicability: SaaS	PaaS	IaaS	Supply Applicability: Service Provider	Tenant	Compliance Mapping: COBIT 4.1	HIPAA / HITECH Act	ISO/IEC 27001:2005	NIST SP800-53	FedRAMP	PCI DSS v2.0	BITS Shared Assessments AUP v5.0 / SIG v6.0	GAPP (Aug 2009)
Resiliency - Business Continuity Planning	RS-03	A consistent unified framework for business continuity planning and plan development shall be established, documented and adopted to ensure all business continuity plans are consistent in addressing priorities for testing and maintenance and information security requirements. Requirements for business continuity plans include the following: • Defined purpose and scope, aligned with relevant dependencies • Accessible to and understood by those who will use them • Owned by a named person(s) who is responsible for their review, update and approval • Defined lines of communication, roles and responsibilities • Detailed recovery procedures, manual work around and reference information • Method for plan invocation	No Change	X	X	X	X	X		45 CFR 164.308 (a)(7)(i) 45 CFR 164.308 (a)(7)(ii)(B) 45 CFR 164.308 (a)(7)(ii)(C) 45 CFR 164.308 (a)(7)(ii)(E) 45 CFR 164.312 (a)(2)(ii) 45 CFR 164.312 (c)(2)(ii)	Clause 5.1 A.5.1.2 A.14.1.3 A.14.1.4	NIST SP800-53 R3 CP-1 NIST SP800-53 R3 CP-2 NIST SP800-53 R3 CP-3 NIST SP800-53 R3 CP-4 NIST SP800-53 R3 CP-6 NIST SP800-53 R3 CP-7 NIST SP800-53 R3 CP-8 NIST SP800-53 R3 CP-9 NIST SP800-53 R3 CP-10 NIST SP800-53 R3 PE-17	NIST SP800-53 R3 CP-1 NIST SP800-53 R3 CP-2 NIST SP800-53 R3 CP-2 (1) NIST SP800-53 R3 CP-2 (2) NIST SP800-53 R3 CP-3 NIST SP800-53 R3 CP-4 NIST SP800-53 R3 CP-4 (1) NIST SP800-53 R3 CP-6 NIST SP800-53 R3 CP-6 (1) NIST SP800-53 R3 CP-6 (3) NIST SP800-53 R3 CP-7 NIST SP800-53 R3 CP-7 (1) NIST SP800-53 R3 CP-7 (2) NIST SP800-53 R3 CP-7 (3) NIST SP800-53 R3 CP-7 (5) NIST SP800-53 R3 CP-8 NIST SP800-53 R3 CP-8 (1) NIST SP800-53 R3 CP-8 (2) NIST SP800-53 R3 CP-9 NIST SP800-53 R3 CP-9 (1) NIST SP800-53 R3 CP-9 (3) NIST SP800-53 R3 CP-10 NIST SP800-53 R3 CP-10 (2) NIST SP800-53 R3 CP-10 (3) NIST SP800-53 R3 PE-17	PCI DSS v2.0 12.9.1 PCI DSS v2.0 12.9.3 PCI DSS v2.0 12.9.4 PCI DSS v2.0 12.9.6	SIG v6.0: K.1.2.3, K.1.2.4, K.1.2.5, K.1.2.6, K.1.2.7, K.1.2.11, K.1.2.13, K.1.2.15,	N/A
Resiliency - Business Continuity Testing	RS-04	Business continuity plans shall be subject to test at planned intervals or upon significant organizational or environmental changes to ensure continuing effectiveness.	No Change	X	X	X	X	X		45 CFR 164.308 (a)(7)(ii)(D)	A.14.1.5	NIST SP800-53 R3 CP-2 NIST SP800-53 R3 CP-3 NIST SP800-53 R3 CP-4	NIST SP800-53 R3 CP-2 NIST SP800-53 R3 CP-2 (1) NIST SP800-53 R3 CP-2 (2) NIST SP800-53 R3 CP-3 NIST SP800-53 R3 CP-4 NIST SP800-53 R3 CP-4 (1)	PCI DSS v2.0 12.9.2	SIG v6.0: K.1.3, K.1.4.3, K.1.4.6, K.1.4.7, K.1.4.8, K.1.4.9, K.1.4.10, K.1.4.11, K.1.4.12	N/A
Resiliency - Environmental Risks	RS-05	Physical protection against damage from natural causes and disasters as well as deliberate attacks including fire, flood, atmospheric electrical discharge, solar induced geomagnetic storm, wind, earthquake, tsunami, explosion, nuclear mishap, volcanic activity, biological hazard, civil unrest, mudslide, tectonic activity, and other forms of natural or man-made disaster shall be anticipated, designed and countermeasures applied.	No Change	X	X	X	X			45 CFR 164.308 (a)(7)(ii) 45 CFR 164.310(a)(2)(ii) (New)	A.9.1.4 A.9.2.1	NIST SP800-53 R3 PE-1 NIST SP800-53 R3 PE-13 NIST SP800-53 R3 PE-14 NIST SP800-53 R3 PE-15 NIST SP800-53 R3 PE-18	NIST SP800-53 R3 PE-1 NIST SP800-53 R3 PE-13 NIST SP800-53 R3 PE-13 (1) NIST SP800-53 R3 PE-13 (2) NIST SP800-53 R3 PE-13 (3) NIST SP800-53 R3 PE-14 NIST SP800-53 R3 PE-14 (1) NIST SP800-53 R3 PE-15 NIST SP800-53 R3 PE-18		AUP v5.0 F.1 SIG v6.0: F.2.9, F.1.2.21, F.5.1, F.1.5.2, F.2.1, F.2.7, F.2.8,	GAPP Ref 8.2.4
Resiliency - Equipment Location	RS-06	To reduce the risks from environmental threats, hazards and opportunities for unauthorized access equipment shall be located away from locations subject to high probability environmental risks and supplemented by redundant equipment located at a reasonable distance.	No Change	X	X	X	X			45 CFR 164.310 (a)	A.9.2.1	NIST SP800-53 R3 PE-1 NIST SP800-53 R3 PE-5 NIST SP800-53 R3 PE-14 NIST SP800-53 R3 PE-15 NIST SP800-53 R3 PE-18	NIST SP800-53 R3 PE-1 NIST SP800-53 R3 PE-5 NIST SP800-53 R3 PE-14 NIST SP800-53 R3 PE-14 (1) NIST SP800-53 R3 PE-15 NIST SP800-53 R3 PE-18	PCI DSS v2.0 9.1.3 PCI DSS v2.0 9.5 PCI DSS v2.0 9.6 PCI DSS v2.0 9.9 PCI DSS v2.0 9.9.1	AUP v5.0 F.1 SIG v6.0: F.2.9, F.1.2.21, F.5.1, F.1.5.2, F.2.1, F.2.7, F.2.8,	N/A
Resiliency - Equipment Power Failures	RS-07	Security mechanisms and redundancies shall be implemented to protect equipment from utility service outages (e.g., power failures, network disruptions, etc.).	No Change	X	X	X	X				A.9.2.2 A.9.2.3 A.9.2.4	NIST SP800-53 R3 CP-8 NIST SP800-53 R3 PE-1 NIST SP800-53 R3 PE-9 NIST SP800-53 R3 PE-10 NIST SP800-53 R3 PE-11 NIST SP800-53 R3 PE-12 NIST SP800-53 R3 PE-13 NIST SP800-53 R3 PE-14	NIST SP800-53 R3 CP-8 NIST SP800-53 R3 CP-8 (1) NIST SP800-53 R3 CP-8 (2) NIST SP800-53 R3 PE-1 NIST SP800-53 R3 PE-9 NIST SP800-53 R3 PE-10 NIST SP800-53 R3 PE-11 NIST SP800-53 R3 PE-11 (1) NIST SP800-53 R3 PE-12 NIST SP800-53 R3 PE-13 NIST SP800-53 R3 PE-13 (1) NIST SP800-53 R3 PE-13 (2) NIST SP800-53 R3 PE-13 (3) NIST SP800-53 R3 PE-14 NIST SP800-53 R3 PE-14 (1)		AUP v5.0 F.1 SIG v6.0: F.1.6, F.1.5.1, F.1.6.2, F.1.9.2, F.2.10, F.2.11, F.2.12,	N/A
Resiliency - Power / Telecommunications	RS-08	Telecommunications equipment, cabling and relays transceiving data or supporting services shall be protected from interception or damage and designed with redundancies, alternative power source and alternative routing.	Telecommunications equipment, cabling and relays transceiving data or supporting services shall be protected from interception unless legally required (wire tape, etc.). These systems shall be designed with redundancies, alternative power source and alternative routing. Tenants shall have informed consent over jurisdiction of transport	X	X	X	X				A.9.2.2 A.9.2.3	NIST SP800-53 R3 PE-1 NIST SP800-53 R3 PE-4 NIST SP800-53 R3 PE-13	NIST SP800-53 R3 PE-1 NIST SP800-53 R3 PE-4 NIST SP800-53 R3 PE-13 NIST SP800-53 R3 PE-13 (1) NIST SP800-53 R3 PE-13 (2) NIST SP800-53 R3 PE-13 (3)		AUP v5.0 F.1 SIG v6.0: F.1.6, F.1.5.1, F.1.6.2, F.1.9.2, F.2.10, F.2.11, F.2.12,	N/A
Security Architecture - Customer Access Requirements	SA-01	Prior to granting customers access to data, assets and information systems, all identified security, contractual and regulatory requirements for customer access shall be addressed and remediated.	No Change	X	X	X	X	X			A.6.2.1 A.6.2.2 A.11.1.1	NIST SP800-53 R3 CA-1 NIST SP800-53 R3 CA-2 NIST SP800-53 R3 CA-5 NIST SP800-53 R3 CA-6	NIST SP800-53 R3 CA-1 NIST SP800-53 R3 CA-2 NIST SP800-53 R3 CA-2 (1) NIST SP800-53 R3 CA-5 NIST SP800-53 R3 CA-6		SIG v6.0: C.2.1, C.2.3, C.2.4, C.2.5.1, H.1	GAPP Ref 1.2.2 GAPP Ref 1.2.6 GAPP Ref 6.2.1 GAPP Ref 6.2.2
Security Architecture - User ID Credentials	SA-02	Implement and enforce (through automation) user credential and password controls for applications, databases and server and network infrastructure, requiring the following minimum standards: • User identity verification prior to password resets. • If password reset initiated by personnel other than user (i.e., administrator), password must be immediately changed by user upon first use. • Timely access revocation for terminated users. • Remove/disable inactive user accounts at least every 90 days. • Unique user IDs and disallow group, shared, or generic accounts and passwords. • Password expiration at least every 90 days. • Minimum password length of at least seven (7) characters. • Strong passwords containing both numeric and alphabetic characters. • Allow password re-use after the last four (4) passwords used. • User ID lockout after not more than six (6) attempts. • User ID lockout duration to a minimum of 30 minutes or until administrator enables the user ID. • Re-enter password to reactivate terminal		X	X	X	X	X	COBIT 4.1 DS5.3 COBIT 4.1 DS5.4	45 CFR 164.308(a)(5)(ii)(c) (New) 45 CFR 164.308 (a)(5)(ii)(D) 45 CFR 164.312 (a)(2)(i) 45 CFR 164.312 (a)(2)(iii) 45 CFR 164.312 (d)	A.8.3.3 A.11.1.1 A.11.2.1 A.11.2.3 A.11.2.4 A.11.5.5	NIST SP800-53 R3 AC-1 NIST SP800-53 R3 AC-2 NIST SP800-53 R3 AC-3 NIST SP800-53 R3 AC-11 NIST SP800-53 R3 AU-2 NIST SP800-53 R3 AU-11 NIST SP800-53 R3 IA-1 NIST SP800-53 R3 IA-2 NIST SP800-53 R3 IA-5 NIST SP800-53 R3 IA-8 NIST SP800-53 R3 SC-10	NIST SP800-53 R3 AC-1 NIST SP800-53 R3 AC-2 NIST SP800-53 R3 AC-2 (1) NIST SP800-53 R3 AC-2 (2) NIST SP800-53 R3 AC-2 (3) NIST SP800-53 R3 AC-2 (4) NIST SP800-53 R3 AC-2 (7) NIST SP800-53 R3 AC-3 NIST SP800-53 R3 AC-3 (3) NIST SP800-53 R3 AC-11 NIST SP800-53 R3 AC-11 (1) NIST SP800-53 R3 AU-2 NIST SP800-53 R3 AU-2 (3) NIST SP800-53 R3 AU-2 (4) NIST SP800-53 R3 AU-11 NIST SP800-53 R3 IA-1 NIST SP800-53 R3 IA-2 NIST SP800-53 R3 IA-2 (1) NIST SP800-53 R3 IA-2 (2) NIST SP800-53 R3 IA-2 (3) NIST SP800-53 R3 IA-2 (8) NIST SP800-53 R3 IA-5 NIST SP800-53 R3 IA-5 (1) NIST SP800-53 R3 IA-5 (2) NIST SP800-53 R3 IA-5 (3) NIST SP800-53 R3 IA-5 (6) NIST SP800-53 R3 IA-5 (7) NIST SP800-53 R3 IA-8 NIST SP800-53 R3 IA-8 NIST SP800-53 R3 SC-10	PCI DSS v2.0 8.1 PCI DSS v2.0 8.2, PCI DSS v2.0 8.3 PCI DSS v2.0 8.4 PCI DSS v2.0 8.5 PCI DSS v2.0 10.1, PCI DSS v2.0 12.2, PCI DSS v2.0 12.3.8	AUP v5.0 B.1 AUP v5.0 H.5 SIG v6.0: E.5.2, E.5.3, H.1.1, H.1.2, H.2, H.3.2, H.4, H.4.1, H.4.5, H.4.8,	N/A

Copyright © 2010, Cloud Security Alliance

Control Area	Control ID	Control Specification	Control Provision (v1.1)	Cloud Service Delivery Model Applicability: SaaS	PaaS	IaaS	Scope Applicability: Service Provider	Tenant	Compliance Mapping: COBIT 4.1	HIPAA / HITECH Act	ISO/IEC 27001:2005	NIST SP800-53	FedRAMP	PCI DSS v2.0	BITS Shared Assessments AUP v5.0 / SIG v6.0	GAPP (Aug 2009)
Security Architecture - Data Security / Integrity	SA-03	Policies and procedures shall be established and mechanisms implemented to ensure security (e.g., encryption, access controls, and business rules enforcement) and integrity of data exchanged between one or more system interfaces, jurisdictions, or with a third party shared services provider to prevent improper disclosure, alteration or destruction complying with legislative, regulatory, and contractual requirements.	No Change	X	X	X	X		COBIT 4.1 DS5.11		A.10.8.1 A.10.8.2 A.11.1.1 A.11.6.1 A.11.4.5 A.12.3.1 A.12.5.1 A.15.1.4	NIST SP800-53 R3 AC-1 NIST SP800-53 R3 AC-4 NIST SP800-53 R3 DC-1 NIST SP800-53 R3 SC-16	NIST SP800-53 R3 AC-1 NIST SP800-53 R3 AC-4 NIST SP800-53 R3 DC-1 NIST SP800-53 R3 SC-16	PCI DSS v2.0 2.3 PCI DSS v2.0 3.1.1, PCI DSS v2.0 4.1 PCI DSS v2.0 4.1.1 PCI DSS v2.0 6.1 PCI DSS v2.0 6.3.2a PCI DSS v2.0 6.5b PCI DSS v2.0 8.3 PCI DSS v2.0 10.5.5 PCI DSS v2.0 11.5	AUP v5.0 8.1 SIG v6.0: G.8.2 G.2, G.8.3, G.12.1, G.12.4, G. 12.8, G.12.10, G.16.2, G.19.2.1, G.18.3.2, G.9.4, G.17.2, G.17.3, G.17.4, G.20.1,	GAPP Ref 1.1.0 GAPP Ref 1.2.2 GAPP Ref 1.2.6 GAPP Ref 4.2.3 GAPP Ref 5.2.1 GAPP Ref 7.1.2 GAPP Ref 7.2.1 GAPP Ref 7.2.2 GAPP Ref 7.2.3 GAPP Ref 7.2.4 GAPP Ref 8.2.1 GAPP Ref 8.2.2 GAPP Ref 8.2.3 GAPP Ref 8.2.5 GAPP Ref 8.2.6 GAPP Ref 1.2.6
Security Architecture - Application Security	SA-04	Applications shall be designed in accordance with industry accepted security standards (i.e., OWASP for web applications) and complies with applicable regulatory and business requirements.	No Change	X	X	X	X		COBIT 4.1 AI2.4	45 CFR 164.312(e)(2)(i)	A.11.5.6 A.11.6.1 A.12.2.1 A.12.2.2 A.12.2.3 A.12.2.4 A.12.5.2 A.12.5.4 A.12.5.5 A.12.6.1 A.15.2.1	NIST SP800-53 R3 SC-2 NIST SP800-53 R3 SC-3 NIST SP800-53 R3 SC-4 NIST SP800-53 R3 SC-5 NIST SP800-53 R3 SC-6 NIST SP800-53 R3 SC-7 NIST SP800-53 R3 SC-8 NIST SP800-53 R3 SC-9 NIST SP800-53 R3 SC-10 NIST SP800-53 R3 SC-11 NIST SP800-53 R3 SC-12 NIST SP800-53 R3 SC-13 NIST SP800-53 R3 SC-14 NIST SP800-53 R3 SC-17 NIST SP800-53 R3 SC-18	NIST SP800-53 R3 SC-2 NIST SP800-53 R3 SC-3 NIST SP800-53 R3 SC-4 NIST SP800-53 R3 SC-5 NIST SP800-53 R3 SC-6 NIST SP800-53 R3 SC-7 NIST SP800-53 R3 SC-7 (1) NIST SP800-53 R3 SC-7 (2) NIST SP800-53 R3 SC-7 (3) NIST SP800-53 R3 SC-7 (4) NIST SP800-53 R3 SC-7 (5) NIST SP800-53 R3 SC-7 (7) NIST SP800-53 R3 SC-7 (8) NIST SP800-53 R3 SC-7 (12) NIST SP800-53 R3 SC-7 (13)	PCI DSS v2.0 6.5	AUP v5.0 I.4 SIG v6.0: G.18.3, I.3	
Security Architecture - Data Integrity	SA-05	Data input and output integrity routines (i.e., reconciliation and edit checks) shall be implemented for application interfaces and databases to prevent manual or systematic processing errors or corruption of data.	No Change	X	X	X	X	X		45 CFR 164.312 (c)(1) (New) 45 CFR 164.312 (c)(2)(New) 45 CFR 164.312(e)(2)(i)(New)	A.10.9.2 A.10.9.3 A.12.2.1 A.12.2.2 A.12.2.3 A.12.2.4 A.12.5.1 A.15.2.1	NIST SP800-53 R3 SI-10 NIST SP800-53 R3 SI-11 NIST SP800-53 R3 SI-2 NIST SP800-53 R3 SI-3 NIST SP800-53 R3 SI-4 NIST SP800-53 R3 SI-6 NIST SP800-53 R3 SI-7 NIST SP800-53 R3 SI-9	NIST SP800-53 R3 SI-10 NIST SP800-53 R3 SI-11 NIST SP800-53 R3 SI-2 NIST SP800-53 R3 SI-2 (2) NIST SP800-53 R3 SI-3 NIST SP800-53 R3 SI-3 (1) NIST SP800-53 R3 SI-3 (2) NIST SP800-53 R3 SI-3 (3) NIST SP800-53 R3 SI-4 NIST SP800-53 R3 SI-4 (2)	PCI DSS v2.0 6.3.1 PCI DSS v2.0 6.3.2	AUP v5.0 I.4 SIG v6.0: G.18.3, I.3	GAPP Ref 1.2.6
Security Architecture - Production / Non-Production Environments	SA-06	Production and non-production environments shall be separated to prevent unauthorized access or changes to information assets.	No Change	X	X	X	X		COBIT 4.1 DS5.7		A.10.1.4 A.10.3.2 A.11.1.1 A.12.5.1 A.12.5.2 A.12.5.3	NIST SP800-53 R3 SC-2	NIST SP800-53 R3 SC-2	PCI DSS v2.0 6.4.1 PCI DSS v2.0 6.4.2	AUP v5.0 8.1 SIG v6.0: I.2.7.1, I.2.20, I.2.17,I.2.22.2, I.2.22.4,I.2.22.10-14, H.1.1	GAPP Ref 1.2.6
Security Architecture - Remote User Multi-Factor Authentication	SA-07	Multi-factor authentication is required for all remote user access.	Tenant authentication requirements must be met for all data access.	X	X	X	X	X			A.11.1.1 A.11.4.1 A.11.4.2 A.11.4.6 A.11.7.1	NIST SP800-53 R3 AC-17 NIST SP800-53 R3 AC-20 NIST SP800-53 R3 IA-1 NIST SP800-53 R3 IA-2 NIST SP800-53 R3 MA-4	NIST SP800-53 R3 AC-17 NIST SP800-53 R3 AC-17 (1) NIST SP800-53 R3 AC-17 (2) NIST SP800-53 R3 AC-17 (3) NIST SP800-53 R3 AC-17 (4) NIST SP800-53 R3 AC-17 (5) NIST SP800-53 R3 AC-17 (7) NIST SP800-53 R3 AC-17 (8) NIST SP800-53 R3 AC-20 NIST SP800-53 R3 AC-20 (1) NIST SP800-53 R3 AC-20 (2) NIST SP800-53 R3 IA-1 NIST SP800-53 R3 IA-2 NIST SP800-53 R3 IA-2 (1) NIST SP800-53 R3 IA-2 (2) NIST SP800-53 R3 IA-2 (3) NIST SP800-53 R3 IA-2 (8) NIST SP800-53 R3 MA-4 NIST SP800-53 R3 MA-4 (1) NIST SP800-53 R3 MA-4 (2)	PCI DSS v2.0 8.3	AUP v5.0 8.1 SIG v6.0: H.1.1, G.9.13, G.9.20, G.9.21,	GAPP Ref 8.2.2
Security Architecture - Network Security	SA-08	Network environments shall be designed and configured to restrict connections between trusted and untrusted networks and reviewed at planned intervals, documenting the business justification for use of all services, protocols, and ports allowed, including rationale or compensating controls implemented for those protocols considered to be insecure. Network architecture diagrams must clearly identify high-risk environments and data flows that may have regulatory compliance impacts.	No Change	X	X	X	X	X			A.10.6.1 A.10.6.2 A.10.9.1 A.10.10.2 A.11.4.1 A.11.4.5 A.11.4.6 A.11.4.7 A.15.1.4	NIST SP800-53 R3 SC-7	NIST SP800-53 R3 SC-7 NIST SP800-53 R3 SC-7 (1) NIST SP800-53 R3 SC-7 (2) NIST SP800-53 R3 SC-7 (3) NIST SP800-53 R3 SC-7 (4) NIST SP800-53 R3 SC-7 (5) NIST SP800-53 R3 SC-7 (7) NIST SP800-53 R3 SC-7 (8) NIST SP800-53 R3 SC-7 (12) NIST SP800-53 R3 SC-7 (13) NIST SP800-53 R3 SC-7 (18)	PCI DSS v2.0 1.1 PCI DSS v2.0 1.1.2 PCI DSS v2.0 1.1.3 PCI DSS v2.0 1.1.5 PCI DSS v2.0 1.1.6 PCI DSS v2.0 1.2 PCI DSS v2.0 1.2.1 PCI DSS v2.0 2.2.2, PCI DSS v2.0 2.2.3	AUP v5.0 G.2 AUP v5.0 G.4 AUP v5.0G.15 AUP v5.0G.18 AUP v5.0 G.16 AUP v5.0 I.3 AUP v5.0 G.17 SIG v6.0: G.9.17, G.9.7, G.10, G.9.11, G.14.1, G.15.1, G.9.2, G.9.3, G.9.13	GAPP Ref 8.2.5
Security Architecture - Segmentation	SA-09	System and network environments are separated by firewalls to ensure the following requirements are adhered to: • Business and customer requirements • Security requirements • Compliance with legislative, regulatory, and contractual requirements • Separation of production and non-production environments • Preserve protection and isolation of sensitive data	No Change	X	X	X	X	X	COBIT 4.1 DS5.10	45 CFR 164.308 (a)(4)(ii)(A)	A.11.4.5 A.11.6.1 A.11.6.2 A.15.1.4	NIST SP800-53 R3 AC-4 NIST SP800-53 R3 SC-2 NIST SP800-53 R3 SC-3 NIST SP800-53 R3 SC-7	NIST SP800-53 R3 AC-4 NIST SP800-53 R3 SC-2 NIST SP800-53 R3 SC-3 NIST SP800-53 R3 SC-7 NIST SP800-53 R3 SC-7 (1) NIST SP800-53 R3 SC-7 (2) NIST SP800-53 R3 SC-7 (3) NIST SP800-53 R3 SC-7 (4) NIST SP800-53 R3 SC-7 (5) NIST SP800-53 R3 SC-7 (7) NIST SP800-53 R3 SC-7 (8) NIST SP800-53 R3 SC-7 (12) NIST SP800-53 R3 SC-7 (13) NIST SP800-53 R3 SC-7 (18)	PCI DSS v2.0 1.1 PCI DSS v2.0 1.2 PCI DSS v2.0 1.2.1 PCI DSS v2.0 1.3 PCI DSS v2.0 1.4	AUP v5.0 G.17 SIG v6.0: G.9.2, G.9.3, G.9.13	N/A

Copyright © 2010, Cloud Security Alliance

Control Area	Control ID	Control Specification	Control Revisions v1.1	Cloud Service Delivery Model Applicability			Scope Applicability		Compliance Frameworks								
				SaaS	PaaS	IaaS	Service Provider	Tenant	COBIT 4.1	HIPAA / HITECH Act	ISO/IEC 27001:2005	NIST SP800-53	FedRAMP	PCI DSS v2.0	NZ ISO Security Assurance Framework ASF v0.1 ISO v4.0	GAPP (Aug 2009)
Security Architecture - Wireless Security	SA-10	Policies and procedures shall be established and mechanisms implemented to protect wireless network environments, including the following: • Perimeter firewalls implemented and configured to restrict unauthorized traffic • Security settings enabled with strong encryption for authentication and transmission, replacing vendor default settings (e.g., encryption keys, passwords, SNMP community strings, etc.) • Logical and physical user access to wireless access devices restricted to authorized personnel • The capability to detect the presence of unauthorized (rogue) wireless network devices for a timely disconnect from the network	No Change	X	X	X	X	X	COBIT 4.1 DS5.8 COBIT 4.1 DS9.1 COBIT 4.1 DS5.9 COBIT 4.1 DS5.10	45 CFR 164.312 (a)(1)(i)(ii)(B) 45 CFR 164.306(a)(1)(i)(ii) (New) 45 CFR 164.312(e)(1)(i) (New) 45 CFR 164.312(e)(2)(ii) (New)	A.7.1.1 A.7.1.2 A.7.1.3 A.5.2.1 A.9.2.4 A.10.6.1 A.10.6.2 A.10.6.1 A.10.6.3 A.10.6.5 A.10.10.2 A.11.5.1 A.11.4.3 A.11.4.5 A.11.4.6 A.11.4.7 A.12.3.1 A.15.1.2	NIST SP800-53 R3 AC-1 NIST SP800-53 R3 AC-18 NIST SP800-53 R3 CM-6 NIST SP800-53 R3 PE-4 NIST SP800-53 R3 SC-3 NIST SP800-53 R3 SC-7	NIST SP800-53 R3 AC-1 NIST SP800-53 R3 AC-18 NIST SP800-53 R3 AC-18 (1) NIST SP800-53 R3 AC-18 (2) NIST SP800-53 R3 AC-18 (3) NIST SP800-53 R3 AC-18 (4) NIST SP800-53 R3 AC-18 (5) NIST SP800-53 R3 CM-6 NIST SP800-53 R3 CM-6 (1) NIST SP800-53 R3 CM-6 (3) NIST SP800-53 R3 PE-4 NIST SP800-53 R3 SC-3 NIST SP800-53 R3 SC-7 NIST SP800-53 R3 SC-7 (1) NIST SP800-53 R3 SC-7 (2) NIST SP800-53 R3 SC-7 (3) NIST SP800-53 R3 SC-7 (4) NIST SP800-53 R3 SC-7 (5) NIST SP800-53 R3 SC-7 (7) NIST SP800-53 R3 SC-7 (8) NIST SP800-53 R3 SC-7 (12) NIST SP800-53 R3 SC-7 (13) NIST SP800-53 R3 SC-7 (18)	PCI DSS v2.0 1.2.3 PCI DSS v2.0 2.1.1 PCI DSS v2.0 4.1 PCI DSS v2.0 4.1.1 PCI DSS v2.0 11.1 PCI DSS v2.0 11.1.3	AUP v5.0 D.1 AUP v5.0 D.3 AUP v5.0 F.1 AUP v5.0 9.1 AUP v5.0 9.15 AUP v5.0 9.17 AUP v5.0 9.18 SIG v6.0 E.3.1, F.1.2.4, F.1.2.5, F.1.2.6, F.1.2.8, F.1.2.9, F.1.2.10, F.1.2.11, F.1.2.12, F.1.2.13, F.1.2.14, F.1.2.15, F.1.2.24, F.1.3, F.1.4.2, F.1.4.6, F.1.4.7, F.1.6, F.1.7 F.1.8, F.2.13, F.2.14, F.2.15, F.2.16, F.2.17, F.2.18 G.9.17, G.9.7, G.10, G.9.11, G.14.1, G.15.1, G.9.2, G.9.3, G.9.13	GAPP Ref 8.2.5
Security Architecture - Shared Networks	SA-11	Access to systems with shared network infrastructure shall be restricted to authorized personnel in accordance with security policies, procedures and standards. Networks shared with external entities shall have a documented plan detailing the compensating controls used to separate network traffic between organizations.	No Change	X	X	X	X	X		45 CFR 164.312 (a)(1) (New)	A.10.6.1 A.11.1.1 A.11.5.2 A.11.4.5	NIST SP800-53 R3 PE-4 NIST SP800-53 R3 SC-4 NIST SP800-53 R3 SC-7	NIST SP800-53 R3 PE-4 NIST SP800-53 R3 SC-4 NIST SP800-53 R3 SC-7 NIST SP800-53 R3 SC-7 (1) NIST SP800-53 R3 SC-7 (2) NIST SP800-53 R3 SC-7 (3) NIST SP800-53 R3 SC-7 (4) NIST SP800-53 R3 SC-7 (5) NIST SP800-53 R3 SC-7 (7) NIST SP800-53 R3 SC-7 (8) NIST SP800-53 R3 SC-7 (12) NIST SP800-53 R3 SC-7 (13) NIST SP800-53 R3 SC-7 (18)	PCI DSS v2.0 1.3.5 PCI DSS v2.0 2.4	AUP v5.0 B.1 SIG v6.0: D.1.1, E.1, F.1.1, H.1.1,	GAPP Ref 8.2.5
Security Architecture - Clock Synchronization	SA-12	An external accurate, externally agreed upon, time source shall be used to synchronize the system clocks of all relevant information processing systems within the organization or explicitly defined security domain to facilitate tracing and reconstitution of activity timeline. Note: specific legal jurisdictions and orbital storage and relay platforms (US GPS & EU Galileo Satellite Network) may mandate a reference clock that differs in synchronization with the organizations domicile time reference. In this event the jurisdiction or platform is treated as an explicitly defined security domain.	No Change	X	X	X	X		COBIT 4.1 DS5.7		A.10.10.1 A.10.10.6	NIST SP800-53 R3 AU-1 NIST SP800-53 R3 AU-8	NIST SP800-53 R3 AU-1 NIST SP800-53 R3 AU-8 NIST SP800-53 R3 AU-8 (1)	PCI DSS v2.0 10.4	AUP v5.0 G.7 AUP v5.0 G.8 SIG v6.0: G.13, G.14.8, G.15.5, G.15.8, G.17.6, G.18.3, G.19.2.6, G.19.3.1,	N/A
Security Architecture - Equipment Identification	SA-13	Automated equipment identification shall be used as a method of connection authentication. Location-aware technologies may be used to validate connection authentication integrity based on known equipment location.	No Change						COBIT 4.1 DS5.7		A.11.4.3	NIST SP800-53 R3 IA-3 NIST SP800-53 R3 IA-4	NIST SP800-53 R3 IA-3 NIST SP800-53 R3 IA-4 NIST SP800-53 R3 IA-4 (4)		AUP v5.0 D.1 SIG v6.0: D.1.1, D.1.3	N/A
Security Architecture - Audit Logging / Intrusion Detection	SA-14	Audit logs recording privileged user access activities, authorized and unauthorized access attempts, system exceptions, and information security events shall be retained, complying with applicable policies and regulations. Audit logs shall be reviewed at least daily and file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis and response to incidents. Physical and logical user access to audit logs shall be restricted to authorized personnel.	No Change	X	X	X	X		COBIT 4.1 DS5.5 COBIT 4.1 DS9.6 COBIT 4.1 DS9.2	45 CFR 164.308 (a)(1)(ii)(D) 45 CFR 164.312 (b) 45 CFR 164.306(a)(5)(ii)(c) (New)	A.10.10.1 A.10.10.2 A.10.10.3 A.10.10.4 A.10.10.5 A.11.2.2 A.11.5.4 A.11.6.1 A.13.1.1 A.13.2.3 A.15.2.2 A.15.1.3	NIST SP800-53 R3 AU-1 NIST SP800-53 R3 AU-2 NIST SP800-53 R3 AU-3 NIST SP800-53 R3 AU-4 NIST SP800-53 R3 AU-5 NIST SP800-53 R3 AU-6 NIST SP800-53 R3 AU-7 NIST SP800-53 R3 AU-9 NIST SP800-53 R3 AU-11 NIST SP800-53 R3 AU-12 NIST SP800-53 R3 AU-14 NIST SP800-53 R3 SI-4	NIST SP800-53 R3 AU-1 NIST SP800-53 R3 AU-2 NIST SP800-53 R3 AU-2 (3) NIST SP800-53 R3 AU-2 (4) NIST SP800-53 R3 AU-3 NIST SP800-53 R3 AU-3 (1) NIST SP800-53 R3 AU-4 NIST SP800-53 R3 AU-5 NIST SP800-53 R3 AU-6 NIST SP800-53 R3 AU-6 (1) NIST SP800-53 R3 AU-6 (3) NIST SP800-53 R3 AU-7 NIST SP800-53 R3 AU-7 (1) NIST SP800-53 R3 AU-9 NIST SP800-53 R3 AU-9 (2) NIST SP800-53 R3 AU-11 NIST SP800-53 R3 AU-12 NIST SP800-53 R3 AU-14 NIST SP800-53 R3 SI-4 NIST SP800-53 R3 SI-4 (2) NIST SP800-53 R3 SI-4 (4) NIST SP800-53 R3 SI-4 (5) NIST SP800-53 R3 SI-4 (6)	PCI DSS v2.0 10.1 PCI DSS v2.0 10.2 PCI DSS v2.0 10.3 PCI DSS v2.0 10.5 PCI DSS v2.0 10.6 PCI DSS v2.0 10.7 PCI DSS v2.0 11.4 PCI DSS v2.0 12.5.2 PCI DSS v2.0 12.9.5	AUP v5.0 G.7 AUP v5.0 G.8 AUP v5.0 G.9 AUP v5.0 J.1 AUP v5.0 L.2 SIG v6.0 G.14.7, G.14.8, G.14.9, G.14.10, G.14.11, G.14.12, G.15.5, G.15.7, G.15.8, G.16.8, G.16.9, G.16.10, G.15.9, G.17.5, G.17.7, G.17.8 G.17.6, G.17.9, G.18.2, G.18.3, G.18.5, G.18.6, G.19.2.6, G.19.3.1, G.9.5.2, G.9.5.3, G.9.5.4, G.9.16, H.2.18, H.3.3, J.1, J.2, L.5, L.9, L.10	GAPP Ref 8.2.1 GAPP Ref 8.2.2
Security Architecture - Mobile Code	SA-15	Mobile code shall be authorized before its installation and use, and the configuration shall ensure that the authorized mobile code operates according to a clearly defined security policy. All unauthorized mobile code shall be prevented from executing.	No Change	X	X	X	X	X			A.10.4.2 A.12.2.2	NIST SP800-53 R3 SC-18	NIST SP800-53 R3 SC-18 NIST SP800-53 R3 SC-18 (4)		SIG v6.0 G.20.12, I.2.5	N/A

Copyright © 2010 Cloud Security Alliance. All rights reserved. You may download, store, display on your computer, view, print, and link to the Cloud Security Alliance "Cloud Controls Matrix (CCM)" at http://www.cloudsecurityalliance.org/ccm.html subject to the following: (a) the Cloud Controls Matrix may be used solely for your personal, informational, non-commercial use; (b) the Cloud Controls Matrix may not be modified or altered in any way; (c) the Cloud Controls Matrix may not be redistributed; and (d) the trademark, copyright or other notices may not be removed. You may quote portions of the Questionnaire as permitted by the Fair Use provisions of the United States Copyright Act, provided that you attribute the portions to the Cloud Security Alliance Cloud Controls Matrix Version 1.1 (2010). If you are interested in obtaining a license to this material for other usages not addresses in the copyright notice, please contact info@cloudsecurityalliance.org.

QA by the HISPI
12/01/10

APPENDIX I

CONTRACT MODIFICATION PROCEDURE

The following guidelines are subject to change at the discretion of OGS. A Contract Amendment requires a formally executed document by mutual agreement of the Parties, to be provided by OGS Contract Administrator, after submission and approval of the Contract Modification Form.

(1) **TYPES OF CONTRACT MODIFICATIONS:** In order to expedite processing of a contract modification, where proposed changes involve more than one category below, each change should be submitted to OGS as a separate request.

a) **UPDATES**: "Updates" are changes that do not require a change to the established Centralized Contract terms and conditions. Updates may include: Centralized Contract changes and updates made in accordance with the previously approved pricing formula (e.g. discount from list price); adding new products or services within the established, previously approved pricing structure; lowering pricing of products or services already on Contract, deleting products or services available through the Centralized Contract, adding product or service that do not fall under the previously established price structure or discounts under the Contract, re-bundled products, and other updates not listed above that are deemed to be in the best interest of the State and do not result in a change to the established Centralized Contract terms and conditions. Updates must be submitted to OGS for review, and must be accompanied by a justification of reasonableness of price if the change results in a change in pricing methodology. OGS will notify Contractor in writing if approved.

b) **AMENDMENTS**: "Amendments" are changes that are not specifically covered by the terms and conditions of the Centralized Contract but inclusion is found to be in the best interest of the State. Requests for product changes and other requests that would require changes to the terms and conditions of the Centralized Contract would fall into the Amendments category. Contractor must provide a written justification of reasonableness of the price levels offered in the applicable Program Agreement and a statement explaining why it is in the best interest of the State to approve the requested amendment. Amendments typically require negotiation between OGS and the Contractor. OGS will work directly with the Contractor to obtain the required documentation for each requested amendment and notify Contractor in writing if approved.

(2) **CONTRACTOR'S SUBMISSION OF CONTRACT MODIFICATIONS:** In connection with any Contract modification, OGS reserves the right to:

- request additional information
- reject Contract modifications
- remove Products from Contract modification requests
- request additional discounts for new or existing Products

(3) **PRICE LEVEL JUSTIFICATION – FORMAT**: Contractor is required to submit the Product and price level information for the update in an Excel spreadsheet format electronically via e-mail (and in hard copy if requested by OGS) to the OGS Contract Administrator. The list must be dated. The Product and

price level information should include and identify (e.g., by use of separate worksheets or by using italics, bold and/or color fonts):

- Price level increases
- Price level decreases
- Products being added

(4) **SUPPORTING DOCUMENTATION:** Each modification request must include the current contract pricing discount relevant to the Products included in the update.

(5) **SUBMITTAL OF MODIFCATION REQUESTS:** A Contract modification request must be accompanied by a completed Contract Modification Form. Contractor should briefly describe the nature and purpose of the update (e.g., update requested in order to reflect a recently approved GSA schedule, to restructure the price level to its customers generally, and/or for new Products which fall into a new group or category that did not exist at the time of approval of the Contract by OGS). The Contract Modification Form must contain original signatures by an individual authorized to sign on behalf of Contractor and must be notarized.