



# Texas Department of Public Safety Purchase Order

Purchase Order Number  
  
405-16-P004451  
  
SHOW THIS NUMBER ON ALL  
PACKAGES, INVOICES AND  
SHIPPING DOCUMENTS.

**V  
E  
N  
D  
O  
R**  
Vendor Number: 00009579  
1263464715500 | CBM ARCHIVES CO LLC  
  
1779 WELLS BRANCH PKWY  
#110 B-369  
USA  
AUSTIN, TX 78728-7090

**S  
H  
I  
P  
T  
O**  
Texas Department of Public Safety  
Law Enforcement Support  
5805 North Lamar Blvd  
Austin, TX 78752-4431  
US  
Email: [eprocurementshipping@dps.texas.gov](mailto:eprocurementshipping@dps.texas.gov)  
Phone: (512) 424-2000

State Sales Tax Exemption Certificate: The undersigned claims an exemption from taxes under Chapter 20, Title 122A, Revised Civil Statutes of Texas, for purchase of tangible personal property described in this numbered order, purchased from contractor and/or shipper listed above, as this property is being secured for the exclusive use of the State of Texas.

**B  
I  
L  
L  
T  
O**  
Texas Department of Public Safety  
Finance - Accounts Payable - MSC 0130  
PO Box 4087  
Austin, TX 78773-0130  
US  
Email: [apinvoices@dps.texas.gov](mailto:apinvoices@dps.texas.gov)  
Phone: (512) 424-2060

Solicitation (Bid) No.:

Payment Terms:  
  
Shipping Terms:  
  
Delivery Calendar Day(s) A.R.O.: 0

Item # 1  
 Class-Item 920-45

Contract for application maintenance and support of existing TxGang database. The period of services will be from 09/01/2015 through 08/31/2016 in the amount of \$388,800.00.

The contract includes three (3) one (1) year Optional Renewal periods as follows: \$428,400.00 - September 01, 2016 through August 31, 2017; \$471,600.00 - September 01, 2017 through August 31, 2018;and \$518,400.00 - September 01, 2018 through August 31, 2019

This PO incorporates the fully executed Statement of Work dated xx/xxxx. In case of conflicting provisions, the documents shall control in the following order of precedence:

1. DIR contract DIR-SDD-1966 and all amendments
2. TXDPS issued Purchase Order and any subsequent Purchase Order Change Notices
3. TXDPS Technology Terms and Conditions dated 12/10/2014
4. Best And Final Offer response dated 8/13/2015.
5. TXDPS Solicitation Pricing Request 405-15-R025523 and any subsequent modifications and amendments
6. CBM Archives Co., LLC response to Request for Offer 405-15-R025523

Vendor Point of Contact: Jerry Sanders  
 jerry.sanders@cbmarchives.com  
 361.241.2310

End User Point of Contact: Michelle Farris  
 michelle.farris@dps.texas.gov  
 Phone: 512.424.7659

Procurement Point of Contact: Luis Blanco  
 512.424.7626  
 luis.blanco@dps.texas.gov

Quantity	Unit Price	UOM	Discount %	Total Discount Amt.	Tax Rate	Tax Amount	Freight	Total Cost
12.00	\$ 32,400.00	EA	0.00 %	\$ 0.00		\$ 0.00	\$ 0.00	\$ 388,800.00

LN/FY/Account Code	Dollar Amount
1/16/16-41031-6245-6001- - -1100- - -	\$ 388,800.00

Item # 2  
 Class-Item 920-40

TX Gang Development - CO-001 - FY16

Quantity	Unit Price	UOM	Discount %	Total Discount Amt.	Tax Rate	Tax Amount	Freight	Total Cost
1.00	\$ 94,800.00	EA	0.00 %	\$ 0.00		\$ 0.00	\$ 0.00	\$ 94,800.00

LN/FY/Account Code	Dollar Amount
2/16/16-65654-6255-1001- - -1100- - -	\$ 94,800.00

TAX:	\$ 0.00
FREIGHT:	\$ 0.00
TOTAL:	\$ 483,600.00

APPROVED

By: Bridget Barksdale, CTCM, CTPM

Phone#: (512) 424-2888

BUYER



**TEXAS DEPARTMENT OF PUBLIC SAFETY (TXDPS)  
Pricing Request (PR)**

PR OPENING ▶ 1:00 p.m. 06/30/2015

SOLICITATION NO: ▶ 405-15-R025523

FAILURE TO SIGN WILL DISQUALIFY PR

<b>AGENCY TO INVOICE</b>
Texas Department of Public Safety Accounting and Budget Control P.O. Box 4087 Austin, Texas 78773-0130 apinvoice@dps.texas.gov
<b>DESTINATION OF GOODS IF DIFFERENT THAN ABOVE</b>
Texas Department of Public Safety 5805 N. Lamar Blvd. Austin, TX 78752

IF NOT  
QUOTING  
DO NOT  
RETURN  
THIS  
FORM.

\_\_\_\_\_  
**AUTHORIZED SIGNATURE**                      **DATE**

By signing this PR, the Respondent certifies that if a Texas address is shown as the address of the response, the Respondent qualifies as a Texas Bidder as defined in 34 TAC Rule 20.32(68).

t VENDOR ADDRESS AND IDENTIFICATION NUMBER t

DELIVERY IN \_\_\_\_\_ DAYS AFTER RECEIPT OF ORDER (ARO)  
 CASH DISCOUNT \_\_\_\_\_% \_\_\_\_\_ DAYS OR NET 30

**WHEN QUOTING:**  
 The Vendor shall indicate pricing with an authorized signature on this PR form and fill out all pricing tables or attachments. The Vendor may at its option enclose a separate Quote on its Company letterhead; however, all terms and conditions or deviation language on the Vendor's Quote will not apply to the PR or any awarded Purchase Order (PO).

Vendor Federal VIN#: \_\_\_\_\_  
 Vendor TINS #: \_\_\_\_\_  
 Vendor Name: \_\_\_\_\_  
 Vendor Address: \_\_\_\_\_  
 \_\_\_\_\_  
 Vendor State: \_\_\_\_\_ Zip: \_\_\_\_\_  
 Vendor contact: \_\_\_\_\_  
 Contact Phone #: \_\_\_\_\_

**THIS PRICING REQUEST (PR) SHALL BE SUBMITTED WITH SIGNATURES AND PRICING**

This PR is solicited in accordance with the Department of Information Resources (DIR) Master Contract(s) awarded for the products and services listed below.

LINE ITEM NO.	CLASS & ITEM	DESCRIPTION	QUANTITY	UNIT	UNIT PRICE	EXTENSION
001	Application Maintenance and Support - Service Term 09/01/15 - 08/31/16		12	MONTHS		
002	Application Maintenance and Support - Renewal Option - Renewal option # 1- 09/01/16 - 08/31/17		12	MONTHS		
003	Application Maintenance and Support - Renewal Option - Renewal option # 2- 09/01/17 - 08/31/18		12	MONTHS		
004	Application Maintenance and Support - Renewal Option - Renewal option # 3- 09/01/18 - 08/31/19		12	MONTHS		

**Check below if preference claimed under 34 TAC Rule 20.38**

- |  |  |
|--|--|
| <input type="checkbox"/> Goods produced or services offered by a Texas bidder that is owned by a Texas resident service-disabled veteran | <input type="checkbox"/> Goods produced or services offered in Texas or offered by a Texas Bidder that is not owned by a Texas resident service-disabled veteran |
| <input type="checkbox"/> Vendors that meet or exceed air quality standards   | <input type="checkbox"/> Energy efficient products   |
| <input type="checkbox"/> Services offered by a Texas bidder that is owned by a Texas resident service-disabled veteran                   | <input type="checkbox"/> Products and services from economically depressed or blighted areas   |
| <input type="checkbox"/> Recycled or Reused Computer Equipment of Other Manufacturers  | <input type="checkbox"/> Products produced at facilities located on formerly contaminated property   |
| <input type="checkbox"/> USA produced supplies, materials, or equipment  | <input type="checkbox"/> Products made of recycled, remanufactured, or environmentally sensitive materials including recycled steel                              |

**ORDER OF PRECEDENCE:**

This Contract is comprised of the following documents and in the event of conflict will control in the following order:  
The DIR Master Contract;  
The TXDPS PO with all subsequent Change Orders;  
The TXDPS Pricing Request Terms and Conditions to DIR Vendors, dated 12/10/14, with all attachments.  
The Pricing Request as posted with all Attachments, Exhibits and Appendices; and  
The Vendor's Response.

**DIR MASTER CONTRACT NUMBER:**

The Vendor shall indicate its DIR Master Contract Number: DIR-SDD-\_\_\_\_\_

**DELIVERY:**

The Vendor shall include an estimated time of delivery (business days) ARO: \_\_\_\_\_

**QUANTITIES:**

Enhancement services will be requested on an as needed basis. TXDPS reserves the right to increase or decrease the quantity of the PO at the same original terms and conditions throughout the service term of the PO. The Vendor shall be notified in writing with a fully executed contract modification of any requirements for additional quantities.

**TERM AND RENEWAL OPTIONS:**

This Contract is effective from 9/1/15 through 8/31/16 and may be renewed for up to three (3) additional one (1) year option periods at the same, original terms and conditions and at the same price quoted for each renewal period providing both parties agree in writing prior to the expiration date.

**Scoring Matrix**

Technical Response:	70%
Cost:	30%
Total:	100%

**CONNECTED AGREEMENTS:**

If software subscriptions / End-User Licenses / Maintenance & Support or Warranty agreements are applicable to the requested products, it is the responsibility of the Vendor to provide such licenses / Agreements with the submission of its PR response. Any documents (Vendor's or 3<sup>rd</sup> Party) which are provided at a later date, may not be accepted by TXDPS nor applied to the products and services procured. Any related requirements will be the sole responsibility of the Vendor to include any costs, deliverables, and contractual requirements - TXDPS will have no obligation to any such Terms, Conditions, and / or Requirements. However; TXDPS will receive in full, all functionality identified and necessary as stated in such omitted agreements.

**PR DOCUMENTS to be submitted with the Vendor's Response:**

- PR document with all attachments, exhibits, and addendas
  - PR Attachment A - Service Category pricing by title and individual (as back-up to monthly maintenance and support fees and as back-up to the flat-fee deliverable for each enhancement Change Order).
- PR Attachment B- Pricing Request (PR) Terms and Conditions for DIR Vendors:
  - Appendix A- System Security and Access,
  - Appendix B- System Architecture and IT Requirements.
- PR Attachment C - Statement of Work
  - Appendix A- Cloud Security Alliance's (CSA) Cloud Control Matrix (CCM)
- PR Exhibit 1 - Change Order Template
- PR Exhibit 2- Change Order Completion Acceptance Document

**FINANCIAL RATING:**

The Vendor shall submit a copy of at least one rating from organizations such as Dun & Bradstreet (D&B) Business Information Report or Fitch Ratings. The report shall include the Respondent's Viability Score and the Portfolio Comparison Score or similar ratings. Failure to submit copies of the required financial ratings will result in disqualification.

The Vendor shall provide information and any other financial information reasonably requested by the TXDPS consistent with the services provided by the Contractor or otherwise required by the then applicable TXDPS policies for similar contracts.

**SUBMIT RESPONSES TO:**

Contract Specialist: Luis Blanco  
Phone: 512.424.7626  
Email: luis.blanco@dps.texas.gov

**SUBMIT QUESTIONS AND CLARIFICATION REQUESTS TO:**

The individual listed above may be telephoned or emailed for clarification of the specifications only. No authority is intended or implied that specifications may be amended or alternates accepted prior to the response due date without written approval. **The deadline for Vendors to submit questions in writing is 06/15/2015. TXDPS will respond to the questions in writing and post the answers on the ESD (Electronic State Bidders Daily) on or before 06/19/2015.**

**HISTORICALLY UNDERUTILIZED BUSINESS PARTICIPATION:**

In accordance with Texas Gov't Code §2161.252, each state agency that considers entering into a contract with an expected value of \$100,000 or more over the life of the contract (including any renewals) shall, before the agency solicits bids, proposals, offers, or other applicable expressions of interest, determine whether subcontracting opportunities are probable under this Contract.

**As a Department of Information Resources (DIR) awarded Contractor, your HUB Subcontracting Plan (HSP) included in your contract is the official HSP. All respondents, including State of Texas certified Historically Underutilized Businesses (HUBs) must submit the HSP with their response to the bid solicitation.**

Note: Responses that do not include their official HSP maybe rejected pursuant to Texas Gov't Code 2161.252(b)

If changes are required to your HSP, the Contractor shall seek written approval from the DIR prior to making any modifications to the HSP. An approved modified HSP must be sent to the Department of Public Safety (DPS) if awarded.

POST-AWARD HSP REQUIREMENTS: After contract award, the Department may coordinate a post-award meeting with the successful respondent to discuss HSP reporting requirements. The Contractor shall submit the "Prime Contractor Progress Assessment Report" (PAR) to the DPS HUB Office at [DPSHUB@DPS.TEXAS.GOV](mailto:DPSHUB@DPS.TEXAS.GOV) and the Contract Administrator on a monthly basis (by the 5th day of the following month). This monthly report is required as a condition for payment to report to the agency the identity and the amount paid to all subcontractors.

This contract is issued in accordance with DIR Outsourced Deliverables-Based Projects which can be reviewed at <http://dir.texas.gov>.

HUB Subcontracting Plan

UPON MUTUAL CONCURRENCE OF TXDPS AND THE CONTRACTOR, MODIFICATION(S) MAY BE ISSUED FOR ANY CHANGES TO THE PURCHASE ORDER (PO), IDENTIFIED DELIVERABLES, AND / OR SERVICETIME LINES SHALL BE AGREED TO BY BOTH PARTIES IN WRITING. CHANGES SHALL NOT BECOME EFFECTIVE UNTIL OFFICIAL NOTICE IS PROVIDED BY TXDPS PROCURMENT AND CONTRACT SERVICES (P&CS). ANY EQUIPMENT OR SERVICES PROVIDED BY THE CONTRACTOR PRIOR TO AUTHORIZATION WILL BE CONSIDERED A DONATION TO THE AGENCY.



**PRICING REQUEST (PR)  
ISSUED BY TXDPS  
TO DIR VENDORS**

1. Vendor understands that TXDPS is a “Customer” under the Vendor’s DIR Contract referenced on page 1 of the TXDPS Purchase Order, PO. In submitting information to TXDPS in response to this PR, Vendor affirms its understanding of the General Provisions of the Vendor’s DIR Contract (generally located in Section 3) of Appendix A, DIR Standard Terms and Conditions for Deliverables Based Information Technology Services (DBITS) Contracts:

**A. Entire Agreement**

The DIR Contract, Appendices, and Exhibits constitute the entire agreement between DIR and the Vendor. No statement, promise, condition, understanding, inducement or representation, oral or written, expressed or implied, which is not contained in the Contract, Appendices, or its Exhibits shall be binding or valid.

**B. Modification of Contract Terms and/or Amendments**

- 1) The terms and conditions of the DIR Contract shall govern all transactions by Customers under the Contract. The Contract may only be modified or amended upon mutual written agreement of DIR and Vendor.
  - 2) Customers will not have the authority to modify the terms of the Contract; however, additional Customer terms and conditions that do not conflict with the Contract and are acceptable to Vendor may be added in a Purchase Order and given effect. No additional term or condition added in a Purchase Order issued by a Customer can conflict with or diminish a term or condition of the Contract. Pre-printed terms and conditions on any Purchase Order issued by Customer hereunder will have no force and effect. In the event of a conflict between a Customer’s Purchase Order and the Contract, the Contract term shall control.
  - 3) Customers and Vendor will negotiate and enter into written agreements regarding statements of work, service level agreements, remedies, acceptance criteria, information confidentiality and security requirements, and other terms specific to their Purchase Orders under the Contract with Vendor.
2. TXDPS issues this PR as Customer under Vendor’s DIR Contract and requests that Vendor submit a response to TXDPS based on these additional terms and conditions which TXDPS has determined are specific to the TXDPS PO and are allowable under the provisions of Vendor’s DIR Contract, reference Section 1 of this PR.
3. Vendor affirms its understanding that under the DIR DBITS Contract, SOW/PO Issuance clause (generally located in Section 7), Vendor shall respond, in writing, to a Statement of Work (SOW) for services as issued by Customers, consistent with the Terms and Conditions of this Contract in order to be awarded a Purchase Order. Customer SOWs must be complete, signed by an authorized representative of Customer and in the form contained in Attachment C of the Vendor’s DIR Contract. Vendor understands that no work under any SOW issued by Customer shall commence until receipt of Purchase Order.

**4. BOX CHECKED IF THIS SECTION 4 APPLICABLE TO THIS PR.  CONFIDENTIALITY AND SECURITY REQUIREMENTS**

**A. General Confidentiality Requirements**

- 1) All information provided by TXDPS or sub-recipients to Vendor or created by Vendor in performing the obligations under this PO is confidential and shall not be used by Vendor or disclosed to any person or entity, unless such use or disclosure is required for Vendor to perform work under this PO.
- 2) The obligations of this section do not apply to information that Vendor can demonstrate:
  - a. Is publicly available;
  - b. Vendor received from a third party without restriction on disclosure and without breach of contract or other wrongful act;
  - c. Vendor independently developed without regard to the TXDPS confidential information; or
  - d. Is required to be disclosed by law or final order of a court of competent jurisdiction or regulatory authority, provided that Vendor shall furnish prompt written notice of such required disclosure and shall reasonably cooperate with TXDPS at TXDPS’ cost and expense, in any effort made by the TXDPS to seek a protection order or other appropriate protection of its confidential information.
- 3) Vendor shall notify sub-recipient in writing of any unauthorized release of confidential information within two (2) business days of when Vendor knows or should have known of any unauthorized release of confidential information obtained from sub-recipient(s).
- 4) Vendor shall maintain all confidential information, regardless whether obtained from TXDPS or from sub-recipient(s) in confidence during the term of this PO and after the expiration or earlier termination of this PO.
- 5) If Vendor has any questions or doubts as to whether particular material or information is confidential information, Vendor shall obtain the prior written approval of TXDPS prior to using, disclosing, or releasing such information.
- 6) Vendor acknowledges that TXDPS’ and sub-recipient’(s) confidential information is unique and valuable, and that TXDPS and sub-recipient(s) may have no adequate remedy at law if Vendor does not comply with its confidentiality obligations under this PO. Therefore, TXDPS shall have the right, in addition to any other rights it may have, to seek in any Travis County court of competent

jurisdiction temporary, preliminary, and permanent injunctive relief to restrain any breach, threatened breach, or otherwise to specifically enforce any confidentiality obligations of Vendor if Vendor fails to perform any of its confidentiality obligations under this PO.

- 7) Vendor shall immediately return to TXDPS all confidential information when this PO terminates, at such earlier time as when the confidential information is no longer required for the performance of this PO or when TXDPS requests that such confidential information be returned.
- 8) Information, documentation and other material in connection with this PO, including the Vendor's Offer, may be subject to public disclosure pursuant to the Texas Government Code, Chapter 552.
- 9) The FBI and TXDPS have computer security requirements. The Vendor's and subcontractor's employees working on this assignment shall sign and submit appropriate agreements and abide by these security requirements, within five (5) calendar days of TXDPS' request.

#### **B. Sensitive Personal Information**

To the extent this subsection does not conflict with the subsection herein entitled "General Confidentiality Requirements," Vendor shall comply with both subsections. To the extent this subsection conflicts with the subsection herein entitled "General Confidentiality Requirements," this subsection entitled "Sensitive Personal Information" controls.

"Sensitive personal information" is defined as follows:

- 1) An individual's first name or first initial and last name in combination with any one or more of the following items, if the name and the items are not encrypted:
  - a. Social security number;
  - b. Driver's license number or government-issued identification number; or
  - c. Account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account; or
- 2) Information that identifies an individual and relates to:
  - a. The physical or mental health or condition of the individual;
  - b. The provision of health care to the individual; or
  - c. Payment for the provision of health care to the individual.
- 3) Sensitive personal information does not include publicly available information that is lawfully made available to the public from the federal government or a state or local government.
- 4) "Breach of system security" is defined as follows: Unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive personal information Vendor maintains under this PO, including data that is encrypted if the Vendor's employee or agent accessing the data has the key required to decrypt the data. Good faith acquisition of sensitive personal information by an employee or agent of Vendor for the purposes of performing under this PO is not a breach of system security unless the employee or agent of Vendor uses or discloses the sensitive personal information in an unauthorized manner.
- 5) Vendor shall implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect from unlawful use or disclosure any sensitive personal information collected or maintained by Vendor under this PO.
- 6) Vendor shall notify TXDPS, any affected sub-recipient and the affected people of any breach of system security immediately after discovering the breach or receiving notification of the breach, if sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person. However, Vendor shall delay providing notice to the affected people and sub-recipients at TXDPS' request, if TXDPS determines that the notification shall impede a criminal investigation. The notification to the affected people shall be made as soon as TXDPS determines that it will not compromise any criminal investigation.
- 7) Vendor shall give notice as follows, at the Vendor's expense:
  - a. Written notice;
  - b. Electronic notice, if the notice is provided in accordance with 15 U.S.C. Section 7001;
  - c. Notice as follows:
    - i. If Vendor demonstrates that the cost of providing notice would exceed \$250,000, the number of affected people exceeds 500,000, or Vendor does not have sufficient contact information for the affected people, Vendor may give notice as follows:
      - Electronic mail, if Vendor has an electronic mail address for the affected people;
      - Conspicuous posting of the notice on the Vendor's website;
      - Notice published in or broadcast on major statewide media; or
    - ii. If Vendor maintains its own notification procedures (as part of an information security policy for the treatment of sensitive personal information) that comply with the timing requirements for notice under this subsection entitled "Sensitive Personal Information," Vendor may provide notice in accordance with that policy.
- 8) If this subsection requires Vendor to notify at one time more than 10,000 people of a breach of system security, Vendor shall also notify, without unreasonable delay, each consumer reporting agency (as defined by 15 U.S.C. Section 1681a) that maintains files on consumers on a nationwide basis, of the timing, distribution, and content of the notices.
- 9) In the event of a breach of system security, if sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person, TXDPS is authorized to assess liquidated damages in the amount of \$1,000.00 per day \_\_\_\_\_ against Vendor for the following damages; however, TXDPS reserves the right to claim actual damages for any damages other than

the following: limited to the initial assessment and review of lost or compromised data. This amount is a reasonable estimate of the damages TXDPS shall suffer as a result of such breach and is enforceable. Vendor will not be responsible and liquidated damages may not be assessed due to a breach of system security caused entirely by someone other than the Vendor, the Vendor's subcontractor, or the Vendor's agent. Any liquidated damages assessed under this Contract may, at TXDPS' option, be deducted from any payments due the Vendor. TXDPS has the right to offset any liquidated damages payable to TXDPS, as specified above, against any payments due to the Vendor. If insufficient payments are available to offset such liquidated damages, then Vendor shall pay to TXDPS any remaining liquidated damages within fifteen (15) calendar days following receipt of written notice of the amount due.

**5. BOX CHECKED IF THIS SECTION 5 APPLICABLE TO THIS PR.  CRIMINAL HISTORY BACKGROUND CHECK:**

- A. Vendor shall have its project personnel – as specifically identified by TXDPS -- submit to TXDPS a fingerprint-based Criminal History Background Investigation, if required by TXDPS, at the Vendor's expense. To facilitate this Criminal History Background Investigation, each person shall complete TXDPS' Vendor Background Information form (HR-22), which shall be provided by TXDPS.
- B. If TXDPS requires a fingerprint-based Criminal History Background Investigation, Vendor will not allow personnel to work on the project who have not successfully completed TXDPS' fingerprint-based Criminal History Background Investigation and who do not otherwise maintain TXDPS' security clearance. TXDPS has the right to prevent the Vendor's personnel from gaining access to TXDPS' building(s) and computer systems if TXDPS determines that such personnel do not pass the background check or fail to otherwise maintain TXDPS security clearance.
- C. When required, the Vendor's Project Manager shall provide the following to TXDPS' Project Manager within 21 calendar days of receiving this PO: a) the completed Vendor Background Information form (HR-22) for all proposed personnel; and b) acceptable fingerprints for all proposed personnel.
- D. Throughout the term of this PO, TXDPS may require Vendor personnel to submit an annual TXDPS fingerprinted-based Criminal History Background Investigation to TXDPS.
- E. Throughout the term of this PO, Vendor shall promptly notify TXDPS of any activity or action by the Vendor's personnel that may affect that individual's ability to continue to work under this PO.

**6. NOTICE:**

Any written notices required under this PO will be by hand delivery to Vendor's office address specified on Page 1 of this PO or by U.S. Mail, certified, return receipt requested, to TXDPS, 5805 N. Lamar Blvd., Austin, Texas 78752. Notice will be effective on receipt by the affected party. Either party may change the designated notice address in this Section by written notification to the other party.

**7. INFORMATION TECHNOLOGY REQUIREMENTS AND STANDARDS:**

Vendor represents and warrants that it shall comply with all technology, security, accessibility, warranty, maintenance, confidentiality, testing and other standards, policies and procedures of TXDPS and the State of Texas that are applicable to Vendor in its performance of this PO as such standards, policies, and procedures are amended by TXDPS or the State throughout the term of this PO, including any renewal or optional periods. The Information Resource Manager designated by TXDPS shall assist Vendor in reviewing these standards, policies and procedures and identifying those that are applicable to Vendor in its performance of this PO. Vendor shall comply with TXDPS standards and requirements wherever they are applicable to this PO. TXDPS shall have the sole right to waive specific requirements if, in its sole judgment doing so would mitigate costs or risks or significantly improve the installed and configured solution. If required for this PR, additional requirements are included as Appendices to this PR.

- A. **System Security and Access**, if required for this PR, this information is provided as Appendix A to this PR.
- B. **System Architecture and TXDPS IT Requirements**, if required for this PR, this information is provided as Appendix B to this PR.

**8. TEXAS PUBLIC INFORMATION ACT:**

The Confidentiality Clause included in Vendor's DIR Contract (generally located in Section 8) of Appendix A, DIR Standard Terms and Conditions for Deliverables Based Information Technology Services (DBITS) Contracts, is modified to include the following sentence. Vendor shall make any information created or exchanged with the state pursuant to this PO, and not otherwise exempted from disclosure under the Texas Public Information Act, available in a format that is accessible by the public at no additional charge to the state. TXDPS requires such information to be available in Arial format.

**9. U.S. DEPARTMENT OF HOMELAND SECURITY'S E-VERIFY SYSTEM**

By entering into this Contract, the Contractor certifies and ensures that it utilizes and will continue to utilize, for the term of this Contract, the U.S. Department of Homeland Security's E-Verify system to determine the eligibility of:

- All persons employed to perform duties within Texas, during the term of the Contract; and
- All persons (including subcontractors) assigned by the Respondent to perform work pursuant to the Contract, within the United States of America.

The Contractor shall provide, upon request of (agency name), an electronic or hardcopy screenshot of the confirmation or tentative non-confirmation screen containing the E-Verify case verification number for attachment to the Form I-9 for the three most recent hires that match the criteria above, by the Contractor, and Contractor's subcontractors, as proof that this provision is being followed.

**If this certification is falsely made, the Contract may be immediately terminated, at the discretion of the state and at no fault to the state, with no prior notification. The Contractor shall also be responsible for the costs of any re-solicitation that the state must undertake to replace the terminated Contract.**

**10. VENDOR AFFIRMATIONS TO TXDPS:**

Signing a response to this PR with a false statement or otherwise providing TXDPS with a false statement is a material breach of contract and shall void this PO, and Vendor shall be removed from all bid lists. During the term of this PO, Vendor shall, for itself and on behalf of its subcontractors, promptly disclose to TXDPS all changes that occur to the foregoing certifications, representations and warranties. Vendor covenants to fully cooperate in the development and execution of resulting documentation necessary to maintain an accurate record of the certifications, representations and warranties. By signature hereon affixed, Vendor hereby certifies that:

- A. Vendor has not given, offered to give, nor intends to give at any time hereafter any economic opportunity, future employment, gift, loan, gratuity, special discount, trip, favor, or service to a public servant in connection with this PO.
- B. The Vendor certifies that it is not currently delinquent in the payment of any franchise tax owed the State of Texas and are not ineligible to receive payment under §231.006(d), Texas Family Code, regarding child support, and the that the individual or business entity named in this PO is not ineligible to receive the specified payment and acknowledges that this PO may be terminated and payment may be withheld if this certification is inaccurate. Furthermore, any Vendor subject to §231.006, Gov't Code, shall include names and Social Security numbers of each person with at least 25% ownership of the business entity submitting this PO. This information must be provided prior to award. Enter the Name & Social Security Numbers for each person below:

Name:	Social Security Number:
Name:	Social Security Number:
Name:	Social Security Number:

- B. Under §2155.004, Gov't Code, Vendor certifies that the individual or business entity named in this Offer is not ineligible to receive a PO and acknowledges that this PO may be terminated and payment withheld if this certification is inaccurate. §2155.004 prohibits a person or entity from receiving a state contract if they received compensation for participating in preparing the solicitation or specifications for this PO.
- C. As required by §2252.903, Gov't Code, Vendor agrees that any payments due under this PO shall be directly applied towards eliminating any debt or delinquency including, but not limited to, delinquent taxes, delinquent student loan payments, and delinquent child support, until the debt is paid in full. Vendor shall comply with rules adopted by TXDPS under §§403.055, 403.0551, 2252.903, Gov't Code and other applicable laws and regulations regarding satisfaction of debts or delinquencies to the State of Texas.
- D. Pursuant to §669.003, Gov't Code, TXDPS may not issue a PO to a person who employs a current or former executive head of any state agency until four years has passed since that person was the executive head of the state agency. Vendor certifies that it does not employ any person who was the executive head of any state agency in the past four years. If Vendor does employ a person who was the executive head of a state agency, provide the following information:

Name of Former Executive:

\_\_\_\_\_

Name of State Agency:

\_\_\_\_\_

Date of Separation from State Agency:

\_\_\_\_\_

Position with Vendor:

\_\_\_\_\_

Date of Employment with Vendor:

\_\_\_\_\_

- A. In accordance with §2155.4441, Gov't Code, Vendor agrees that during the performance of this PO it shall purchase products and materials produced in Texas when they are available at a price and time comparable to products and materials produced outside this state.

- B. Vendor certifies that the entity and its principals are eligible to participate in this transaction and have not been subjected to suspension, debarment, or similar ineligibility determined by any federal, state or local governmental entity and that Vendor is in compliance with the State of Texas statutes and rules relating to procurement and that Vendor is not listed on the federal government's terrorism watch list as described in Executive Order 13224. Entities ineligible for federal procurement are listed at <http://www.epls.gov>.
- C. Sections 2155.006 and 2261.053, Gov't Code, prohibit state agencies from awarding contracts to any person who, in the past five years, has been convicted of violating a federal law or assessed a penalty in connection with a contract involving relief for Hurricane Rita, Hurricane Katrina, or any other disaster, as defined by §418.004, Gov't Code, occurring after September 24, 2005. Under §2155.006, Gov't Code, Vendor certifies that the individual or business entity named in this PO is not ineligible to receive a PO and acknowledges that this PO may be terminated and payment withheld if this certification is inaccurate.
- D. Vendor represents and warrants that payment to Vendor and the Vendor's receipt of appropriated or other funds under this PO are not prohibited by §556.005 or §556.008, Gov't Code, relating to the prohibition of using state funds for lobbying activities.
- E. Vendor represents and warrants that it has no actual or potential conflicts of interest in providing the requested items to TXDPS under this PO, if any, and that the Vendor's provision of the requested items under this PO, if any, would not reasonably create an appearance of impropriety.
- F. Vendor certifies that it, nor anyone acting for it, has violated the antitrust laws of the United States or the State of Texas, nor communicated directly or indirectly to any competitor or any other person engaged in such line of business for the purpose of obtaining an unfair price advantage.
- G. Vendor certifies that to the best of its knowledge and belief, there are no suits or proceedings pending or threatened against or affecting it, which if determined adversely to it will have a material adverse effect on its ability to fulfill its obligations under this PO.
- H. To the extent applicable to the scope of this PO, Vendor hereby certifies that it is in compliance with Subchapter Y, Chapter 361, Health and Safety Code related to the Computer Equipment Recycling Program and its rules, 30 TAC Chapter 328.
- N. Vendor certifies for itself and its subcontractors that it has identified all current or former, within the last five (5) years, employees of the State of Texas assigned to work on the TXDPS PO 20% or more of their time and has disclosed them to TXDPS and has disclosed or does not employ any relative of a current or former state employee within two (2) degrees of consanguinity, and, if these facts change during the course of this PO, Vendor certifies it shall disclose for itself and on behalf of subcontractors the name and other pertinent information about the employment of current and former employees and their relatives within two (2) degrees of consanguinity.

**APPENDIX A**  
**SYSTEM SECURITY AND ACCESS**

**PRICING REQUEST (PR)**  
**ISSUED BY TXDPS**  
**TO DIR DBITS VENDORS**

**SYSTEM SECURITY AND ACCESS****Information Technology Standards**

The Contractor represents and warrants that it shall comply with all technology, security, accessibility, warranty, maintenance, confidentiality, testing and other standards, policies and procedures of the Department and the State of Texas that are applicable to the Contractor in its performance of this Contract as such standards, policies, and procedures are amended by the Department or the State throughout the term of this Contract, including any renewal or optional periods. The Information Resource Manager designated by the Department shall assist the Contractor in reviewing these standards, policies and procedures and identifying those that are applicable to the Contractor in its performance of this Contract.

**Cloud Security**

The Contractor shall comply with the current Cloud Security Alliance's (CSA) Cloud Control Matrix (CCM) security requirements for Contractor hosted services or applications that are included as part of Contractor's solution. Information pertaining to CSA <https://cloudsecurityalliance.org/> and CCM information may be found at <https://cloudsecurityalliance.org/research/ccm/>.

**User Security**

- A. Account Management: Establish and administer user accounts in accordance with role-based scheme and shall track and monitor role assignment.
- B. Account Management: Automatically audit account creations, modifications, disabling and termination actions with notification to the Department's personnel.
- C. Prevent multiple concurrent active sessions for one user identification.
- D. Enforce a limit of no more than 3 consecutive invalid access attempts by a user.
- E. Automatically lock the account/node for a 15 minute time period unless released by the Department's Administrator.
- F. Prevent further access to the system by initiating a session lock after a maximum of thirty (30) minutes of inactivity, and the session lock shall remain in effect until the user reestablishes access using appropriate identification and authentication procedures.
- G. Ensure all users shall be uniquely identified.
- H. Force users to follow the secure password attributes, below, to authenticate a user's unique ID. The secure password attributes shall:
  - 1) Be a minimum length of twelve characters;
  - 2) Not be a dictionary word or proper name;
  - 3) Not be the same as the User ID;
  - 4) Expire within a maximum of ninety (90) calendar days;
  - 5) Not be identical to the previous ten (10) passwords;
  - 6) Not be transmitted in the clear text outside the secure location;
  - 7) Not be displayed in clear text when entered; and
  - 8) Never be displayed in clear text on the screen.
  - 9) Must contain two number, two symbols, two upper and two lower case characters.

**System Security**

- A. Provide audit logs that enable tracking of activities taking place on the system.
- B. Audit logs must track successful and unsuccessful system log-on attempts.
- C. Audit logs must track successful and unsuccessful attempts to access, create, write, delete or change permission on a user account, file, directory or other system resource.

- D. Audit logs must track successful and unsuccessful attempts to change account passwords.
- E. Audit logs must track successful and unsuccessful actions by privileged accounts.
- F. Audit logs must track successful and unsuccessful attempts for users to access, modify, or destroy the audit log.
- G. Provide the following content to be included with every audited event:
  - 1) Date and time of the event;
  - 2) The component of the information system (e.g. software component, hardware component) where the event occurred;
  - 3) IP address;
  - 4) Type of event;
  - 5) User/subject identity; and
  - 6) Outcome (success or failure) of the event.
- H. Provide real-time alerts to appropriate Department officials in the event of an audit processing failure. Alert recipients and delivery methods must be configurable and manageable by the Department's System Administrators.
- I. Undergo vulnerability scan/penetration testing conducted by the Department or the Texas Department of Information Resources. The Contractor shall remediate legitimate vulnerabilities and system/application shall not be accepted until all vulnerability issues are resolved at no cost to the Department.
- J. Notifications shall display an approved system use notification message or banner before granting access to the system. The notification shall state:
  - 1) Users are accessing a Department system;
  - 2) System usage shall be monitored, recorded and subject to audit;
  - 3) Unauthorized use of the system is prohibited and subject to criminal and civil penalties; and
  - 4) A description of the authorized use of the system.
- K. The Contractor shall implement and use management and maintenance applications and tools, appropriate fraud prevention and detection, and data confidentiality/protection/encryption technologies for endpoints, servers and mobile devices. This must include mechanisms to identify vulnerabilities and apply security patches.
- L. The Contractor shall establish and maintain a continuous security program as part of the Services. The security program must enable the Organization (or its selected third party) to:
  - 1) Define the scope and boundaries, policies, and organizational structure of an information security management system;
  - 2) Conduct periodic risk assessments to identify the specific threats to and vulnerabilities of the Organization due to the Services, subject to the terms, conditions and procedures;
  - 3) Implement appropriate mitigating controls and training programs, and manage resources; and
  - 4) Monitor and test the security program to ensure its effectiveness. The Contractor shall review and adjust the security program in light of any assessed risks.

### Physical Access Controls

- A. The Contractor shall restrict physical access to the system(s) containing the Department's data to authorized personnel with appropriate clearances and access authorizations.
- B. The Contractor shall enforce physical access authorizations for all physical access points to the facility where information system resides;
- C. The Contractor shall verify individual access authorizations before granting access to the facility containing the information system;
- D. The Contractor shall control entry to the facility containing the information system using physical access devices and guards; and
- E. The Contractor shall change combinations and keys when keys are lost, combinations are compromised, or individuals are transferred or terminated.
- F. The Department and the Contractor shall collaborate on security monitoring and incident response, define points of contact on both sides, establish monitoring and response procedures, set escalation thresholds, and conduct training. The Contractor shall, at the

request of the Department or, in the absence of any request from the Department, at least quarterly, provide the department with a report of the incidents that it has identified and taken measures to resolve.

### Data Security

- A. If the Contractor or any subcontractors require access to the Department's network; the Department's data; or the network processing, transporting, or storing of the Department's data (may at the Department's discretion), the Contractor shall be required to sign the CJIS Security Addendum, and all of the Contractor's employees requiring access to the Department's network shall sign the FBI Certification to the CJIS Security Addendum and complete a fingerprint based background check.
- B. The Contractor's solution shall protect against an employee falsely denying having performed a particular action (non-repudiation).
- C. Require the Contractor, subcontractor, and their staff to obtain and provide proof of PII certifications for its employees accessing the Department's data at the request of the Department.
- D. Comply with relevant federal and state statutes and rules, and the Department's policies, and standards, including but not limited to CJIS requirements.
- E. Data shall not be exported to an external location without the permission of the Department.
- F. In the event of any impermissible disclosure, loss or destruction of Confidential Information, the receiving Party must immediately notify the disclosing Party and take all reasonable steps to mitigate any potential harm or further disclosure, loss or destruction of such Confidential Information.

### Encryption

The system shall protect the confidentiality of the Department's information. All data transmitted outside or stored outside the secure network shall be encrypted. When cryptography (encryption) is employed within information systems, the system shall perform all cryptographic operations using Federal Information Processing Standard (FIPS) PUB140-2 validated cryptographic modules with approved modes of operation. The system shall produce, control, and distributes symmetric cryptographic keys using NIST-approved key management technology and processes. The key management process is subject to audit by the Department. Bcrypt shall be used to mitigate against brute force attacks.

- A. Wireless: The following requirements specifies the minimum set of security measures required on WLAN-enabled portable electronic devices (PEDs) that transmit, receive, process, or store PII or confidential information:
  - 1) Personal Firewall: WLAN-enabled PED shall use personal firewalls or run a Mobile Device Management system that facilitates the ability to provide firewall services.
  - 2) Anti-Virus Software: Anti-virus software shall be used on wireless ECMs-capable PEDs or run a Mobile Device Management System that facilitates the ability to provide anti-virus services.
  - 3) Encryption of PII or confidential data-in-transit via WLAN-enabled PEDs, systems and technologies will be implemented in a manner that protects the data end-to-end. All systems components within a WLAN that wirelessly transmit PII or confidential information shall have cryptographic functionality that is validated under the National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program as meeting requirements per Federal Information Processing Standards (FIPS) Publication 140-2. Encryption shall be a minimum of 128 bit.
  - 4) Data-at-Rest: Data at rest encryption shall be implemented in a manner that protects PII and confidential information stored on WLAN enabled PEDs by requiring that the PED must be powered on and credentials successfully authenticated in order for the data to be deciphered. Data-at-rest encryption shall include the encryption of individual files, portions of the file system (e.g., directories or partitions), or the entire drive (e.g. hard disks, on-board memory cards, memory expansion cards). In recognition of the increased risk of unauthorized access to PII or confidential information in the event that a PED is lost or stolen and the inherently mobile nature of these devices, encryption shall be provided for data-at-rest on all WLAN enabled PEDs that is validated as meeting FIPS 140-2.
  - 5) WLAN Infrastructure: WLAN infrastructure systems may be composed of either stand-alone (autonomous) access points (AP) or thin APS that are centrally controlled by a WLAN controller.
  - 6) Validated Physical Security: APs used in the WLANS should not be installed in unprotected environments due to an increased risk of tampering and/or theft.
- B. Mobile Device Management Requirement. Mobile Device Management (MDM) facilitates the implementation of sound security controls for mobile devices and allows for centralized oversight of configuration control, application usage, and device protection and recovery. MDM shall include the following core features:
  - 1) The ability to push security policies to managed devices;
  - 2) The ability to query the device for its configuration information;
  - 3) The ability to modify device configuration as required;
  - 4) Security functionality that ensures the authenticity and integrity of the transaction in the three categories above;

- 5) Asset management (track/enable/disable) mobile devices being managed via the MDM server;
- 6) The ability to manage proxy access to network resources via the connection of the mobile device to the MDM server;
- 7) The ability to query devices being managed on the status of security policy compliance and to implement a specified mediation function based on compliance status;
- 8) The ability to download and store mobile device audit records;
- 9) The ability to receive alerts and other notifications from managed mobile devices;
- 10) The ability to receive alerts and other notifications from managed mobile devices;
- 11) The ability to generate audit record reports from mobile device audit records; and
- 12) Application management (application white list) for applications installed on managed mobile devices.

### **Secure Erasure Of Hard Disk Capability**

All equipment provided to the Department by the Contractor that is equipped with hard disk drives (i.e. computers, telephones, printers, fax machines, scanners, multifunction devices, etc.) shall have the capability to securely erase data written to the hard drive prior to final disposition of such equipment, either at the end of the equipment's useful life or the end of the related services agreement for such equipment, in accordance with 1 TAC §202.

### **Data Center Location Requirements**

The data center must be located in the continental United States of America.

### **Access to Internal Department Network and Systems**

As a condition of gaining remote access to any internal Department network and systems, the Contractor shall comply with Department policies and procedures. The Department's remote access request procedures shall require the Contractor to submit a Remote Access Request form for the Department's review and approval.

- A. Remote access technologies provided by the Contractor shall be approved by the Department's CISO.
- B. Individuals who are provided with access to the Department network may be required to attend or review the Department's Security Awareness Training on an annual basis.
- C. The Contractor shall secure its own connected systems in a manner consistent with Department requirements.
- D. The Department reserves the right to audit the security measures in effect on the Contractor's connected systems without prior warning.
- E. The Department also reserves the right to immediately terminate network and system connections not meeting such requirements.

### **FBI CJIS Security Addendum**

The Contractor shall execute an originally signed CJIS Security Addendum which can be downloaded from <http://www.txdps.state.tx.us/securityreview>. Additionally, a CJIS Security Addendum Certification shall be signed by each employee performing duties related to this project prior to final Contract award. Each original Certification shall include an original signature of the employee and the Contractor's representative. Non-compliance by Respondent will be cause for termination of contract negotiations and the Department may elect to enter into negotiations with the next highest evaluated Offer.

### **Criminal History Background Checks**

- A. The Contractor shall have its project personnel submit to the Department a fingerprint-based Criminal History Background Investigation, if required by the Department, at the Contractor's expense. To facilitate this Criminal History Background Investigation, each person shall complete the Department's Vendor Background Information form (HR-22), which shall be provided by the Department.
- B. If the Department requires a fingerprint-based Criminal History Background Investigation, the Contractor shall not allow personnel to work on the project who have not successfully completed the Department's fingerprint-based Criminal History Background Investigation and who do not otherwise maintain the Department's security clearance. The Department has the right to prevent the Contractor's personnel from gaining access to the Department's building(s) and computer systems if the Department determines that such personnel do not pass the background check or fail to otherwise maintain the Department security clearance.

- C. When required, the Contractor's Project Manager shall provide the following to the Departments Project Manager within 10 calendar days of executing this Contract:
- 1) the completed Vendor Background Information form (HR-22) for all proposed personnel; and acceptable fingerprints for all proposed personnel.
  - 2) Throughout the term of this Contract, the Department may require the Contractor personnel to submit an annual Department fingerprinted-based Criminal History Background Investigation to the Department.
  - 3) Throughout the term of this Contract, the Contractor shall promptly notify the Department of any activity or action by the Contractor's personnel that may affect that individual's ability to continue to work under this Contract

#### **Department Information Protection Policies, Standards & Guidelines**

- A. Contractor, its employees, and any subcontractors shall comply with all applicable Department Information Protection Policies, Standards & Guidelines and any other Department requirements that relate to the protection or disclosure of Department Information. Department Information includes all data and information
- 1) submitted to Contractor by or on behalf of the Department,
  - 2) obtained, developed, produced by the Contractor in connection with this Contract,
  - 3) communicated verbally whether intentionally or unintentionally, or
  - 4) to which the Contractor has access in connection with the services provided under this Contract.
- B. Such Department Information may include taxpayer, vendor, and other state agency data held by the Department.
- C. As used herein, the terms "Sensitive" and "Confidential" information shall have the meanings set forth in the Department's Information Protection Policies, Standards & Guidelines.
- D. All waiver requests shall be processed in accordance with the Department's Information Protection Policies, Standards & Guidelines Waiver Policy.
- E. The Department reserves the right to audit the Contractor's compliance with the Department's Information Protection Policies, Standards & Guidelines
- F. The Department reserves the right to take appropriate action to protect the Department's network and information including the immediate termination of system access.
- G. The Contractor shall ensure that any confidential Department Information in the custody of the Contractor is properly sanitized or destroyed when the information is no longer required to be retained by the Department or the Contractor in accordance with this Contract.
- H. Electronic media used for storing any confidential Department Information shall be sanitized by clearing, purging or destroying in accordance with NIST Special Publication 800-88 Guidelines for Media Sanitization. The Contractor shall maintain a record documenting the removal and completion of all sanitization procedures with the following information:
- 1) Date and time of sanitization/destruction,
  - 2) Description of the item(s) and serial number(s) if applicable,
  - 3) Inventory number(s), and
  - 4) Procedures and tools used for sanitization/destruction.
- I. No later than sixty (60) days from contract expiration or termination or as otherwise specified in this Contract, the Contractor shall complete the sanitization and destruction of the data and provide to the Department all sanitization documentation.

#### **Disclosure of Security Breach**

Without limitation on any other provision of this Contract regarding information security or security breaches, the Contractor shall provide notice to the Department's Project Manager and the CISO as soon as possible following the Department's discovery or reasonable belief that there has been unauthorized exposure, access, disclosure, compromise, or loss of sensitive or confidential Department information ("Security Incident").

- A. Within twenty-four (24) hours of the discovery or reasonable belief of a Security Incident, the Contractor shall provide a written report to the CISO detailing the circumstances of the incident, which includes at a minimum:
- 1) A description of the nature of the Security Incident;
  - 2) The type of Department information involved;
  - 3) Who may have obtained the Department information;

- 4) What steps the Contractor has taken or shall take to investigate the Security Incident;
  - 5) What steps the Contractor has taken or shall take to mitigate any negative effect of the Security Incident; and
  - 6) A point of contact for additional information.
- B. Each day thereafter until the investigation is complete, the Contractor shall provide the CISO with a written report regarding the status of the investigation and the following additional information as it becomes available:
- 1) Who is known or suspected to have gained unauthorized access to the Department's information;
  - 2) Whether there is any knowledge if the Department information has been abused or compromised;
  - 3) What additional steps the Contractor has taken or shall take to investigate the Security Incident;
  - 4) What steps the Contractor has taken or shall take to mitigate any negative effect of the Security Incident; and
  - 5) What corrective action the Contractor has taken or shall take to prevent future similar unauthorized use or disclosure.
- C. The Contractor shall confer with the CISO regarding the proper course of the investigation and risk mitigation. The Department reserves the right to conduct an independent investigation of any Security Incident, and should the Department choose to do so, the Contractor shall cooperate fully by making resources, personnel, and systems access available to the Department and the Department's authorized representative(s).
- D. Subject to review and approval of the CISO, the Contractor shall, at its own cost, provide notice that satisfies the requirements of applicable law to individuals whose personal, confidential, or privileged data were compromised or likely compromised as a result of the Security Incident. If the Department, in its sole discretion, elects to send its own separate notice, then all costs associated with preparing and providing notice shall be reimbursed to the Department by the Contractor. If the Contractor does not reimburse such costs within thirty (30) calendar days of the Department's written request, the Department shall have the right to collect such costs.

### Cyber Insurance Requirement

The Contractor will maintain sufficient cyber insurance to cover any and all losses, security breaches, privacy breaches, unauthorized distributions, or releases or uses of any data transferred to or accessed by Contractor under or as a result of this Contract.

- A. This insurance shall provide sufficient coverage(s) for the Contractor, the Department, and affected third parties for the review, repair, notification, remediation and other response to such events, including but not limited to, breaches or similar incidents under Chapter 521, Texas Business and Commerce Code.
- B. The Department may, in its sole discretion, confer with the Texas Department of Insurance to review such coverage(s) prior to approving them as acceptable under this Contract.
- C. The Contractor shall obtain modified coverage(s) as reasonably requested by the Department within ten (10) calendar days of the Contractor's receipt of such request from the Department.

### Representations And Warranties Related To Software

If any software is provided under this Contract, the Contractor represents and warrants each of the following:

- A. The Contractor has sufficient right, title, and interest in the Software to grant the license required.
- B. Contract terms and conditions included in any "clickwrap", "browsewrap", "shrinkwrap", or other license agreement that accompanies any Software, including but not limited to Software Updates, Software Patch/Fix, or Software Upgrades, provided under this Contract are void and have no effect unless the Department specifically agrees to each licensure term in this Contract.
- C. The Software provided under this Contract does not infringe upon or constitute a misuse or misappropriation of any patent, trademark, copyright, trade secret or other proprietary right;
- D. Software and any Software Updates, Software Maintenance, Software Patch/Fix, and Software Upgrades provided under this Contract shall not contain viruses, malware, spyware, key logger, back door or other covert communications, or any computer code intentionally designed to disrupt, disable, harm, or otherwise impede in any manner, including aesthetical disruptions or distortions, the operation of the computer program, or any other associated software, firmware, hardware, or computer system, (including local area or wide-area networks), in a manner not intended by its creator(s); and
- E. Software provided under this Contract does not and will not contain any computer code that would disable the Software 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 mechanism (sometimes referred to as "time bombs", "time locks", or

“drop dead” devices) or that would permit the Contractor to access the Software to cause such disablement or impairment (sometimes referred to as “trap door” devices”).

**Rights to Data, Documents and Computer Software (State Ownership)**

- A. Any biographic data, demographic data, image data inclusive of fingerprints, photograph and signatures or any other data or metadata in any form acquired or accessed by the Contractor in the performance of its obligations under this Contract shall be the exclusive property of the State of Texas and all such data shall be delivered to the Department by the Contractor upon completion, termination, or cancellation of this Contract.
- B. The Contractor shall not use, willingly allow, or cause to have such data used for any purpose other than the performance of the Contractor’s obligations under this Contract without the prior written consent of the Department.
- C. The ownership rights described herein shall include, but not be limited to, the right to copy, publish, display, transfer, prepare derivative works, or otherwise use the works.
- d. The Contractor shall provide, at no additional charge, appropriate licenses for the Department to use and access, as necessary for the Department to use and access the turnkey solution during the term of the lease, the Contractor’s pre-existing software or other intellectual or proprietary property that the Contractor determines is necessary to facilitate the performance of the Contractor’s obligations under this Contract.

**APPENDIX B**  
**SYSTEM ARCHITECTURE AND IT REQUIREMENTS**

**PRICING REQUEST (PR)**  
**ISSUED BY TXDPS**  
**TO DIR DBITS VENDORS**

**INFORMATION TECHNOLOGY (IT) REQUIREMENTS**

The Contractor shall comply with the following standards and requirements wherever they are applicable to this Contract. The Department shall have the sole right to waive specific requirements if in its sole judgment doing so would mitigate costs or risks or significantly improve the installed and configured solution.

**Environment Standards**

The COTS Software shall be hosted within Contractor's computing infrastructure or within the Departments' IT infrastructure. The Contractor shall provide a complete hardware and software inventory including any servers required, an architectural diagram, security diagram, network diagram, network usage assessment, and communications port diagram of the complete overall system and narrative describing requested diagrams and any API and Web service components, and the recommended workstation configuration if any. The Contractor shall also itemize all assumed capabilities and minimum hardware and software requirements of any Department IT related systems required to access or support contractor's product or system. The Respondent must provide copies of the 508 compliance VPAT documentation for all components of the proposed system.

A. Contractor Hosted COTS Software:

1. Any applicable server hardware shall identify:
  - a. The processor requirements;
  - b. The memory requirements;
  - c. Operating system details and dependencies; and
  - d. Data storage requirements.
2. All workstation recommendations shall identify:
  - a. The processor requirements;
  - b. Display requirements;
  - c. The memory requirements;
  - d. Operating system details and dependencies;
  - e. Data storage requirements; and
  - f. Any support applications required such as Internet Explorer, Adobe PDF Reader etc.
3. Peripherals required:
  - a. Printers;
  - b. Scanners; and
  - c. Fax.

- B. The Respondents system must support the following
- a. DPS issued desktop or laptop PCs:
    - i. Windows 7
    - ii. Internet Explorer 8 or greater
    - iii. Firefox 27 or greater
  - b. DPS issued Mobile Devices
    - i. IOS version 7 or greater
    - ii. iPhone 4s or greater
    - iii. iPad 3 or greater
  - c. Publicly owned desktop or laptops PCs
    - i. Windows 7 or greater
    - ii. Mac OS X 10.6.8 or greater

- iii. Internet Explorer 8 or greater
- iv. Safari 10.6.4 or greater
- v. Firefox 27 or greater
- d. Publicly owned mobile devices, phones and tablets
  - i. Using IOS 7 or greater
  - ii. Using Android 4.1 or greater

C. The Department Hosted COTS Software:

The Contractor shall follow the Department's hosting standards for any software and hardware that is hosted within the Department Data Centers. The Contractor hosted software and hardware are not required to meet these requirements. However, the Contractor hosted software and hardware shall meet these standards prior to migrating from the Contractor hosted to the Department hosted.

The existing Department infrastructure framework supports several industry standard products and platforms. The Contractor shall identify the products required to properly support the contracted solution.

1. The Contractor shall identify:
  - a. Required hardware platforms and operating system to support the proposed solution:
    - i. The processor requirements;
    - ii. The memory requirements;
    - iii. Operating system details and dependencies; and
    - iv. Data storage requirements.
  - b. Required application server platforms:
    - i. The processor requirements;
    - ii. The memory requirements;
    - iii. Operating system details and dependencies; and
    - iv. Data storage requirements.
  - c. Required web server platforms:
    - v. The processor requirements;
    - vi. The memory requirements;
    - vii. Operating system details and dependencies; and
    - viii. Data storage requirements.
  - d. Any required support services such as email servers etc.:
    - ix. The processor requirements;
    - x. The memory requirements;
    - xi. Operating system details and dependencies; and
    - xii. Data storage requirements.
2. The Department's IT infrastructure only allows the following database platforms:
  - a. Contractor SQL Server 2012
  - b. DB2 9.7.2 on Distributed (AIX and LINUX)
  - c. Oracle on a case by case basis
3. The Department's IT infrastructure report services are supported with Crystal Reports.

### Communication Standards

The COTS Software shall support integration with other Department systems utilizing standard web services or provide API tools that can be incorporated into the Department's applications or secure file transfer protocol with data encryption.

### Network Topography

- A. The Department utilizes a combination of public and private TCP/IP network resources. All internal communications between client resources, other systems, and system services shall be through this network.
- B. The Respondent shall include in its Offer an estimate on the amount of bandwidth or formulas to calculate usage required to support the number of expected internal DPS Users and volume of work. The Offer must also provide information on how they will provide adequate network capacity for DPS Users and External Users.
- C. The Respondents system use standard TCP/IP network access ports. The system must be accessible on Port 80 for standard Web Browser access and Port 443 for Secure Web Browser support.

#### **Workstation installed software**

If the software solution is client based and needs to be installed on each computer, the Contractor shall provide the client software in a MSI format so that the install can be packaged to operate as a silent install for Windows based systems. OS X applications must support Apple Application installation package standards. Any software required for mobile devices must be available from the appropriate App store based on the device operating system. Mobile device software must also be compatible with Mobile Device Management software distribution tools.

### **MAINTENANCE AND SUPPORT**

#### **Contractor Hosted COTS Software Services**

The Contractor shall provide COTS Software that includes and may not be limited to all hardware and software maintenance and support, upgrades to equipment to meet and maintain performance service levels, backup hardware and Internet connections in accordance within Section C.11.1, Cloud Security.

#### **Department Hosted COTS Software**

The Contractor shall provide a software maintenance solution to include, but may not be limited to provide:

- A. Support for the COTS Software to include software changes that the Contractor develops for the Department under this Contract shall be managed through the Service Level Agreement.
- B. Preventative scheduled and unscheduled system diagnosis and correction of faults as well as modification of the software to maintain the service level performance of the COTS Software.
- C. Web-based support portal for the Department to report minor problems shall be available twenty-four (24) hours per day, seven (7) days per week, and three-hundred-sixty-five (365) days a year with a searchable knowledge base for known issues. Response to reported problems shall be managed as defined in the Service Level Agreement.
- D. Maintenance services to resolve usability problems to include but may not be limited to bugs, security issues, and installation of software updates and major software releases.
- E. New software versions or releases at no additional cost to the Department occurring in the normal maintenance yearly support as Offered in Section B.2, Pricing Schedules.

#### **Software Updates**

The Contractor shall provide periodic system software updates that shall incorporate corrections of any defects, and enhancements to the system's software.

- A. COTS Software updates released by the Contractor shall be installed by the Contractor during periods during the maintenance window mutually agreed upon by the Department and the Contractor as defined in the Service Level Agreements.
- B. Updates to Documentation or manuals resulting from system software updates shall be provided or made available on demand to the Department.

#### **Hardware**

- A. The Contractor shall provide maintenance services for hardware equipment owned by the Contractor installed to support a Contractor's Hosted COTS Software.

- B. The Contractor shall provide notice to the Department a minimum of five (5) business days prior to scheduled maintenance including length of anticipated downtime plus the description or purpose of scheduled maintenance. The Contractor shall provide notice to The Department and employees prior to unscheduled maintenance where possible including length of anticipated downtime plus the description or purpose of unscheduled maintenance.

1. Preventive Maintenance

The Contractor shall provide preventive maintenance services in order to maintain the system in good condition and working order on a mutually agreeable scheduled basis. The preventive maintenance schedule is to be based on the Contractor's and the Departments' mutual agreement of the particular service required for each system component, it being understood that this schedule shall be oriented to avoid periods when the system is expected to have the heaviest use.

During the term of this Contract, the Department may, by providing five (5) calendar days prior written notice, select any alternative period of maintenance coverage whether or not such alternative represents an increase or decrease in service.

2. Remedial Maintenance

The Contractor shall provide remedial maintenance to the system on a twenty-four (24) hour per day, seven (7) day per week basis, with a response time of no more than one (1) hour for each incident.

## SERVICE OUTAGE ESCALATION AND COMMUNICATION

The Contractor shall provide a detailed communication plan that specifies how the Contractor shall be contacted in the event of a system outage. If the solution is hosted by the Contractor, the Contractor shall provide its notification and escalation process as part of the communication plan.

## SERVICE LEVEL STANDARDS

The purpose of these Service Level Standards is to ensure that the proper elements are in place to provide the Department employees with the optimal level of system performance. The Service Level Standards define the terms, conditions, requirements, responsibilities, and obligations of the Department, employees, and the Contractor.

### System Production Control

The Contractor shall schedule production management such as batch processing, job scheduling, automated import/exports, etc. at a minimum of once every twenty-four (24) hours, seven (7) days per week and three hundred sixty-five (365) days per year. The production control schedule shall be mutually agreed upon by both the Contractor and the Department and shall be oriented around periods when the system is expected to have the lightest use.

### System Support

The Contractor shall support all software licensed to the Department for use during the term of this Contract. The Contractor shall provide toll-free telephone, or e-mail accessibility to the Department for the system, Monday through Friday, 8:00 a.m. to 6:00 p.m., Central Time, excluding State or federal holidays. A list of the Departments holiday schedule is available upon request. These days and times may change at the discretion of the Department. The Contractor shall provide the capability for the Department and employees to leave a message for occasions outside of that time period.

A. System support for the Department and employees includes responsibilities such as:

1. New Department or employee training;
2. System configuration;
3. Record contribution methodologies or practices;
4. System navigation;
5. Data query or export procedures;
6. Search criteria, best practices, parameters, etc.; and
7. Troubleshooting for system hardware, system software, network, etc.

B. System support for the Department and employee excludes responsibilities such as:

1. Record content;

2. Record quality;
3. Record interpretation;
4. Employee administration (including new accounts, password creation or resets);
5. Non-system software owned, purchased, installed, developed or utilized by the Department or the Department's hardware; and
6. The Departments/User's ISP or other internal method of access.

## System Performance

### Basic Requirements

#### A. Basic Requirements

In addition to the office hours uptime requirements, as defined in Section C.16.2.3, System Rate Calculation, the Contractor agrees to maintain optimal system performance twenty-four (24) hours per day, seven (7) days per week, three hundred sixty-five (365) days per year at a rate of 99.5% (hereafter referred to as the "Rate") as calculated by Rate Calculation below. The Contractor is cautioned to quickly resolve the source or sources of failure. Inability to meet or exceed the Rate in any twelve (12) month period may at the Department's sole discretion result in the following actions:

1. First Remedy: Verbal warning.
2. Second Remedy: Written warning added to the Contract File Folder as stated in accordance with Section H.3, Further Opportunity to Cure, of this Contract.
3. Continuing Remedy: The Department may consider exercising the Contract remedies, which may include termination as stated in accordance with Section H.4, Termination, of this Contract.

### Rate of Calculation

#### B. Rate Calculation

The Contractor shall measure the rate of system performance by the amount of downtime during a calendar month. This metric gauges the system performance as a percentage of available hours tracked to the quarter of an hour (rounded). The rate of system performance shall be measured and monitored as follows:

Available hours equal total number of hours in a month (24 hours x number of days in the month) minus the actual amount of time spent to the quarter of an hour for scheduled maintenance for the hosted application.

Downtime is the total number of hours (rounded to the quarter hour) during which the solution is not in operation.

System Performance Rate equals available hours Downtime divided by available hours.

**Example** for the month of January:

Available time per month was 744 hours (31 days X 24 hours)

Downtime per month was 3.75 hours (start 1:00 am - end 4:40 am)

$744.00 - 3.75 = 740.25$

$740.25 \div 744 = 99.5\%$

### Reports

For Vendor hosted solutions, the Vendor shall report both system performance Rate and average Response Time of the system by 5:00 pm CST Monday following the last business day of the month throughout the life of an active Change Order. Reports may be made available through the system or distributed to the Department's Contract Monitor.

### Data Backups

The Vendor or system shall perform backups on all system Records once every twenty-four (24) hours, seven (7) days per week, and three hundred sixty-five (365) days per year to facilitate data and system restoration in the event of any failures, including but not limited to, hardware. The data backup schedule shall be mutually agreed upon by both the Vendor and the Department and shall be oriented around periods when the system is expected to have the lightest use.

### Contact Persons

The Vendor's point of contact for maintenance and service levels shall be the Division and ITD Project Managers. The Departments' primary point of contact shall be the Departments' Contract Administrator in accordance with this Contract in Section {X}, Contract Administrator.

- A. The vendor will comply with the Disaster Recovery Plan.

**Hardware and Software Refresh**

The Vendor shall provide hardware and software refresh plans to address end of support or end of life products. The plan shall also address system and application patches and implementation methodology and schedule. Refresh of hardware and software will be at the sole discretion of the Department.

**ADA Compliance**

The Respondent represents and warrants that it will comply with the requirements of the Americans with Disabilities Act (ADA).

**TESTING REQUIREMENTS, IMPLEMENTATION AND ACCEPTANCE**

All testing activities shall include the following but not be limited to:

**Implementation and Acceptance**

TXDPS will work closely with the Respondent to insure each phase of this project is complete; however, completion of any one phase specified in this RFO does not constitute full completion and acceptance of the project's requirements.

**Unit Testing:**

- A. Respondent shall provide a listing of test cases based on the requirements of this solicitation, the Implementation Plan, Project Plan and Schedule and in direct coordination with TXDPS Project Manager.
- B. Respondent shall also provide TXDPS with the results of the Unit test cases that were executed to completion.
- C. Based on the outcome of successful unit testing, Respondent shall advance to the next step of System Testing. Successful unit testing shall be defined as 100% pass rate of all defined unit test cases with no outstanding issues/defects. Respondent shall perform all these tests in a development environment.

**System Testing:**

- A. Respondent shall provide to TXDPS for review and approval by TXDPS QA testing staff, documented test cases that shall be performed during Respondent system testing to validate the successful migration and installation of the software package before any System Testing begins.
- B. Respondent shall be responsible for performing system testing in the Respondent QA Environment and provide test results to TXDPS.
- C. Respondent shall log all defects found during the System Testing in the agreed upon defect tracking application.
- D. Respondent shall investigate any defects found during System Testing and participate in Defect Triage meetings with TXDPS to determine defect outcome and resolution.
- E. Respondent shall provide defect fixes in the timeframe as defined in SLA.
- F. Respondent shall demonstrate all components of the Application Software are performing as defined in the System Test cases and Business Requirements, including interfaces with other systems (Baseline Interfaces), in the specified System Hardware, Operating Software and Network Environment (System Environment).

**Performance/Load Testing:**

Performance/Load Testing will be performed by TXDPS in coordination with the Respondent in instances where internal metrics (network load, etc.) cannot be captured by the Respondent. TXDPS will also help coordinate internal resources to provide oversight and assistance when necessary.

- A. Respondent shall provide documented test cases to TXDPS that shall be performed during Respondent performance and load testing to validate the successful performance of the software package.
- B. Respondent shall capture the average data throughput for solution and the maximum number of concurrent users before service degradation to ensure user traffic does not have an adverse effect the TXDPS network and provide these results to TXDPS.
- C. Respondent shall be responsible for conducting performance and load testing that will demonstrate their system is capable of meeting metrics as defined by TXDPS.

- D. Respondent shall provide performance and load test results to TXDPS for review and approval.
- E. Based on the outcome of successful performance and load testing, Respondent shall advance to the next step of System Integration Testing. Successful performance testing shall be defined as 100% pass rate of all defined test cases with no outstanding issues/defects. Respondent shall perform all these tests in a production-like environment.

**Integration Testing:**

TXDPS shall perform System Integration Testing independently or jointly with the Respondent, following successful completion and documentation of Respondent and TXDPS System Testing. Successful completion is defined as 100% pass rate of all defined System Test cases with no outstanding issues/defects.

- A. Respondent shall provide assistance during the System Integration Testing process by providing technical and QA resources that will answer questions and provide clarifications and/or fixes to any issues encountered during the System Integration Testing cycle. This support can be performed remotely or in person at the TXDPS facility. Remote support shall consist of, but is not limited to, remote server control mechanisms, WebEx review sessions, telephone conference calls and email exchanges. System Integration Testing will focus on the integration and interaction with other TXDPS systems, external systems, or third party components and shall be based on the TXDPS requirements as well as the Respondent System Design Specification.
- B. The vendor must provide a User Acceptance Testing environment upon successful completion of System Integration Testing.
- C. TXDPS shall log all defects found during the System Integration Testing in the agreed upon defect tracking application.
- D. Respondent shall investigate any defects and participate in Defect Triage meetings with TXDPS to determine defect outcome and resolution.
- E. Respondent shall provide a documented response to the documented defect in the agreed upon defect tracking application.
- F. Respondent shall provide defect fixes in the timeframe as defined in SLA.
- G. Respondent shall provide Release Notes containing an open issues log for each test iteration.
- H. At TXDPS' sole discretion, test cases may be modified or added to ensure completeness, accuracy and quality of the delivered software package as defined in business and technical documentation.
- I. Based on the successful outcome of System Integration Testing, TXDPS shall advance to User Acceptance Testing (UAT). Successful System Integration Testing shall be defined in the Test Plan documentation created by TXDPS.
- J. System Integration testing shall not be considered successful if outstanding Severity one (1) or Severity two (2) defects pending resolution remain.

**User Acceptance Testing (UAT):**

- A. Following successful completion of the System Integration Testing, or System Test for Contractor Hosted systems, TXDPS shall coordinate and execute UAT in the Contractor's (UAT) environment.
- B. UAT shall be performed by TXDPS end users based on UAT test cases created by TXDPS.
- C. TXDPS shall notify Respondent of any defects found during User Acceptance Testing of the Software Solution.
- D. Respondent shall investigate any defects and participate in Defect Triage meetings with TXDPS to determine defect outcome and resolution.
- E. Respondent shall provide defect fixes in the timeframe as defined in the SLA.
- F. If the number of defect failures prevents all systems from operating as described above, the TXDPS may reject the entire final software package.
- G. If all criteria is not met as defined in the TXDPS Quality Assurance Entry and Exit Criteria document (Exhibit ##), or the respondent's solution does not meet the defined business requirements, the TXDPS may reject the final software solution.

**Final Acceptance:**

Final acceptance of the Software Solution shall not occur until ninety (90) business days after the review period, to include thirty (30) days failure free operation of the system and delivery of all required documentation.

**Failure Resolution:**

Upon failure of any test within the control of the Respondent shall submit a report describing the nature of the failure and the actions to be taken to remedy the situation prior to any modification or replacement of the system, within ten (10) business days. TXDPS shall provide written approval or denial within five (5) business days. If a system requires modification, the fault shall be corrected and the test repeated until successfully completed.

- A. Major discrepancies that will substantially delay receipt and acceptance of the system shall be sufficient cause for rejection of the system. Failure to satisfy the requirements of any test is considered a defect and the system shall be subject to rejection by TXDPS. Any rejected software package may be offered again for retest provided all noncompliance has been corrected.
- B. Resolution of System Integration Test Failure. If the software package fails the System Integration Test, Respondent shall correct the fault and then TXDPS will repeat the Systems Integration Test until successfully completed.
- C. Resolution of Final Acceptance Test Failure. If a defect within the system is detected during the Final Acceptance Test, TXDPS shall document the failure. Respondent will be required to research, document and correct the source of failure. Once corrective measures are taken, TXDPS shall monitor the point of failure until a consecutive thirty (30) calendar day period free of defects is achieved.

**Retest**

Respondent and TXDPS shall mutually agree to re-test per C.17 Testing Requirements, Implementation, and Acceptance, as determined by the environment where the issue is to be addressed. If the system downtime exceeds seventy-two (72) hours or system has not operated for thirty (30) consecutive days free of defects within the ninety (90) day period, TXDPS may extend the test period by an amount of time equal to the greater of the downtime in excess of seventy-two (72) hours or the number of days required to complete the performance requirement of an individual point of failure.

**DEPARTMENT RECORDS AND DATA RETENTION**

- A. Upon conclusion of this Contract, including management transition to the Department or another Contractor, all agency data and reports and the complete, certified set of fully, properly documented, and commented application programming files and logs developed by the Contractor specifically for this Contract shall revert to the Department. This shall include customized code, data and images, data and images indices, data and image indexing or analysis, and logging tools and information not present in Contractor's product as normally initially delivered to other clients.
- B. Agency records shall be labeled and delivered in a manner satisfactory to the Department. The Contractor shall comply with additional instructions pertaining to Department records as detailed in Section H.55, Books and Records, of this Contract.
- C. In the event the Contractor requires copies of any records after conclusion of this Contract or this Contract's expiration and Facility management transition, the Department shall furnish copies to the Contractor at the Contractor's expense.
- D. Records shall be maintained in accordance with the Department's Records Retention Schedule as detailed in Section E.2, Inspection by State Employees.

**Attachment C**

**STATEMENT OF WORK**

**FOR**

**A Pricing Request (PR)**

**TITLE**

**TXDPS Texas Gang Intelligence Index (TX Gang)**

**TECHNOLOGY CATEGORIES**

***Deliverables Based Information Technology Services (DBITS)***

*Application Development*

*Technology Upgrade/Migration and Transformation*

*Application Maintenance and Support*

**DIR Vendor Name**

---

**DIR Vendor Contract Numbers (list all applicable DIR Master Contract Numbers)**

**DIR-SDD-\_\_\_\_\_**

**Date Issued: 6/09/15**

**Response must be received on or before 6/30/2015 by 1:00 P.M.**

## **1. Introduction**

TXDPS issues this Statement of Work (SOW) under this PR number 405-15-R012836 for services under the Department of Information (DIR) Deliverables Based Information Technology (DBITS) Master Contracts for a TXDPS Crime Records Service (CRS) application.

Chapter 61 of the Texas Code of Criminal Procedure mandates that the TXDPS create and maintain a statewide gang intelligence database operated in accordance with Title 28 of the Code of Federal Regulations Chapter 23. This database is provided at no cost to law enforcement and criminal justice agencies throughout Texas for the purposes of maintaining a central gang intelligence source. Any law enforcement agency collecting gang intelligence in Texas, any sheriff's office in a county with a population of greater than 100,000, and any police department jurisdiction with a population of more than 50,000 are required to submit gang data to the TXDPS-provided gang database. The database was officially created in 1999 as the Texas Gang Intelligence Index ("TX Gang" or "the System"), and has been through three major iterations in that time, each of which has had an increase in participation and scope. TX Gang has become, and is continuing to grow as, a major resource in both the Texas and national gang intelligence communities. Currently, the Crime Records Service (CRS) of the Law Enforcement Support (LES) division oversees and maintains the database.

TX Gang serves as an effective investigative, analytical, and statistical criminal investigative resource by providing the tools necessary to identify, relate, and track gangs, gang members, and their activities and by allowing for the sharing of data across multiple local, state, and national jurisdictions. The primary objectives of TX Gang are receipt, storage, and sharing of essential criminal investigative information related to gangs and gang members. It is the intent of TXDPS to issue a Purchase Order (PO) for maintenance and support tasks, and accompanying Change Orders for application development needs as identified.

## **2. Scope - Technical Environment and Identified Application Enhancement Projects**

- A. The Vendor shall provide continuous maintenance services for the TXDPS' TX Gang related software utilized by the TXDPS for the System to include, but not be limited to, preventive and remedial maintenance and enhancement services for upgrades, refreshes, enhancements, customization, test and acceptance, and other related services.
- B. The Vendor's services for the System shall be an open solution to allow for customization and enhancements to meet all CJIS security requirements.
- C. Enhancement services: The TXDPS will assign and then issue Change Order Plan(s) as incorporated in Exhibit 1, Change Order Template, for additional services to include but not be limited to customization, enhancements, and other related services. The Contract Monitor shall work with the Vendor to prepare the COP(s). The Contract Monitor shall submit a requisition to Procurement and Contract Services to finalize the modification to this Contract.

Examples of factors requiring application enhancement include but are not limited to:

- Open Records Requests
- Mandated Legislative Changes

405-15-R025523  
Attachment C - SOW  
**TXDPS Texas Gang Intelligence Index (TX Gang)  
Application Development, Maintenance & Support,  
Technology Upgrade/Migration and Transformation**

- FBI Program Specific Changes through its Technical Operational Update documents
- FBI Audit
- TXDPS Audit
- TXDPS Administrative Mandates
- TXDPS Internal Data Aggregation Mandates (Web Services)
- TXDPS IT and Infrastructure Design Mandates
- TXDPS CRS Tertiary Programs (Texas Crime Information Center / National Crime Information Center /Texas Law Enforcement Telecommunications System)
- Oversight board requirements

The Vendor shall provide continual application development and support services through enhancements and software updates plus support services contracted through its DIR Master Contract. Support services shall include:

- System analysis
- Scope assessment
- Specification development
- Programming
- Web based services
- Data import and export processes
- Interfaces
- System Infrastructure
- Report generation
- Testing and quality assurance
- Implementation
- Documentation of new features and functionality
- Technical support
- Database design
- Support code framework ensuring the system meets all compliance requirements with Title 1 Texas Administrative Code chapters 206 and 213
- 24x7x365 maintenance of the System
- Maintenance and patching of software
- Preventative and routine maintenance to include but not be limited to patching of servers and other relevant commercial software such as Microsoft SQL Server

## **2.1 Technical Environment**

**2.1.1 Software Environment:** Operating System(s): Red Hat Enterprise Linux Server release 5.4;  
Application Server: Tomcat 7.0.23

**2.1.2 Hardware:** Cisco UCS Server (production); Cisco UCS Server (development/test)

**2.1.3 Database Environment:** DB2 v9.7.0.2 and any subsequent releases

**2.1.4 Programming Languages:** Java 1.6.0\_2; stored procedures (see database environment); JavaScript; Tapestry 5.1

**2.1.5 User accessibility:** will be on a 24x7x365 basis, with at least 99.5% availability via approved platforms. Web based access will be available regardless of user platform, but at a minimum will support all common browser configurations.

**2.1.6 Data throughput:** Data transmitted from TX Gang will meet NIEM 2.1 standards with an anticipated upgrade to 3.0 within twelve (12) calendar months of its release. Future iterations of the NIEM standard will also be supported.

## **2.2. Application Development and / or Enhancement Change Orders**

Application development or technology upgrade/migration and transformation tasks will be governed by issuing task specific Change Orders (Exhibit 1). Each Change Order will be negotiated and agreed to by both parties. Change Orders will be officiated by signatures of the Vendor, the TXDPS Division's Contract Monitor (CM) or assigned designee, requesting the work, and the TXDPS Procurement & Contract Services (P&CS) Contract Administrator, and will be incorporated into this Contract. The TXDPS CM or assigned designee will initiate this process by providing the Vendor with a draft Change Order for update and negotiations. Once the TXDPS CM or assigned designee and the Vendor have determined and agreed to all deliverables and updated the draft Change Order accordingly, the draft Change Order will be forwarded to the TXDPS Contract Administrator for scope and pricing verification. Once all identified groups concur, the TXDPS Contract Administrator will facilitate final signatures to incorporate the Change Order into this Contract. No work is authorized without an approved and executed Change Order as provided to the Vendor by the TXDPS Contract Administrator.

### **2.2.1 Change Order Format and Methodology**

The format of the Change Order will not be altered by either the TXDPS Division CM or assigned designee or the Vendor. The TXDPS Division CM or assigned designee and the Vendor shall only update applicable deliverable language, provide pertinent project information and background necessary to explain the project tasks and scope, and update all Change Order tables as the project progresses.

Change Orders will be issued for any and all application customizations, updates, and/or modifications, to include but not be limited to: alterations of software, programming, documentation, and other applications or services beyond those originally stated within this SOW for standard maintenance and hosting requirements as detailed within this Contract.

## **3. Maintenance and Support Requirements**

The Vendor shall provide maintenance and support for the TX Gang application will need to meet the following criteria. Please refer to Section 7 of this SOW for service level requirements.

### **3.1 Application Hosting Requirements for Vendor Hosted Applications**

The Vendor shall comply with all Terms and Conditions of this Contract and shall:

405-15-R025523  
Attachment C - SOW  
TXDPS Texas Gang Intelligence Index (TX Gang)  
Application Development, Maintenance & Support,  
Technology Upgrade/Migration and Transformation

- Provide each application with a separate test and redundant production environment to mitigate application downtime.
- Allow an unlimited number of unique remote Administrator Access Users for the production and test environments for each application.
- Provide TXDPS Administrator Access Users capabilities to maximize administration of each application, including but not limited to the creation, modification, and removal of users, groups, and roles and permissions management.
- Coordinate and obtain written approval from the TXDPS' Project Manager for requirements necessary to providing and maintain the Administrator roles-based accounts. The Vendor shall ensure accounts meet TXDPS standards.
- Provide web based access to all applications by users and Administrator Access Users.
- Provide web-based access independent of user platform, but at a minimum, support Internet Explorer 8, other common web browsers, and common mobile devices to include, but not be limited to, iPhone, iPad, Android, and IOS devices.
- Ensure user access to applications support web based protocols and not require a fat client for system administration and / or user operations.
- Provide data archiving to comply with statutory requirements as defined in the State Library requirements and the TXDPS Records Retention schedule.
- Provide full and indelible audit logs as requested by TXDPS for all operations performed within each application to include, but not be limited to, compliance with the most up to date version of the CJIS Security Policy, including auditing, accountability, access control, identification and authentication. Reference Section 12.1 of this SOW for CJIS details and Section 13 of this SOW for documentation required with the PR response.
- Include data security features within each application that protect the security and privacy of personally identifiable information (PII) and which comply with the storage and dissemination of reports involving juveniles, victims, suspects, and sex-offenders as required by statute.
- Ensure, and provide documentation within its PR response, that all applications comply with the current Cloud Security Alliance's (CSA) Cloud Control Matrix (CCM) security requirements for Vendor hosted applications. Information pertaining to CSA <https://cloudsecurityalliance.org/> and CCM information may be found at <https://cloudsecurityalliance.org/research/ccm/>.
- Provide an updated hardware (HW) and software (SW) inventory as changes are made, including any servers and network technology required and, as requested by TXDPS, an architectural diagram of the complete overall system, to demonstrate compliance with CSA CCM, and provide specific detail related to:
  - a. the processor requirements;
  - b. the memory requirements;
  - c. operating system details and dependencies; and
  - d. data storage requirements.

### 3.2 Data Backups

The Vendor shall perform backups of all applications daily, for the term of this Contract.

- 3.2.1** The data backups will be performed at a mutually agreed upon time outside the hours of 8:00 A.M. to 5:00 P.M. CT. Exceptions to this schedule require prior written consent from the TXDPS CM. The TXDPS CM will have one (1) business day to respond to exception requests.

- 3.2.2 Automatic notification of backup failures will be sent to the application TXDPS' Project Manager.
- 3.2.3 The Vendor shall perform backups on all applications and application data once every twenty-four (24) hours, seven (7) days per week, and three hundred sixty-five (365) days per year to facilitate data and system restoration in the event of any failures, including but not limited to hardware or network.
- 3.2.4 The daily data backup general operation start time shall be mutually agreed to by both the Vendor and TXDPS and will be oriented around periods when the system is expected to have the lightest use. The Vendor shall ensure no more than twenty-four (24) hours of data are at risk.
- 3.2.5 The Vendor shall ensure data and application backups allow for the complete recovery of data and application functionality up to the point of failure.
- 3.2.6 Data backup failures will be reported via email to the TXDPS' Project Manager within one (1) hour of failure.
- 3.2.7 Data backup failures will be reported on the monthly incident report.

### 3.3 **Hosting Center Disaster Recovery and Disaster Recovery Plan**

The Vendor shall author and design a Disaster Recovery Plan (DRP) for each hosted application.

- 3.3.1 The Vendor shall update the DRP for any enhancement.
- 3.3.2 DRP will be approved by the TXDPS IT Division, TXDPS Cyber Security, the TXDPS Division requesting the enhancement, and the TXDPS Procurement and Contract Services (P&CS) Contract Administrator. Final acceptance of the DRP will be communicated from the Contract Administrator to the Vendor via email.
- 3.3.3 The Disaster Recovery (DR) solution will reside at a secondary location.
- 3.3.4 The DRP will be reviewed and updated every six (6) months to ensure the plan reflects current priorities, processes, and execution strategies.
- 3.3.5 The Vendor shall provide its proposed DRP to the TXDPS Contract Administrator within fifteen (15) calendar days of Contract award. 3.3.6 The Vendor and TXDPS shall negotiate and agree on the initial DRP within thirty (30) calendar days of awarded of this Contract.
- 3.3.7 The Vendor and TXDPS shall negotiate and agree on the updated DRPs within ten (10) business days of submission.
- 3.3.8 **The Recovery Time Objective (RTO) is seven (7) days. The Recovery Point Objective (RPO) is less than 30 minutes. The RTO is the targeted duration of time and a service level within which a business process must be restored after a disaster (or disruption) in order to avoid unacceptable consequences associated with a break in business continuity. An RPO is defined by business continuity planning. It is the maximum targeted period in which data might be lost from an IT service due to a major incident.**

### 3.4 **Transition Plan/Procedures**

The Vendor, with the assistance of TXDPS, as part of the application maintenance and support requirements, shall provide a detailed plan for transitioning all applications, data, software, and documentation ("Application Data"), in whole or part, to a subsequent Vendor, TXDPS or other entity. The Vendor shall update the

405-15-R025523  
Attachment C - SOW  
**TXDPS Texas Gang Intelligence Index (TX Gang)  
Application Development, Maintenance & Support,  
Technology Upgrade/Migration and Transformation**

Transition Plan within fifteen (15) calendar days following any enhancement work that alters application or system design.

The Vendor shall provide, within its Offer, a detailed draft transition plan (“Transition Plan”) for a ninety (90) calendar day transition period that meets industry and best practices standards and will include, at a minimum, step by step processes, timelines, involved parties’ responsibilities, knowledge transfer, training and functional requirements to ensure that transition of all Application Data includes without limitation:

- Detail of all hardware (if applicable) and associated operating software requirements necessary to support all applications.
- Detail of all platform and development software necessary to support, maintain and administer all application test, application production, and application monitoring environments.
- Detail of all network hardware (if applicable) and software necessary to support, maintain and monitor all application test, application production, and application monitoring environments.
- Detail to ensure all Application Data can integrate with other TXDPS or other identified entities’ systems utilizing standard web services, or provide application program interface (API) tools that can be incorporated into TXDPS or other identified entities’ applications or secure file transfer protocol with data encryption.

The Vendor shall provide to TXDPS a finalized Transition Plan within thirty (30) calendar days of Contract award. TXDPS shall review the Transition Plan within fifteen (15) calendar days of submission, and shall discuss any issues, requirements or concerns with the Vendor.

As directed by TXDPS as a result of such discussions, the Vendor shall modify the Transition Plan and return the Plan to TXDPS for review and written acceptance within fifteen (15) calendar days of receipt. The fifteen (15) business day cycle, at a maximum, shall continue between TXDPS and the Vendor until it is determined the Transition Plan achieves TXDPS’ satisfaction. Upon determining that the Transition Plan meets the requirements of this Contract including these provisions, TXDPS shall notify the Vendor of its written acceptance of the Transition Plan and upon such written acceptance, the Transition Plan shall be incorporated by reference into this Contract. Notice to the Vendor will be provided by the Contract Administrator via email.

TXDPS shall ensure cooperation on the part of any subsequent Vendor, other entity or TXDPS personnel, depending on the entity to which TXDPS directs that all or part of this Contract shall be transitioned; however, the Vendor shall maintain all responsibility for all tasks, deliverables and performances under this Contract during the transition period. At the end of the ninety (90) day transition period, or earlier depending on TXDPS approvals, the subsequent Vendor, other entity or TXDPS shall assume full responsibility for all tasks, deliverables and performances as directed by TXDPS.

During this Contract term, additional revisions of the Transition Plan may be required due to information, processes or issues that originally were not included or addressed in the Transition Plan. Revisions to the Transition Plan shall be processed under the same procedures as the initial Transition Plan, including provision to TXDPS for review, comment, revision, written acceptance, and incorporation into this Contract. Any enhancement activities that alter application or system design shall necessitate an update to the Transition Plan.

Knowledge transfer shall occur over the entirety of the 90-day transition period. The knowledge transfer shall take place via various methods. The Vendor shall, at a minimum, coordinate and conduct two (2) formal classroom training sessions. These sessions shall focus on the specific Transition Plan requirements and any other tasks or activities identified by the Vendor and TXDPS as needed to ensure a successful transition of

technology necessary to continue applications operations. Training sessions shall be completed no later than sixty (60) calendar days prior to the end of the transition period. The Vendor, TXDPS and the subsequent Vendor or other entity shall meet a minimum of once per week to determine if further training or knowledge transfer is required.

TXDPS shall meet with the Vendor and the subsequent Vendor or other entity to ensure all concerns and issues have been met and addressed appropriately. TXDPS shall make the determination, in its discretion, of when the transition is complete and shall provide the Vendor and the subsequent Vendor or other entity with formal written acceptance indicating such transfer of responsibilities. The formal transfer of duties shall be documented, in writing, on a TXDPS Contract Modification or Contract Amendment, to include acceptance signatures from TXDPS, the Vendor and the subsequent Vendor or other entity.

Activation of the Transition Plan approved by TXDPS under these provisions (the beginning of the ninety (90) day transition period), will begin on the Vendor's receipt of written notification from TXDPS that this Contract, in whole or in part, is being transitioned. The Vendor shall comply with these provisions and the Transition Plan. The Vendor's failure to comply with these provisions and the Transition Plan shall constitute a material breach of this Contract.

### **3.5 Software Maintenance and Support for TXDPS Owned/Hosted Applications**

The Vendor shall provide all SW maintenance and support, to meet and maintain performance service levels. Maintenance of TX Gang will include Preventative Maintenance, Remedial Maintenance and Special Maintenance as defined herein: The Vendor shall provide the following:

Maintenance, support, or implementation for existing interfaces or TXDPS required future interfaces.

Maintenance and support for all existing database features.

Provide users with a method of contacting one another within the database.

Visibility of documenting officer, entering user, and user that performs the most recent validation of the record to TX Gang users

The means to notify users of fundamental database transactions, including but not limited to additions, modifications, deletions, expirations, views, subscriptions, or other similar data changes.

Relational ties within the database for comparison of similar records.

Provide and support methods for all types of reports current to the system as well as future reports requested by the TXDPS.

Maintain up to date knowledge of the existing data set rules required for export to NCIC, TCIC, and any other TXDPS resource required.

Assurance that the database is maintained in full compliance with all applicable government laws, rules, procedures, and statutes.

Support for external agencies wishing to contribute data to TX Gang via one-time data migration or

ongoing batch upload. Support shall consist of coordinating with agencies to provide transfer specifications, field matching, and automated report emails.

Full and indelible audit logs as requested by TXDPS for all operations performed within the database to include but not be limited to compliance with the most up to date version of the CJIS Security Policy including auditing, accountability, access, control, identification and authentication.

Means for participating agencies to export their own data either en masse or singularly to both an analysis software program as well as a spreadsheet format.

Data archiving to comply with statutory requirements and TXDPS Records Retention Schedules

Assurance that records that have met legislatively mandated expiration dates are not retained past their legally mandated expiration dates by programmatically removing such records from the active record database

Provide system edits to verify the validity of a record during the life of the record, from creation to expiration

Provide a user management component that will allow local users to manage their own users (resetting passwords, etc.), as well as, provide the ability for Administrators to create and manage user accounts statewide

The Vendor will supply to TXDPS all necessary reference manuals, sample data, source documents, and any other information required to perform maintenance.

### **3.6 Preventive Maintenance**

The Vendor shall provide preventive maintenance services in order to maintain the System in good condition and working order on a mutually agreeable scheduled basis. The preventive maintenance schedule is to be based on the Vendor and TXDPS CM or assigned designee mutual agreement of the particular service required for each system component, it being understood that this schedule will be oriented around periods when the System is expected to have the lightest use and outside of the PRINCIPAL PERIOD OF OPERATION.

The PRINCIPAL PERIOD OF OPERATION coverage is Monday through Friday during the hours of 8:00 a.m. to 6:00 p.m. CST, excluding state or federal holidays.

The Vendor shall:

- A. Provide an advance notice reminder to the TXDPS' Project Manager or assigned designee at least five (5) calendar days prior to scheduled preventive maintenance activities for those activities that impact System operation.
- B. Provide the TXDPS' Project Manager or designee with email or phone notice of unscheduled preventive maintenance activities and receive approval from the TXDPS prior to services being rendered.
- C. Provide installation of patches and upgrades of all application and operating system software associated with the System, with written preauthorization of the TXDPS to keep current with FBI

CJIS and TXDPS IT Division standards. Updates to manuals resulting from System software updates will be supplied to the TXDPS free of charge.

- D. Install, without charge outside Principal Period of Operation, all mandatory changes with written preauthorization from the TXDPS.
- E. Replace faulty, malfunctioning, or end-of-life System software to maintain the current level of System functionality and operational effectiveness.

Cost for preventive maintenance services will be included in the predetermined monthly maintenance cost.

### **3.7 Remedial Maintenance**

Remedial Maintenance is defined as maintenance performed during System component failure that is performed by the Vendor on an unscheduled basis.

The Vendor shall:

- A. Provide all necessary maintenance at no cost to the TXDPS to remedy malfunctioning system hardware or software to regain full operability.
- B. If the TXDPS gives notice to the Vendor of a System failure, notification shall be considered approval to provide remedial maintenance. If the Vendor discovers a System failure, the Vendor shall notify the TXDPS according to the terms defined in the Service Level Agreement. The Vendor shall follow Critical Blocker procedures defined in the Service Level Agreement for instances of remedial maintenance.
- C. Produce a notification banner for users attempting to access the faulty System. Such notification banner shall indicate the System is down and will show an estimated time of System availability. The Vendor shall update the banner hourly, providing the current status and estimated time of System availability.

### **3.8 System Modifications and Enhancements**

System modifications and/or enhancements shall be performed by the Vendor outside the scope of Preventive or Remedial Maintenance. These activities will include but not be limited to customization, enhancements or other related services.

The Vendor shall:

- A. Perform modifications/enhancements as requested by the TXDPS if the service to be rendered is less than three (3) hours, at no additional cost to the TXDPS. Coordination of the requested services will be mutually agreed upon in writing prior to services being rendered.
- B. Complete a Change Order Plan (COP) issued by the TXDPS.
  - 1. Provide modification/enhancement services that are estimated to exceed three (3) hours by the issuance of a COP utilizing Exhibit 1, Change Order template.
  - 2. Properly fill out the COP to include the specific areas added or changed by the TXDPS. Areas may include Work Breakdown Structure (“WBS”), delivery dates, responsibilities and other critical information necessary for the services to be rendered.

3. Upon approval and signatures from the Vendor and the TXDPS PM, the COP will be forwarded to the Contract Monitor, who will secure approval and issuance from the Contract Administrator. The Contract Administrator will not approve and issue the COP until such time as all appropriate TXDPS signatories have reviewed and approved the COP request. After all signatories have reviewed and approved the COP, the Contract Administrator will initiate a Contract modification. A Contract modification is required for all COPs. No services will be rendered until the Vendor receives an approved COP from the Contract Administrator with all appropriate TXDPS signatures.
  4. Ensure all services are within scope of this Contract and have been requested at the sole discretion of the TXDPS.
  5. Abide by the terms and conditions within this Contract and not add any contractual terms and conditions to the COP.
- C. Repair defects enumerated in the COP caused by the following: acts of God; the TXDPS or its designated agent or users; neglect; misuse or abuse of the System; or use of non-recommended products or services.

### **3.9 Software Support**

The Vendor shall:

- Provide 24 x 7 x 365 monitoring of all support software necessary to administer all applications per stated SLAs.
- Provide routine patching and upgrades of all software that directly or indirectly impacts application production availability to maintain compliance with software manufacturer's versioning requirements and TXDPS IT Division standards.
  - Identify all (both reported and non-reported) software issues within one (1) hour of occurrence.
  - Begin remediation of all (both reported and non-reported) issues within one (1) hour of identification.
  - If the issue cannot be resolved in the stated timeframe, the Vendor shall contact, via email communication, the TXDPS Information Technology Division Operations Intelligence Center (ITD OIC): 1-888-377-6420 and designated TXDPS CM or assigned designee assigned to the specific application.
- Support response times and ticket detail will be submitted to the TXDPS CM or assigned designee or assigned designee with each month's per application, incident report.

### **3.10 Application, Software, Network Infrastructure Support Requirements**

The Vendor shall:

- Identify and notify TXDPS of all software, and network technology issues that arise within all dependent and independent components of all applications and technology infrastructure.
- Track software and networking issues and identify each incident via a unique designation identifier. The incident ticket will provide all information and documentation as required within Section 6.
- Assign a severity level to each incident. Severity level scale is detailed within Section 7 of this SOW.
- Report all issues encountered to the TXDPS ITD OIC, provide severity level, root cause, and estimated resolution time.

- Provide a monthly summary of all incident tickets encountered while providing application maintenance and support.
- Provide software refresh plans to address end of support or end of life products. The plans shall also address application patches and implementation methodology and proposed deployment schedules.

### **3.11 Maintenance Responsibilities of TXDPS**

#### **3.11.1 Notification**

TXDPS shall notify the Vendor's designated contact immediately upon discovery of system failure and shall permit the Vendor prompt and unfettered access to the system. TXDPS shall provide the Vendor use of necessary data communications facilities and equipment at no charge to Vendor subject only to TXDPS security regulations.

#### **3.11.2 Vendor Office and Storage**

TXDPS may provide the Vendor with a work area at no charge. The Vendor shall, at a minimum, supply field engineering materials, devices, and aids necessary to maintain the system in good working order.

#### **3.11.3 Authorized Support**

TXDPS personnel will not attempt any repair or maintenance on the System while the System is covered by this SOW unless previously agreed upon in writing by the Vendor as part of normal operator maintenance responsibilities. TXDPS will not request or allow any individual other than the Vendor's support personnel or TXDPS employees specifically approved to make any adjustment, repair or maintenance.

#### **3.11.4 Maintenance Personnel**

Depending upon the availability of TXDPS manpower and the practicability for TXDPS to do so, TXDPS will assign a person or persons (TXDPS employee(s) specifically approved) to coordinate all maintenance activities and to work with the Vendor. The Vendor shall work with said person(s). TXDPS shall bear all responsibility for any actions performed by the TXDPS employee(s), which were not directed by or requested by or under the control of the Vendor. The Vendor shall bear all responsibility for activities performed by all of its employees. Some TXDPS employees will be considered under the direction of the Vendor (for training purposes). The Vendor shall bear final responsibility for control of any TXDPS employees in training or placed under the Vendor's direction as specified by SLA(s) or separate Contract provisions. Depending upon the availability of TXDPS manpower and the practicability for TXDPS to do so, TXDPS will assign competent, trained personnel to cooperate with the Vendor. Should the Vendor feel any recommended TXDPS employee is not performing or able to perform the duties necessary for training or as specified by SLA(s) or separate contract the Vendor must submit its concerns in writing to the designated TXDPS CM or assigned designee. TXDPS personnel will be available for consultation and to answer pertinent questions as specified in the SLA.

### **4. Outsourced Services**

The prime Vendor shall ensure any subcontractors working under this Contract comply with all Contract Requirements.

## **5. Deliverable Receipt, Acceptance and Change Management**

### **5.1 Application Development or Enhancement Test, Acceptance, and Receipt.**

- All deliverables will be provided on the dates specified in each uniquely identified and approved Change Order.
- All deliverables will have a testing period of ten (10) calendar days, with acceptance contingent upon five (5) calendar days of error free operation.
- If test and acceptance is not achieved by the tenth business day, the testing period will continue until achievement of test requirements and acceptance by TXDPS. The Vendor will not be paid for any additional work provided to achieve deliverable acceptance beyond the quantity of hours originally agreed upon within the signed Change Order. If successful testing and acceptance of the identified deliverable is not achieved, payment will not be provided.
- If the deliverable cannot be provided within the agreed upon and scheduled timeframe, the Vendor is required to contact the TXDPS CM or assigned designee, per the Change Management Requirements below.

Beyond the test and acceptance period, all deliverables will have up to a ninety (90) day post-launch production quality validation period. The TXDPS CM or assigned designee and the Vendor shall monitor application performance for stability and validate that deliverables meet current and projected performance requirements. Post-launch production validation will be considered complete when both parties sign the Change Order Acceptance Form (Exhibit 2)

### **5.2 Application Maintenance and Support Acceptance and Receipt.**

The TXDPS PM or assigned designee will review the monthly summary of incident reports during the first week of each following month. If all incidents were addressed within the time frames, the TXDPS PM or assigned designee will certify all maintenance and support activities were provided within the stated requirements

### **5.3 Change Management**

- Any changes to the Change Order delivery dates shall be reviewed and approved by the TXDPS CM or assigned designee before being placed in effect.
- The Vendor's request for a revised schedule shall include the impact on: related and/or dependent tasks, overall project, resolution methodology for correcting deficiencies, and change to specific and overall timeframes.
- TXDPS shall document changes to delivery dates by the update of Change Order governance table(s) by the TXDPS CM or assigned designee and provide such documentation to the Vendor PM or assigned designee.
- Any administrative or substantive requirement changes to this SOW shall be approved by both parties in writing and documented by a TXDPS Modification of Contract form. TXDPS or the Vendor PM or assigned designee shall initiate the change process by notifying the other party in writing; email is acceptable, and by submitting a written Change Order signed by both parties, to TXDPS Contract Administrator. No work is to begin until Change Order is executed by Procurement and Contract Services.

The Vendor is hereby advised that changes to the Software Solution system will be subject to the TXDPS' Change Control Board (CCB) process. This requirement is mandatory for the Vendor hosted and the TXDPS hosted packages. The TXDPS shall initiate and manage the change control process. The purpose of the TXDPS' IT Change Management (ITCM) is to ensure that Change Requests (CRs) to the TXDPS' IT systems are properly reviewed, authorized, implemented and tracked with minimum disruption to service levels. The purpose of our change management policy is to ensure accountability, communication, transparency and visibility between IT and the Business. The Vendor shall submit a change request to the CCB detailing what is changing and where it is changing, along with test plans, test results, and communication processes for before and after a change. There are two types of change requests:

A. Standard CR

Standard CRs follow the 'normal' change request process. This means these changes will be approved by the CCB prior to being released to a production environment.

B. Emergency CR

Emergency CRs will follow an abbreviated version of the CCB process. The following are considered emergency CRs:

1. Production system down;
2. Multiple users/sites affected ;
3. Misprocessing data; and
4. Security risk.

**6. Reports and Meetings**

- For all Change Order events, the Vendor, if requested by the TXDPS, shall arrange a kickoff meeting to be held at the TXDPS Main Campus located at 5805 N. Lamar Blvd. Austin, TX 78752, at a date and time agreeable to the TXDPS at no additional cost to the TXDPS. The Vendor PM or assigned designee and TXDPS CM or assigned designee, shall attend all project meetings. The TXDPS CM shall be informed of all meetings prior to occurrence.
- The Vendor shall provide the TXDPS CM with monthly, written, progress reports for each in-process Change order and maintenance and support incident reports.
  - "Progress Reports" are monthly status summaries of Change Order progress.
  - "Incident Reports" are monthly summaries of all "incident tickets", "tickets".
- Progress and incident reports shall be submitted by 5:00 pm CST Monday following the last working day of the month throughout the life of an active Change order or this Contract term. Email submission of the reports is acceptable.
- Progress reports shall cover all work performed and completed during the month for which the progress report is provided and will present the work to be performed during the subsequent month.
- Progress reports will identify any problems encountered with that month's development, all outstanding issues with an explanation of the cause, resolution methodology, and updated Change Order governance tables.
  - Incident reports will detail: each issue encountered by incident ticket identifier, affected application(s), , affected software, affected networking infrastructure, incident discovery method (e.g.

infrastructure monitoring, technical support call / email, error discovered while performing maintenance, etc.), severity level, root cause analysis findings, detailed actions taken to resolve the issue, time expensed in correcting the issue, name of person reporting the issue and report method, the Vendor's staff assigned to the issue, initial response time and method, and other agreed to report details requested by the TXDPS CM.

- The Vendor shall provide a listing of all programming languages used, updated as changes are made, in development and maintenance of the applications. Languages applicable to application functionality will be identified within the Transition Plan and included in monthly maintenance reports.

## 7. Service Level Agreements – SLAs

The Vendor shall provide a service credit to TXDPS equal to one-hundred dollars (\$100.00) for failure to meet any stated SLAs. Service credits will be applied on a per-application development and / or enhancement, or application maintenance basis.

### 7.1 Definitions:

“Uptime” is defined as any period of time 24 x 7 x 365 when an application is available to the “customer base” within the stated “availability technical requirements”.

“Downtime” is defined as any period of time 24 x 7 x 365 when an application is unavailable to the “customer base” to include but not limited to: outages, unscheduled maintenance & support events, software failures, or access to application is less than the stated “availability technical requirements”.

“Technical Availability” is defined as the customer base’s application access to an application, customer base’s access to test environments, and associated information or data results and/or exports based on customer base’s interaction with any application or supporting technology.

“Customer Base” is defined as any person or representative of TXDPS, the network-accessible, or an Authorized Data Access Entity (ADAE).

“Issue” is defined as any event that results in a loss of access to an applications production environment, test environment, or supporting technology that results in an application not achieving availability or technical requirements.

“Severity Level” is a defining classification scheme for all issues with corresponding resolution times.

- Critical/blocker (system is down and non-usable – Severity 1) -- Respond within in 1 hour, fix delivered in 24 hours.
- High (system is functional but suffering from significant impact to operations – Severity 2) -- Respond in 4 hours, fix delivered in 72 hours.
- Medium (system is functional, some impact to operations – Severity 3) – Respond in 8 hours, Fix delivered in 10 days or less.
- Low (minor issue, no impact to operations – Severity 4) – Respond in 24 hours, Fixed delivered based on prioritization of planned releases.

## 7.2. Application Performance Service Levels

The Vendor shall provide application, test and production environments, uptime on a 24 x 7 x 365 basis at a rate of ninety-nine and one-half percent (99.5%) operational availability to meet customer base needs.

The Vendor shall provide the customer base with application accessibility at the following minimum requirements assuming TXDPS' hardware is fully operational:

- .05 second limit for manipulating webpage objects
- 1 second limit for navigating to, from, and between main webpage, subordinate webpages and associated hyperlinks
- 1 second limit for navigating webpage command space
- 2 second limit for submitting a data request and getting a processing acknowledgment
- 10 second limit for retrieving data from a data request

## 7.3 Rate calculation

The rate calculation will be measured as the rate of System's technical availability by the amount of downtime during a calendar month. This metric gauges the application(s) performance as a percentage of available hours tracked to the quarter of an hour (rounded). The rate of system performance will be measured and monitored as follows:

- Available hours equal total number of hours in a month (24 hours x number of days in the month) minus the actual amount of time spent to the quarter of an hour for scheduled maintenance for the hosted application.
- Downtime is the total number of hours (rounded to the quarter hour) during which the solution is not in operation.
- System Performance Rate equals available hours Downtime divided by available hours.

Example for the month of January:

Available time per month was 744 hours (31 days X 24 hours)

Downtime per month was 3.75 hours (start 1:00 am - end 4:40 am)

$744.00 - 3.75 = 740.25$

$740.25 \div 744 = 99.5\%$

### 7.3.1 Escalation Process

Inability to meet or exceed the RATE during this Contract period will result in the following actions:

First event – verbal warning

Second event – written warning added to this Contract file

Third event – Negative Vendor Performance report

TXDPS reserves the right (as per TXDPS Technical Terms and Conditions) to terminate this Contract at any time.

## 8. Training

- A. The Vendor shall provide a detailed training plan within thirty (30) calendar days after contract award for the TXDPS users to acquire the necessary skills and proficiencies. All training programs will be conducted at TXDPS Headquarters, located in Austin, Texas. Training will be interactive with an emphasis on all appropriate development skills, and users shall have the ability to ask questions of the trainer during the sessions. The schedule of training sessions will be coordinated with the TXDPS' Project Manager. The requirements of the training programs are as follows:
1. Train the Trainer:
    - a. The Train the Trainer training will be offered to selected TXDPS users to acquire the necessary information, skills, and proficiencies of the user interface and database to allow those users to train other typical users how to use the user interface and database to its fullest potential.
    - b. The training will include advanced user techniques and basic technical troubleshooting skills.
    - c. It is estimated that the TXDPS will receive a minimum of no less than eight (8) training sessions during the total potential contract term, including the Base term and each Renewal Option Periods.
  2. Developer Training:
    - a. The developer training will be provided to select TXDPS personnel who will be responsible for the daily operation and maintenance of the database.
    - b. The developer training will provide TXDPS personnel with the skills needed to integrate new data into the database.
    - c. The developer training will include data integration training designed for TXDPS personnel to be able to interface with internal and external data sources.
    - d. The developer training course will include overviews of the entity model, importing an SQL database, multi-level security related to data sources and analysis outcomes, and entity resolution.
    - e. It is estimated that the TXDPS will receive a minimum of no less than three (3) developer training sessions during each of the Base and Renewal.
- B. The Vendor's training programs will allow the TXDPS and the Vendor to jointly alter the proportion of train the trainer, analyst, developer, and certified training programs so as to maximize the overall effectiveness of the training for the TXDPS. All training sessions including any web-based sessions will be live and/or interactive.
- C. The Vendor shall scale, detail, and tie training to match the user interface and database.
- D. The Vendor shall submit to the TXDPS' Project Manager copies of the curricula and associated User Guides for trainees for acceptance by the TXDPS no less than fifteen (15) calendar days prior to the first training program for each type of training.
- E. The Vendor shall make available to the TXDPS video recorded training for each training program as a review/refresher resource for TXDPS personnel who have already completed the live training.

## 9. Reproduction of Materials

TXDPS may reproduce all documentation and printed materials provided by the Vendor. If the documentation described above is revised at any time or if the Vendor develops additional documentation for the System, the Vendor shall deliver an electronic copy of such revised or additional documentation to TXDPS at no additional cost.

## 10. Period of Performance

The term of this Contract shall be September 1, 2015, or the date of TXDPS PO issuance, through August 31, 2016.

## 11. Invoices

Invoices associated with the provided services will be submitted monthly to [APIInvoices@dps.texas.gov](mailto:APIInvoices@dps.texas.gov) for all accepted Change Order deliverables and maintenance & support requirements associated with this Contract. A copy of the submitted invoice will also be sent, via email, to the TXDPS CM or assigned designee identified for each specific application or individual Change Order. Invoices will contain all required information per the State of Texas Procurement Manual listed on the Texas Comptroller of Public Accounts website (<http://www.cpa.state.tx.us/procurement/pub/manual/2-43.pdf>).

### 11.1 Maintenance invoices shall detail:

- a. The TXDPS Purchase Order number,
- b. The TXDPS application name for which maintenance was provided,
- c. Detail of any SLAs missed for the month and the cumulative credit being applied.

### 11.2 Application development and / or enhancement invoice shall detail:

- a. The TXDPS Purchase Order Number,
- b. The assigned TXDPS Change Order Alpha Designation,
- c. Identified Service Provided by Description,
- d. Quantity of Hours Associated with the Service Provided per Service Title,
- e. Actual cost to TXDPS for the Service Provided per Service Title,
- f. Detail of any SLAs missed for the month and the cumulative credit being applied,
- g. A copy of the TXDPS Change Order Acceptance Document signed by both parties.

## 12. Additional Customer Terms and Conditions

### 12.1 FBI CJIS Security Addendum

The Vendor shall execute an original signed CJIS Security Addendum which can be downloaded from <http://txdps.state.tx.us/securityreview>. Additionally, a CJIS Security Addendum Certification shall be signed by each employee performing duties related to this project prior to working on this Contract. Each original Certification shall include an original signature of the employee and the Vendor's representative. Non-compliance by the Vendor will be cause for termination of this Contract.

The Vendor shall, prior to beginning work on this Contract, enter into the CJIS online system all Vendor employees and subcontractors who will work on this Contract (further instructions will be provided to the Vendor prior to execution of this Contract), and have those employees/subcontractors complete the CJIS online training/testing. The Vendor shall meet or exceed all requirements contained in the CJIS Security Policy.

### 12.2 Vendor Background Check Completion

The Vendor's Authorized Representative shall provide the following to the TXDPS' Contract Manager within ten (10) calendar days of executing this Contract:

- i. The completed TXDPS Contractor Background Information form (HR-22) for all proposed personnel; and
- ii. Acceptable fingerprints for all proposed personnel.

The Vendor will not allow any personnel to work on the project that have not submitted to and successfully completed a TXDPS fingerprint-based Criminal History Background Investigation. The TXDPS has the right to prevent the Vendor's personnel from gaining access to the TXDPS building(s) and computer systems if the TXDPS determines that such personnel did not pass the background check or failed to otherwise maintain a security clearance.

### **13. Vendor Requirements and Response Submission**

Respondents interested in this opportunity shall detail as part of their Pricing Request response, how they meet the following qualifications. Qualification demonstration shall include but not be limited to verifiable documentation of:

- Year of experience
- Similar in scope projects

Respondents shall also response with sufficient detail necessary to prove competency in meeting all requirements stated within this SOW.

At a minimum, the Vendor shall have demonstrated experience in each of the following:

**13.1 Application Language:** JAVA, DB2 SQL Stored Procedures

#### **13.2 Operating Systems**

Web based access will be available regardless of user platform, but at a minimum will support Internet Explorer 7 and higher versions, and common mobile devices to include, but not be limited to, iPhone, iPad, Android, and BlackBerry devices. Red Hat Enterprise Linux Server release 5.4; Tomcat 7.0.23

#### **13.3 SQL Technologies**

Advanced Query Analysis and Optimization  
SQL Server Linked Servers  
Supporting large scale web applications

#### **13.4 System Knowledge**

The Vendor shall have verifiable experience in the following areas:

- All technologies referenced in Section 2.1
- Working with TCIC/NCIC transactions and communications
- Export formats such as Comma Separated Value (.csv) for certain information and reports
- XML for individual gang member data
- 12 Analyst Notebook (.anb) for individual gang member data

Respondents shall provide references from three (3) projects of similar size databases that involved intelligence data regulated by the Code of Federal Regulations Title 28, Chapter I, Part 23.

405-15-R025523  
Attachment C - SOW  
TXDPS Texas Gang Intelligence Index (TX Gang)  
Application Development, Maintenance & Support,  
Technology Upgrade/Migration and Transformation

The Vendor's augmented deliverable response information shall be phrased in terms and language that can be easily understood by non-technical personnel (e.g., laypersons without subject matter expertise).

- Any acronyms used in the Respondent's response, shall be clearly detailed and spelled out.
- SOW responses shall be in the same form and fashion as provided by TXDPS through this solicitation. The PR documents including all attachments, addendas, and exhibits are to be modified using Track Changes, identifying all additions, deletions, and / or modifications from the original.
- Any Respondent-added information shall be placed within the corresponding and relevant section of this SOW.

Respondent shall provide a response narrative for each Section and Subsection in the format in which requirements are presented. Supplemental justification and / or documentation may be provided as attachments. The Respondent shall ensure that all material submitted is directly pertinent to the requirements of this SOW and shall be formatted as to the specific requirements of the SOW Sections.

Respondent shall submit in editable, public format, all required documents via email to the TXDPS Contract Administrator by the date and time listed on the SOW. Required documentation shall include:

- **1.** Cover Page - List name and address of the Respondent, date of Offer, SOW identifier, and signature of authorized official.
- **2.** Completed SOW document and Attachment A
- **3.** Respondent's Project Team Resumes:
  - Employee names
  - Employee titles
  - Employees work experiences and corresponding dates - relevant to scope of this SOW
  - Additional in-scope skills, abilities, knowledge
- **4.** Respondent's organizational chart to include phone and email contact information
- **5.** An original and signed CJIS Security Addendum - Reference Section 12.
- **6.** An FBI Certification page to the CJIS Security Addendum for each employee performing duties related to the project - Reference Section 12.
- **7.** Documentation verifying compliance with CSA CCM - Reference Section 3.1.
- **8.** Documentation verifying experience with and familiarity of working with the State's payment portal.
- **9.** Completed HUB HSP Plan

**14. SOW Authorization**

Vendor	<b>Texas Department of Public Safety</b>
By:	By:
Name: _____	_____
Title: _____	Name: <u>Robert J. Bodisch</u>
Date: _____	Title: <u>Deputy Director, Homeland Security and Services</u>
_____	Date: _____
_____	_____

## Consensus Assessments Initiative Questionnaire

Control Group	CGID	CID	Consensus Assessment Questions
Independent Audits	CO-02	CO-02.2	How often do you conduct network penetration tests of your cloud service infrastructure.
		CO-02.3	How often do you conduct regular application penetration tests of your cloud infrastructure?
		CO-02.4	How often do you conduct internal audits?
		CO-02.5	Do you conduct external audits regularly as prescribed by industry best practices and guidance?
		CO-02.6	Are the results of the network penetration tests available to tenants at their request?
		CO-02.7	Are the results of internal and external audits available to tenants at their request?
Third Party Audits	CO-03	CO-03.1	Will you permit DPS to conduct vulnerability scans on hosted applications and your network?
		CO-03.2	Do you have external third-party conduct vulnerability scans and periodic penetration tests on your applications and networks?
Audit Tools Access	IS-29	IS-29.1	How do you restrict, log, and monitor access to your information security management systems? (Ex. Hypervisors, firewalls, vulnerability scanners, network sniffers, APIs, etc.)
Information System Regulatory Mapping	CO-05	CO-05.1	How do you ensure customer data is logically segmented that data may be produced for a single tenant only, without inadvertently accessing another tenant's data?
		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?
Intellectual Property	CO-06	CO-06.1	Describe the controls you have in place to protect tenants intellectual property?

### Data Governance

## Consensus Assessments Initiative Questionnaire

Control Group	CGID	CID	Consensus Assessment Questions
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)?
Classification	DG-02	DG-02.4	Can you provide the physical location/geography of storage of a tenant's data upon request?
		DG-02.5	Do you allow tenants to define acceptable geographical locations for data routing or resource instantiation?
Handling / Labeling / Security Policy	DG-03	DG-03.1	Are Policies and procedures established for labeling, handling and security of data and objects which contain data?
Retention Policy	DG-04	DG-04.1	Describe technical control you have in place to enforce tenant data retention policies?
Secure Disposal	DG-05	DG-05.1	Describe your process for secure disposal or destruction of physical media and secure deletion or sanitization of all computer resources of DPS data once DPS has
Nonproduction Data	DG-06	DG-06.1	How do you ensure production data is not be replicated or used in non-production environments?
Information Leakage	DG-07	DG-07.1	Describe the controls in place to prevent data leakage or intentional/accidental compromise between tenants.
		DG-07.2	What a Data Loss Prevention (DLP) or extrusion prevention solution is in place for all systems which interface with your cloud service offering?
<b>Facility Security</b>			
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?
Unauthorized Persons Entry	FS-05	FS-05.1	How are ingress and egress points such as service areas and other points where unauthorized personnel may enter the premises, monitored, controlled or isolated from data storage and process?
Asset Management	FS-07	FS-07.1	What are your procedures governing asset management and repurposing of equipment used to support DPS hosted services or data?
<b>Human Resources Security</b>			

## Consensus Assessments Initiative Questionnaire

Control Group	CGID	CID	Consensus Assessment Questions
Background Screening	HR-01	HR-01.1	Are state of residency and national fingerprint-based record checks conducted on employees or contractors who have access to DPS's data, applications or the networks supporting DPS's data and or applications?
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?
		HR-02.2	Do you document employee acknowledgment of training they have completed?
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?
<b>Information Security</b>			
Management Program	IS-01	IS-01.1	Do you provide tenants with documentation describing your Information Security Management Program (ISMP)?
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?
Policy	IS-03	IS-03.1	Do your information security and privacy policies align with particular industry standards (ISO-27001, ISO-22307, CoBIT, etc.)?
		IS-03.2	Do you have agreements which ensure your providers adhere to your information security and privacy policies?
	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?
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?
Policy Enforcement	IS-06	IS-06.1	Is a formal disciplinary or sanction policy established for employees who have violated security policies and procedures?
		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?

## Consensus Assessments Initiative Questionnaire

Control Group	CGID	CID	Consensus Assessment Questions
User Access Policy	IS-07	IS-07.1	What controls do you controls in place to ensure timely removal of systems access which is no longer required for business purposes?
User Access Restriction /	IS-08	IS-08.1	Describe process for granting and approving access to DPS data or hosted services.
User Access Revocation	IS-09	IS-09.1	Describe process for timely deprovisioning, revocation or modification of user access to the DPS data or hosted services upon any change in status of employees, contractors, customers, business partners or third parties?
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)?
		IS-10.2	If users are found to have inappropriate entitlements, are all remediation and certification actions recorded?
Training / Awareness	IS-11	IS-11.1	Do you provide annually a formal security awareness training program for cloud-related access and data management issues for all persons with access to DPS or hosted services?
	IS-12	IS-12.2	Do you benchmark your security controls against industry standards?
Segregation of Duties	IS-15	IS-15.1	How do you maintain segregation of duties within your cloud service offering?
Encryption	IS-18	IS-18.1	Do you have a capability to allow creation of unique encryption keys per tenant?
		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)?
Encryption	IS-19	IS-19.1	What encryption method and level of encryption is applied to DPS's data at rest and does it meet FIPS 140-2?
		IS-19.3	For DPS data in transport, what encryption level is applied and is the cryptographic module FIPS 140-2 certified.
		IS-19.4	Describe your key management procedures?
Encryption Key Management			
Vulnerability / Patch Management	IS-20	IS-21.1	Describe your patch management process?

## Consensus Assessments Initiative Questionnaire

Control Group	CGID	CID	Consensus Assessment Questions
Antivirus / Malicious Software	IS-21	IS-21.1	Do you have anti-malware programs installed on all systems which support DPS hosted services and data?
		IS-21.2	How do you ensure that security threat detection systems which use signatures, lists, or behavioral patterns are updated across all infrastructure components which support DPS's hosted services.
Incident Management	IS-22	IS-22.1	Do you have a documented security incident response plan
			Do you have processes for handling and reporting of security incidents that include preparation, detection, analysis, containment eradication, and recovery?
			What steps are taken to ensure all employees are made aware of the incident reporting procedures?
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?
Network Monitoring	IS-27	IS-27.1	List the tools used to monitor network events, detect attacks, and provide identification of unauthorized use.
Source Code Access Restriction	IS-33	IS-33.1	Describe the controls in place to prevent unauthorized access to your application, program or object source code, and assure it is restricted to authorized personnel only?
Utility Programs Access	IS-34	IS-34.1	How are utilities that can significantly manage virtualized partitions (ex. shutdown, clone, etc.) appropriately restricted and monitored?
<b>Release Management</b>			
Production Changes	RM-02	RM-02.1	Do you have documented change management procedures?
Quality Testing	RM-03	RM-03.1	Do you provide your tenants with documentation which describes your quality assurance process?
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?
		RM-04.2	Do you have controls in place to detect source code security defects for any outsourced software development activities?
Unauthorized Software Installations	RM-05	RM-05.1	What controls do you have in place to restrict and monitor the installation of unauthorized software onto your systems?

## Consensus Assessments Initiative Questionnaire

Control Group	CGID	CID	Consensus Assessment Questions
<b>Resiliency</b>			
Business Continuity Testing	RS-01	RS-01.1	Are Policy, process and procedures defining business continuity and disaster recovery in place to minimize the impact of a realized risk event?
	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?
Equipment Power Failures	RS-07	RS-07.1	How are Security mechanisms and redundancies implemented to protect equipment from utility service outages (e.g., power failures, network disruptions, etc.)?
<b>Security Architecture</b>			
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?
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?
Password			Describe password requirements
Application Security	SA-04	SA-04.2	Do you utilize an automated source-code analysis tool to detect code security defects prior to production?
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?
Remote User Multifactor Authentication	SA-07	SA-07.1	Describe multi-factor authentication method required for all remote user access.
Segmentation	SA-09	SA-09.4	Are system and network environments logically separated to ensure protection and isolation of sensitive data?
Wireless Security	SA-10	SA-10.1	Are policies and procedures established and mechanisms implemented to protect network environment perimeter and configured to restrict unauthorized traffic?

## Consensus Assessments Initiative Questionnaire

Control Group	CGID	CID	Consensus Assessment Questions
		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.)
		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?
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?
Audit Logging / Intrusion Detection	SA-14	SA-14.1	What file integrity controls and network intrusion detection (IDS) tools are deployed to help facilitate timely detection, investigation by root cause analysis and response to incidents?
		SA-14.2	Is Physical and logical user access to audit logs restricted to authorized personnel?

## **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							GAPP (Aug 2009)
				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	
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 4.2.3 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
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-2 (1) NIST SP800-53 R3 RA-5 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 (9) NIST SP800-53 R3 RA-5 (6)	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.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
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 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 1.2.6 GAPP Ref 1.2.11 GAPP Ref 3.2.4 GAPP Ref 5.2.1

# 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 - 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 v6.0: D.2.2	SIG 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 8.2.6
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.  Removed the specific reference to tape and disk backup as there are other media types	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.	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 164.308(a)(7)(ii)(D) (New) 45 CFR 164.316(b)(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-2 (1) NIST SP800-53 R3 CP-2 (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 3.1 PCI DSS v2.0 3.1.1 PCI DSS v2.0 3.2 PCI DSS v2.0 9.9.1 PCI DSS v2.0 9.5 PCI DSS v2.0 9.6 PCI DSS v2.0 10.7	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
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.2.2.14,	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.2.18	GAPP Ref 1.2.6

# 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							GAPP (Aug 2009)
				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	
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-8 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-8 NIST SP800-53 R3 SI-7 (1) 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: 1.2.18	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) 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-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.1.6, F.1.7, F.1.8, F.1.9, F.2.1, F.2.2, F.2.3, F.2.4, F.2.5, F.2.6, 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, F.1.4.6, 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, 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	GAPP Ref 8.2.3

# 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							GAPP (Aug 2009)
				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	
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 attestation mechanisms shall be designed to address the requirements of legislative plurality and their results shared with tenants	X	X	X	X		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 R3 PE-7 NIST SP800-53 R3 PE-8 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-7 NIST SP800-53 R3 PE-7 (1) NIST SP800-53 R3 PE-8 NIST SP800-53 R3 PE-18	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 9.2	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, 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	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 prevent 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, 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	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 9.8 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
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 repurposing 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 Security - 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

# 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							GAPP (Aug 2009)
				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	
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: <ul style="list-style-type: none"> <li>• Risk management</li> <li>• Security policy</li> <li>• Organization of information security</li> <li>• Asset management</li> <li>• Human resources security</li> <li>• Physical and environmental security</li> <li>• Communications and operations management</li> <li>• Access control</li> <li>• Information systems acquisition, development,</li> </ul>	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 164.306(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
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-11 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
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 leadership and officer 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.8.2.2	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 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 reassessed at least annually or upon significant	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

# 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							GAPP (Aug 2009)
				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	
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 CFE 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 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 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.1.5	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.6.2, 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

# 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							GAPP (Aug 2009)
				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	
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
Information Security - User Access Reviews	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 tiers (IaaS, SaaS, PaaS, IDaaS...). Automatic or manual remediation 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)(iii)(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	PCI DSS v2.0 8.5.4 PCI DSS v2.0 8.5.5	SIG v6.0:H.2.6, H.2.7, H.2.9,	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 an 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	PCI DSS v2.0 12.6 PCI DSS v2.0 12.6.1 PCI DSS v2.0 12.6.2	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	PCI DSS v2.0 12.6 PCI DSS v2.0 12.6.1 PCI DSS v2.0 12.6.2	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

# 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							GAPP (Aug 2009)
				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	
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)(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	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 8.5.7 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
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)(1) 45 CFR 164.312 (e)(2)(ii)	A.10.6.1 A.10.8.3 A.10.8.4 A.10.9.2 A.10.9.3 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-16 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 4.2	AUP v5.0 G.4 AUP v5.0 G.15 AUP v5.0 I.3 SIG v6.0: G.10.4, G.11.1, G.11.2, G.12.1, G.12.2, G.12.4, G.12.10, G.14.18, G.14.19, G.16.2, G.16.18, G.16.19, G.17.16, G.17.17, G.18.13, G.18.14, G.19.1.1, G.20.14	GAPP Ref 8.1.1 GAPP Ref 8.2.1 GAPP Ref 8.2.5

# 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							GAPP (Aug 2009)
				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	
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 (5) 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	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)(ii)(A) 45 CFR 164.308 (a)(1)(i)(ii)(B) 45 CFR 164.308 (a)(5)(i)(ii)(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 (9) NIST SP800-53 R3 RA-5 (6) 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 6.1 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 1.2.6 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)(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-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-6 (1) 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

# 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							GAPP (Aug 2009)
				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	
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 12.9.6	SIG v6.0: J.1.2,	GAPP Ref 1.2.7 GAPP Ref 1.2.10
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 analysis output	X	X	X	X	X	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-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 12.3.5	AUP v5.0 B.3. SIG v6.0: B.1.7, 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-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.19.1.1, G.19.1.2, G.19.1.3, 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 8.2.5
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-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	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

# 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							GAPP (Aug 2009)
				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	
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 (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 6.2.1	
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:H.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 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	

# 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							GAPP (Aug 2009)
				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	
Legal - Third Party Agreements	LG-02	Third party agreements that directly, or indirectly, impact the organizations 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. Assets agreements 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)(ii)(A) 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 (c)(1) (New) 45 CFR 164.312(e)(2)(ii) (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 (b)(1) 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)	A.6.2.3 A.10.2.1 A.10.8.2 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-6 NIST SP800-53 R3 SA-7 NIST SP800-53 R3 SA-9	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 (1)	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, G.16.3,	GAPP Ref 1.2.5
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.8.2.2 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

# 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							GAPP (Aug 2009)
				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	
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 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 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 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 v6.0: A.1, L.1	SIG GAPP Ref 1.2.4
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 should 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 I.1 AUP v5.0 I.4 SIG v6.0: C.2.1, I.4.1, I.5, G.15.1.3, I.3	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 v5.0I.4 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.1.6, B.1.7.2, G.2, L.9, L.10	N/A

# 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							GAPP (Aug 2009)	
				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		
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	Service Providers shall implement and communicate disaster recovery, business continuity, capacity overflow and operational redundancy plans to all dependant service tiers. Service Providers shall perform failure impact analysis studies and communicate potential service impacts and reduced capacity projections to	X	X	X	X	X	COBIT 4.1 DS 2.3		A.6.2.1 A.8.3.3 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, A16.1		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-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 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	
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, A17.6	45 CFR 164.308 (a)(5)(iii)(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 (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.2.21, I.2.23, I.2.26, 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	

# 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							GAPP (Aug 2009)
				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	
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 legally 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.10.2.2 A.10.2.3 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.12.5.5 A.12.6.1 A.13.1.2 A.15.2.1 A.15.2.2	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 (1) NIST SP800-53 R3 SA-12 NIST SP800-53 R3 SA-13	PCI DSS v2.0 3.6.7 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 9.3.1 PCI DSS v2.0 10.5.2 PCI DSS v2.0 11.5 PCI DSS v2.0 12.3.1 PCI DSS v2.0 12.3.3	AUP v5.0 C.2 AUP v5.0 I.2 AUP v5.0 I.4 AUP v5.0 I.1 SIG v6.0: C.2.4, G.4, G6, I.1, I.4.4, I.4.5, I.2.7.2, I.2.8, I.2.9, I.2.15, I.2.18, I.2.22.6, 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, L.7, L.9, 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.10.4.1 A.11.5.4 A.11.6.1 A.12.4.1 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 (1)		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

# 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							GAPP (Aug 2009)
				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	
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	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: <ul style="list-style-type: none"> <li>Identify critical products and services</li> <li>Identify all dependencies, including processes, applications, business partners and third party service providers</li> <li>Understand threats to critical products and services</li> <li>Determine impacts resulting from planned or unplanned disruptions and how these vary over time</li> <li>Establish the maximum tolerable period for disruption</li> <li>Establish priorities for recovery</li> <li>Establish recovery time objectives for resumption of critical products and services within their maximum tolerable period of disruption</li> </ul>	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

# 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							GAPP (Aug 2009)
				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	
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: <ul style="list-style-type: none"> <li>• Defined purpose and scope, aligned with relevant dependencies</li> <li>• Accessible to and understood by those who will use them</li> <li>• Owned by a named person(s) who is responsible for their review, update and approval</li> <li>• Defined lines of communication, roles and responsibilities</li> <li>• Detailed recovery procedures, manual work-around and reference information</li> </ul>	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 164.310 (a)(2)(i) 45 CFR 164.312 (a)(2)(ii)	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 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)(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
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 a reasonable distance.	No Change	X	X	X	X			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,	N/A

# 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							GAPP (Aug 2009)
				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	
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.1.6.1, 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 taps, 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.1.6.1, 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.2.6.1, 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		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-6 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-6 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.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,	N/A

# 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)
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 leakage prevention) 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.11.4.6 A.12.3.1 A.12.5.4 A.15.1.4	NIST SP800-53 R3 AC-1 NIST SP800-53 R3 AC-4 NIST SP800-53 R3 SC-1 NIST SP800-53 R3 SC-16	NIST SP800-53 R3 AC-1 NIST SP800-53 R3 AC-4 NIST SP800-53 R3 SC-16	PCI DSS v2.0 2.3 PCI DSS v2.0 3.4.1, 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 6.5c PCI DSS v2.0 8.3 PCI DSS v2.0 10.5.5 PCI DSS v2.0 11.5	AUP v5.0 B.1 SIG v6.0: G.8.2.0.2, G.8.2.0.3, G.12.1, G.12.4, G.12.9, G.12.10, G.16.2, G.19.2.1, G.19.3.2, 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 9.2.1
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.16.3, I.3	GAPP Ref 1.2.6
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.12.6.1 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	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
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 B.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 B.1 SIG v6.0: H.1.1, G.9.13, G.9.20, G.9.21,	GAPP Ref 8.2.2

# 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							GAPP (Aug 2009)
				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	
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 (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 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	
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 network 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 DS5.5 COBIT 4.1 DS5.7 COBIT 4.1 DS5.8 COBIT 4.1 DS5.10	45 CFR 164.312 (e)(4)(2)(ii) 45 CFR 164.308(a)(5)(ii)(D) (New) 45 CFR 164.312(e)(1) (New) 45 CFR 164.312(e)(2)(ii) (New)	A.7.1.1 A.7.1.2 A.7.1.3 A.9.2.1 A.9.2.4 A.10.6.1 A.10.6.2 A.10.8.1 A.10.8.3 A.10.8.5 A.10.10.2 A.11.2.1 A.11.4.3 A.11.4.5 A.11.4.6 A.11.4.7 A.12.3.1 A.12.3.2	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-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 (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 v2.011.1 PCI DSS v2.0 9.1.3	AUP v5.0 D.1 AUP v5.0 B.3 AUP v5.0 F.1 AUP v5.0 G.4 AUP v5.0 G.15 AUP v5.0 G.17 AUP v5.0 G.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, 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 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.10.8.1 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 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	

# 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							GAPP (Aug 2009)
				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	
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 timelines. 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.16.8, 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 DS5.6 COBIT 4.1 DS9.2	45 CFR 164.308 (a)(1)(ii)(D) 45 CFR 164.312 (b) 45 CFR 164.308(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.9.6.2, G.9.6.3, G.9.6.4, G.9.19, H.2.16, 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 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/cm.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](mailto:info@cloudsecurityalliance.org)

# 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

QA by the HISPI  
12/01/10

Change Order *Template*

**1. Introduction:**

TXDPS Contract 405-xx-xxxxxxx with \_\_\_\_\_ incorporates the ability to scope, detail, and administer specific application enhancement Change Orders (CO). CO will be administered per the requirements of Section 3.1 and follow the change management requirements of Section 5.3 of Statement of Work to TXDPS 405-xx-xxxxxxx. An approved CO shall set forth the specific services to be performed by (Company Name).

TXDPS Business Division Project Manager (PM) and (Company Name) shall update the following sections of this CO through cooperative negotiations. The Sections, Tables, and format of this CO shall be augmented with information specific to the particular application enhancement. Sections, Tables, and format outlined will not be modified.

**2. Scope**

2.1. *TXDPS requires (Company Name) to provide services related to Application Enhancements and Technology Upgrade / Migration and Transformation. Specific business and functional requirements will include but may not be limited to: hardware (HW) and software (SW) customizations, HW and SW upgrades, programming services, project documentation, and successful testing of each required deliverable(s) identified in this CO. All services provided by (Company Name) shall be in accord with deliverables available through named DIR contracts identified within 405-xx-xxxxxxx.*

2.2. *TXDPS has indentified the following, itemized services to be performed:*

- 2.2.1. \_\_\_\_\_
- 2.2.2. \_\_\_\_\_
- 2.2.3. \_\_\_\_\_

2.3. *(Company Name) shall deliver, through updates to this CO, the project detail necessary to address information commonly found within Implementation Plan, Project Plan, Schedule, and Pricing Quotes for enhancement services related to achieving he identified deliverables. The CO will address the processes, sub-tasks, itemized costs and duration for completion of each deliverable and the Pricing will set the associated cost. Tables 1, 2, 3, and 4 are provided as the tools to clearly itemize all identified deliverables.*

2.3.1. Table 1 - Project Points of Contact and Responsibilities

Organization	Title / Responsibility	Name	Office Phone	Cell Phone	Email Address
TXDPS	Project Sponsor				
TXDPS	Project Manager				
TXDPS	Technical SME - Hardware				
TXDPS	Technical SME - Software				
TXDPS	Technical SME - Data transmission				
TXDPS	Contract Monitor				
TXDPS	Contract Administrator				

Organization	Title / Responsibility	Name	Office Phone	Cell Phone	Email Address
	Relationship Representative				
	Project Manager				
	Programmer				
	DBA				
	HW / SW SME				

## 2.3.2. Table 2 - Project Specific Roles &amp; Responsibility

Table 2 – Roles and Responsibilities Matrix	Micro Assist	TXDPS
Project requirement / dependency #1		
Project requirement / dependency #2		
<b>*primary (P)</b>		

## 2.3.3. Table 3 - Project Schedule

W.O. Ref #	Deliverable Description	Date				Comments
		Due Date	Actual	Test / Review	Acceptance	
2.2.1	“Same info as is provided in section 2.2.x above”					
2.2.2						
2.2.3						

## 2.3.4. Table 4 - Pricing

W.O. Ref #	Deliverable - Description	Service Category / Description (e.g. Programmer) and (Company Name) Employee Name	Qty of Hours	Hourly Rate	Cost Extension
2.2.1	“Same info as is provided in section 2.2.x above”				
2.2.2					
2.2.3					

2.4. Services are not complete until all testing and acceptance is successfully completed as defined in Section 5 of the 405-xx-xxxxxxx, SOW. During the testing and acceptance period, (Company Name) shall capture and document performance issues identified by (Company Name) and / or reported by TXDPS and resolve all HW, SW, and programming defects. Time and materials used to resolve defects will not be billed to TXDPS.

2.5. Final testing and acceptance completion, and all unplanned work to achieve acceptance, will be documented within Table 3 of the final CO version.

2.6. Final acceptance will be memorialized in writing by sign-off of the CO Acceptance Document, Exhibit 2 to this document.

### 3. Risk and Issue Management

*The TXDPS PM shall update Section 3 with any and all pertinent and known risks and issue management items related to the specific application enhancement CO. (Company Name) shall add information as necessary to ensure all possible CO risks and issue management items are clearly addressed during negotiations with the TXDPS Business Division.*

The following general procedures shall be used to manage active CO issues and risks:

- 3.1. *The TXDPS PM shall identify and document project issues (current problems) and risks (potential events that impact the project).*
- 3.2. *The TXDPS PM shall assess, analyze and prioritize the impact and determine the highest priority risks and issues that will be managed actively, according to priority, by (Company Name).*
- 3.3. *(Company Name) shall plan and schedule high-priority risks and issues assigning responsibility for risk management and issue resolution in a documented risk register or issues log, as determined by TXDPS.*
- 3.4. *(Company Name) shall track and report the status of risks and issues, and communicate risk mitigation plans and issue resolutions using the risk register or issue log as determined by TXDPS.*
- 3.5. *The TXDPS PM shall monitor and control the effectiveness of the risk and issue management actions.*
- 3.6. *Active issues and risks shall be monitored and reassessed on a weekly basis by the TXDPS PM and (CompanyName). Mutually agreed upon escalation and risk management processes will be defined at the outset of the CO.*

**4. Service Levels:**

(Company Name) shall meet the following service levels for work performed under this CO. All Service Levels for this CO will meet the same standards as written in the Statement of Work Section 7.

Meantime to Resolution (MTR): Upon verbal or written notification (Company Name) shall provide the following MTR's for defect resolution.

Time and materials applied to fix (Company Name) defects will not be billed to TXDPS.

**5. Required Reporting and Communication:**

(Company Name) shall:

- 5.1. *Create and maintain a Risk and Issues Log if requested by TXDPS.*
- 5.2. *Be accountable for tracking of all technical staff hours and provide a written monthly report due by 5:00 pm CT Monday following the last working day of the month throughout the life of the Change Order reflecting current cost and total Contract usage.*
- 5.3. *Provide one (1) weekly status report and prepare and lead one (1) status meeting per week of no more than one (1) hour in duration, if requested by TXDPS.*
- 5.4. *Attend any required or requested meeting(s) or submit any requested documentation at the discretion of the TXDPS PM.*

**6. Pricing:**

(Company Name) shall identify the specific CO pricing within Table 4 above. In addition (Company Name) shall ensure:

6.1. All CO pricing is provided per a deliverable basis, identifies the Service Category, and identifies the (Company Name) employee providing the work as listed within Attachment A.

6.2. CO pricing will be a fixed / not to exceed cost of (enter total cost here).

**7. Change Order Authorization Signatures:**

\_\_\_\_\_  
TXDPS Business Representative                      Date

\_\_\_\_\_  
(Company Name) Authorized Agent                      Date

\_\_\_\_\_  
TXDPS Contract Administrator                      Date

TXGangs 405-15-R025523 Exhibit 2  
**CHANGE ORDER COMPLETION ACCEPTANCE DOCUMENT**

TEXAS DEPARTMENT OF PUBLIC SAFETY

Section 1. General Information

Contract # \_\_\_\_\_

Change Order Name \_\_\_\_\_

Change Order # \_\_\_\_\_

Section 2. Vendor Acknowledgement of Change Order Completion

*The following project deliverables, as required by Section C Scope of Work and as assigned by Subsection Change Order Plan, have been completed.*

CO Ref. #	Completed Deliverable Description

This is to acknowledge that \_\_\_\_\_ has completed this Change Order project for the Texas Department of Public Safety.

Vendor Approver Name	Title	Signature	Date

Section 3. TXDPS Acceptance of Change Order Completion

This document certifies that the above-referenced services from Change Order Plan # \_\_\_\_\_ have hereby been tested and accepted by the Texas Department of Public Safety.

Upon execution of this acceptance document, an invoice in the amount of \$ \_\_\_\_\_ may be submitted to the Texas Department of Public Safety.

TXDPS Approver Name	Title	Signature	Date



**TEXAS DEPARTMENT OF PUBLIC SAFETY (TXDPS)  
Pricing Request (PR)**

PR OPENING ▶ 1:00 p.m. 06/30/2015

SOLICITATION NO: ▶ 405-15-R025523

FAILURE TO SIGN WILL DISQUALIFY PR

IF NOT  
QUOTING  
DO NOT  
RETURN  
THIS  
FORM.

  
 AUTHORIZED SIGNATURE

08/19/2015  
 DATE

By signing this PR, the Respondent certifies that if a Texas address is shown as the address of the response, the Respondent qualifies as a Texas Bidder as defined in 34 TAC Rule 20.32(68).

<b>AGENCY TO INVOICE</b>
Texas Department of Public Safety Accounting and Budget Control P.O. Box 4087 Austin, Texas 78773-0130 apinvoice@dps.texas.gov
<b>DESTINATION OF GOODS IF DIFFERENT THAN ABOVE</b>
Texas Department of Public Safety 5805 N. Lamar Blvd. Austin, TX 78752

DELIVERY IN <u>1</u> DAYS AFTER RECEIPT OF ORDER (ARO) CASH DISCOUNT <u>   </u> % <u>   </u> DAYS OR NET 30
<b>WHEN QUOTING:</b>
The Vendor shall indicate pricing with an authorized signature on this PR form and fill out all pricing tables or attachments. The Vendor may at its option enclose a separate Quote on its Company letterhead; however, all terms and conditions or deviation language on the Vendor's Quote will not apply to the PR or any awarded Purchase Order (PO).

t VENDOR ADDRESS AND IDENTIFICATION NUMBER t

Vendor Federal VIN#:	_____
Vendor TINS #:	1263464715500
Vendor Name:	CBM Archives Co., LLC
Vendor Address:	1779 Wells Branch Pkwy, #110B-369, Austin
Vendor State:	Texas Zip: 78728
Vendor contact:	Jerry Sanders
Contact Phone #:	361-241-2310 x101

**THIS PRICING REQUEST (PR) SHALL BE SUBMITTED WITH SIGNATURES AND PRICING**

This PR is solicited in accordance with the Department of Information Resources (DIR) Master Contract(s) awarded for the products and services listed below.

LINE ITEM NO.	CLASS & ITEM DESCRIPTION	QUANTITY	UNIT	UNIT PRICE	EXTENSION
001	Application Maintenance and Support - Service Term 09/01/15 - 08/31/16	12	MONTHS	\$32,400	\$388,800
002	Application Maintenance and Support - Renewal Option - Renewal option # 1- 09/01/16 - 08/31/17	12	MONTHS	\$35,700	\$428,400
003	Application Maintenance and Support - Renewal Option - Renewal option # 2- 09/01/17 - 08/31/18	12	MONTHS	\$39,300	\$471,600
004	Application Maintenance and Support - Renewal Option - Renewal option # 3- 09/01/18 - 08/31/19	12	MONTHS	\$43,200	\$518,400

<b>Check below if preference claimed under 34 TAC Rule 20.38</b>	
<input type="checkbox"/> Goods produced or services offered by a Texas bidder that is owned by a Texas resident service-disabled veteran	<input type="checkbox"/> Goods produced or services offered in Texas or offered by a Texas Bidder that is not owned by a Texas resident service-disabled veteran
<input type="checkbox"/> Vendors that meet or exceed air quality standards	<input type="checkbox"/> Energy efficient products
<input type="checkbox"/> Services offered by a Texas bidder that is owned by a Texas resident service-disabled veteran	<input type="checkbox"/> Products and services from economically depressed or blighted areas
<input type="checkbox"/> Recycled or Reused Computer Equipment of Other Manufacturers	<input type="checkbox"/> Products produced at facilities located on formerly contaminated property
<input type="checkbox"/> USA produced supplies, materials, or equipment	<input type="checkbox"/> Products made of recycled, remanufactured, or environmentally sensitive materials including recycled steel

**ORDER OF PRECEDENCE:**

This Contract is comprised of the following documents and in the event of conflict will control in the following order:  
The DIR Master Contract;  
The TXDPS PO with all subsequent Change Orders;  
The TXDPS Pricing Request Terms and Conditions to DIR Vendors, dated 12/10/14, with all attachments.  
The Pricing Request as posted with all Attachments, Exhibits and Appendices; and  
The Vendor's Response.

**DIR MASTER CONTRACT NUMBER:**

The Vendor shall indicate its DIR Master Contract Number: DIR-SDD- 1966

**DELIVERY:**

The Vendor shall include an estimated time of delivery (business days) ARO: 1

**QUANTITIES:**

Enhancement services will be requested on an as needed basis. TXDPS reserves the right to increase or decrease the quantity of the PO at the same original terms and conditions throughout the service term of the PO. The Vendor shall be notified in writing with a fully executed contract modification of any requirements for additional quantities.

**TERM AND RENEWAL OPTIONS:**

This Contract is effective from 9/1/15 through 8/31/16 and may be renewed for up to three (3) additional one (1) year option periods at the same, original terms and conditions and at the same price quoted for each renewal period providing both parties agree in writing prior to the expiration date.

**Scoring Matrix**

Technical Response:	70%
Cost:	30%
Total:	100%

**CONNECTED AGREEMENTS:**

If software subscriptions / End-User Licenses / Maintenance & Support or Warranty agreements are applicable to the requested products, it is the responsibility of the Vendor to provide such licenses / Agreements with the submission of its PR response. Any documents (Vendor's or 3<sup>rd</sup> Party) which are provided at a later date, may not be accepted by TXDPS nor applied to the products and services procured. Any related requirements will be the sole responsibility of the Vendor to include any costs, deliverables, and contractual requirements - TXDPS will have no obligation to any such Terms, Conditions, and / or Requirements. However; TXDPS will receive in full, all functionality identified and necessary as stated in such omitted agreements.

**PR DOCUMENTS to be submitted with the Vendor's Response:**

- PR document with all attachments, exhibits, and addendas
  - PR Attachment A - Service Category pricing by title and individual (as back-up to monthly maintenance and support fees and as back-up to the flat-fee deliverable for each enhancement Change Order).
- PR Attachment B- Pricing Request (PR) Terms and Conditions for DIR Vendors:
  - Appendix A- System Security and Access,
  - Appendix B- System Architecture and IT Requirements.
- PR Attachment C - Statement of Work
  - Appendix A- Cloud Security Alliance's (CSA) Cloud Control Matrix (CCM)
- PR Exhibit 1 - Change Order Template
- PR Exhibit 2- Change Order Completion Acceptance Document

**FINANCIAL RATING:**

The Vendor shall submit a copy of at least one rating from organizations such as Dun & Bradstreet (D&B) Business Information Report or Fitch Ratings. The report shall include the Respondent's Viability Score and the Portfolio Comparison Score or similar ratings. Failure to submit copies of the required financial ratings will result in disqualification.

The Vendor shall provide information and any other financial information reasonably requested by the TXDPS consistent with the services provided by the Contractor or otherwise required by the then applicable TXDPS policies for similar contracts.

**SUBMIT RESPONSES TO:**

Contract Specialist: Luis Blanco  
Phone: 512.424.7626  
Email: luis.blanco@dps.texas.gov

**SUBMIT QUESTIONS AND CLARIFICATION REQUESTS TO:**

The individual listed above may be telephoned or emailed for clarification of the specifications only. No authority is intended or implied that specifications may be amended or alternates accepted prior to the response due date without written approval. **The deadline for Vendors to submit questions in writing is 06/15/2015. TXDPS will respond to the questions in writing on or before 06/19/2015.**

**HISTORICALLY UNDERUTILIZED BUSINESS PARTICIPATION:**

In accordance with Texas Gov't Code §2161.252, each state agency that considers entering into a contract with an expected value of \$100,000 or more over the life of the contract (including any renewals) shall, before the agency solicits bids, proposals, offers, or other applicable expressions of interest, determine whether subcontracting opportunities are probable under this Contract.

**As a Department of Information Resources (DIR) awarded Contractor, your HUB Subcontracting Plan (HSP) included in your contract is the official HSP. All respondents, including State of Texas certified Historically Underutilized Businesses (HUBs) must submit the HSP with their response to the bid solicitation.**

Note: Responses that do not include their official HSP maybe rejected pursuant to Texas Gov't Code 2161.252(b)

If changes are required to your HSP, the Contractor shall seek written approval from the DIR prior to making any modifications to the HSP. An approved modified HSP must be sent to the Department of Public Safety (DPS) if awarded.

**POST-AWARD HSP REQUIREMENTS:** After contract award, the Department may coordinate a post-award meeting with the successful respondent to discuss HSP reporting requirements. The Contractor shall submit the "Prime Contractor Progress Assessment Report" (PAR) to the DPS HUB Office at [DPSHUB@DPS.TEXAS.GOV](mailto:DPSHUB@DPS.TEXAS.GOV) and the Contract Administrator on a monthly basis (by the 5th day of the following month). This monthly report is required as a condition for payment to report to the agency the identity and the amount paid to all subcontractors.

This contract is issued in accordance with DIR Outsourced Deliverables-Based Projects which can be reviewed at <http://dir.texas.gov>.

HUB Subcontracting Plan

UPON MUTUAL CONCURRENCE OF TXDPS AND THE CONTRACTOR, MODIFICATION(S) MAY BE ISSUED FOR ANY CHANGES TO THE PURCHASE ORDER (PO), IDENTIFIED DELIVERABLES, AND / OR SERVICETIME LINES SHALL BE AGREED TO BY BOTH PARTIES IN WRITING. CHANGES SHALL NOT BECOME EFFECTIVE UNTIL OFFICIAL NOTICE IS PROVIDED BY TXDPS PROCURMENT AND CONTRACT SERVICES (P&CS). ANY EQUIPMENT OR SERVICES PROVIDED BY THE CONTRACTOR PRIOR TO AUTHORIZATION WILL BE CONSIDERED A DONATION TO THE AGENCY.

All Possible Employees by Service Category and Name

The following pricing indicates a fixed hourly rate per DIR-SDD-1966\_\_\_\_\_ for ALL Vendor employees that will be or may be involved with Application Maintenance and Support (M&S) AND Application Development and Technology Upgrade/Migration and Transformation (Enhancement). Service Category pricing shall reflect the fixed hourly rate, which extended, shall identified deliverable cost associated with Enhancement deliverables. Please Expand Cells As Needed.

<b>Application Enhancement Employees</b>				
<b>Service Category (Service Description)</b>	<b>Employee Name</b>	<b>MSRP</b>	<b>% off MSRP</b>	<b>Unit Price Hourly Rate</b>
#1 - Analysis, Design, Project Management, Requirements Gathering, Research		\$225	33%	\$150
#2 - Development, Testing		\$225	33%	\$150
#3 - Implementation, Troubleshooting		\$225	33%	\$150
#4 - Documentation, Disaster Planning, Reporting		\$225	33%	\$150
#5 - Training		\$225	33%	\$150
1,2,3,4,5	Jerry Sanders			
1,2,3,4,5	Roy McNett			
2, 4,5	Rudy Hinojosa			
2,4,5	Richard Gonzalez			
2,3,4,5	Daniel Hentshel			
1,2,3,4,5	DPG - Charles Golson			
1,2,3,4,5	DPG - John Turman			
1,2,3,4,5	DPG - Barry Books			
2,3,4,5	DPG - Ken Paris			
2,3,4,5	DPG - Brian Deterling			
2,3,4,5	DPG - Jason Peronne			
2,3,4,5	DPG - Jeffrey Tran			
<b>Application M&amp;S Employees</b>				
<b>Service Category (Service Description)</b>	<b>Employee Name</b>	<b>MSRP</b>	<b>% off MSRP</b>	<b>Unit Price Hourly Rate</b>
#1 - Analysis, Design, Project Management, Requirements Gathering, Research		\$225	33%	\$150
#2 - Development, Modificaton, Testing		\$225	33%	\$150
#3 - Implementation, Troubleshooting		\$225	33%	\$150

All Possible Employees by Service Category and Name

#4 - Documentation, Disaster Planning, Reporting		\$225	33%	\$150
1,2,3,4	Jerry Sanders			
1,2,3,4	Roy McNett			
2, 4	Rudy Hinojosa			
2,4	Richard Gonzalez			
2,3,4	Daniel Hentshel			
1,2,3,4	DPG - Charles Golson			
1,2,3,4	DPG - John Turman			
1,2,3,4	DPG - Barry Books			
1,2,3,4	DPG - Ken Paris			
1,2,3,4	DPG - Brian Deterling			
2,3,4	DPG - Jason Peronne			
2,3,4	DPG - Jeffrey Tran			

**PRICING REQUEST (PR)  
ISSUED BY TXDPS  
TO DIR VENDORS**

1. Vendor understands that TXDPS is a "Customer" under the Vendor's DIR Contract referenced on page 1 of the TXDPS Purchase Order, PO. In submitting information to TXDPS in response to this PR, Vendor affirms its understanding of the General Provisions of the Vendor's DIR Contract (generally located in Section 3) of Appendix A, DIR Standard Terms and Conditions for Deliverables Based Information Technology Services (DBITS) Contracts:
  - A. **Entire Agreement**  
The DIR Contract, Appendices, and Exhibits constitute the entire agreement between DIR and the Vendor. No statement, promise, condition, understanding, inducement or representation, oral or written, expressed or implied, which is not contained in the Contract, Appendices, or its Exhibits shall be binding or valid.
  - B. **Modification of Contract Terms and/or Amendments**
    - 1) The terms and conditions of the DIR Contract shall govern all transactions by Customers under the Contract. The Contract may only be modified or amended upon mutual written agreement of DIR and Vendor.
    - 2) Customers will not have the authority to modify the terms of the Contract; however, additional Customer terms and conditions that do not conflict with the Contract and are acceptable to Vendor may be added in a Purchase Order and given effect. No additional term or condition added in a Purchase Order issued by a Customer can conflict with or diminish a term or condition of the Contract. Pre-printed terms and conditions on any Purchase Order issued by Customer hereunder will have no force and effect. In the event of a conflict between a Customer's Purchase Order and the Contract, the Contract term shall control.
    - 3) Customers and Vendor will negotiate and enter into written agreements regarding statements of work, service level agreements, remedies, acceptance criteria, information confidentiality and security requirements, and other terms specific to their Purchase Orders under the Contract with Vendor.
2. TXDPS issues this PR as Customer under Vendor's DIR Contract and requests that Vendor submit a response to TXDPS based on these additional terms and conditions which TXDPS has determined are specific to the TXDPS PO and are allowable under the provisions of Vendor's DIR Contract, reference Section 1 of this PR.
3. Vendor affirms its understanding that under the DIR DBITS Contract, SOW/PO Issuance clause (generally located in Section 7), Vendor shall respond, in writing, to a Statement of Work (SOW) for services as issued by Customers, consistent with the Terms and Conditions of this Contract in order to be awarded a Purchase Order. Customer SOWs must be complete, signed by an authorized representative of Customer and in the form contained in Attachment C of the Vendor's DIR Contract. Vendor understands that no work under any SOW issued by Customer shall commence until receipt of Purchase Order.
4. **BOX CHECKED IF THIS SECTION 4 APPLICABLE TO THIS PR.     CONFIDENTIALITY AND SECURITY REQUIREMENTS**
  - A. **General Confidentiality Requirements**
    - 1) All information provided by TXDPS or sub-recipients to Vendor or created by Vendor in performing the obligations under this PO is confidential and shall not be used by Vendor or disclosed to any person or entity, unless such use or disclosure is required for Vendor to perform work under this PO.
    - 2) The obligations of this section do not apply to information that Vendor can demonstrate:
      - a. Is publicly available;
      - b. Vendor received from a third party without restriction on disclosure and without breach of contract or other wrongful act;
      - c. Vendor independently developed without regard to the TXDPS confidential information; or
      - d. Is required to be disclosed by law or final order of a court of competent jurisdiction or regulatory authority, provided that Vendor shall furnish prompt written notice of such required disclosure and shall reasonably cooperate with TXDPS at TXDPS' cost and expense, in any effort made by the TXDPS to seek a protection order or other appropriate protection of its confidential information.
    - 3) Vendor shall notify sub-recipient in writing of any unauthorized release of confidential information within two (2) business days of when Vendor knows or should have known of any unauthorized release of confidential information obtained from sub-recipient(s).
    - 4) Vendor shall maintain all confidential information, regardless whether obtained from TXDPS or from sub-recipient(s) in confidence during the term of this PO and after the expiration or earlier termination of this PO.
    - 5) If Vendor has any questions or doubts as to whether particular material or information is confidential information, Vendor shall obtain the prior written approval of TXDPS prior to using, disclosing, or releasing such information.
    - 6) Vendor acknowledges that TXDPS' and sub-recipient'(s) confidential information is unique and valuable, and that TXDPS and sub-recipient(s) may have no adequate remedy at law if Vendor does not comply with its confidentiality obligations under this PO. Therefore, TXDPS shall have the right, in addition to any other rights it may have, to seek in any Travis County court of competent

jurisdiction temporary, preliminary, and permanent injunctive relief to restrain any breach, threatened breach, or otherwise to specifically enforce any confidentiality obligations of Vendor if Vendor fails to perform any of its confidentiality obligations under this PO.

- 7) Vendor shall immediately return to TXDPS all confidential information when this PO terminates, at such earlier time as when the confidential information is no longer required for the performance of this PO or when TXDPS requests that such confidential information be returned.
- 8) Information, documentation and other material in connection with this PO, including the Vendor's Offer, may be subject to public disclosure pursuant to the Texas Government Code, Chapter 552.
- 9) The FBI and TXDPS have computer security requirements. The Vendor's and subcontractor's employees working on this assignment shall sign and submit appropriate agreements and abide by these security requirements, within five (5) calendar days of TXDPS' request.

#### **B. Sensitive Personal Information**

To the extent this subsection does not conflict with the subsection herein entitled "General Confidentiality Requirements," Vendor shall comply with both subsections. To the extent this subsection conflicts with the subsection herein entitled "General Confidentiality Requirements," this subsection entitled "Sensitive Personal Information" controls.

"Sensitive personal information" is defined as follows:

- 1) An individual's first name or first initial and last name in combination with any one or more of the following items, if the name and the items are not encrypted:
  - a. Social security number;
  - b. Driver's license number or government-issued identification number; or
  - c. Account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account; or
- 2) Information that identifies an individual and relates to:
  - a. The physical or mental health or condition of the individual;
  - b. The provision of health care to the individual; or
  - c. Payment for the provision of health care to the individual.
- 3) Sensitive personal information does not include publicly available information that is lawfully made available to the public from the federal government or a state or local government.
- 4) "Breach of system security" is defined as follows: Unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive personal information Vendor maintains under this PO, including data that is encrypted if the Vendor's employee or agent accessing the data has the key required to decrypt the data. Good faith acquisition of sensitive personal information by an employee or agent of Vendor for the purposes of performing under this PO is not a breach of system security unless the employee or agent of Vendor uses or discloses the sensitive personal information in an unauthorized manner.
- 5) Vendor shall implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect from unlawful use or disclosure any sensitive personal information collected or maintained by Vendor under this PO.
- 6) Vendor shall notify TXDPS, any affected sub-recipient and the affected people of any breach of system security immediately after discovering the breach or receiving notification of the breach, if sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person. However, Vendor shall delay providing notice to the affected people and sub-recipients at TXDPS' request, if TXDPS determines that the notification shall impede a criminal investigation. The notification to the affected people shall be made as soon as TXDPS determines that it will not compromise any criminal investigation.
- 7) Vendor shall give notice as follows, at the Vendor's expense:
  - a. Written notice;
  - b. Electronic notice, if the notice is provided in accordance with 15 U.S.C. Section 7001;
  - c. Notice as follows:
    - i. If Vendor demonstrates that the cost of providing notice would exceed \$250,000, the number of affected people exceeds 500,000, or Vendor does not have sufficient contact information for the affected people, Vendor may give notice as follows:
      - Electronic mail, if Vendor has an electronic mail address for the affected people;
      - Conspicuous posting of the notice on the Vendor's website;
      - Notice published in or broadcast on major statewide media; or
    - ii. If Vendor maintains its own notification procedures (as part of an information security policy for the treatment of sensitive personal information) that comply with the timing requirements for notice under this subsection entitled "Sensitive Personal Information," Vendor may provide notice in accordance with that policy.
- 8) If this subsection requires Vendor to notify at one time more than 10,000 people of a breach of system security, Vendor shall also notify, without unreasonable delay, each consumer reporting agency (as defined by 15 U.S.C. Section 1681a) that maintains files on consumers on a nationwide basis, of the timing, distribution, and content of the notices.
- 9) In the event of a breach of system security, if sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person, TXDPS is authorized to assess liquidated damages in the amount of \$1,000.00 per day \_\_\_\_\_ against Vendor for the following damages; however, TXDPS reserves the right to claim actual damages for any damages other than

the following: limited to the initial assessment and review of lost or compromised data. This amount is a reasonable estimate of the damages TXDPS shall suffer as a result of such breach and is enforceable. Vendor will not be responsible and liquidated damages may not be assessed due to a breach of system security caused entirely by someone other than the Vendor, the Vendor's subcontractor, or the Vendor's agent. Any liquidated damages assessed under this Contract may, at TXDPS' option, be deducted from any payments due the Vendor. TXDPS has the right to offset any liquidated damages payable to TXDPS, as specified above, against any payments due to the Vendor. If insufficient payments are available to offset such liquidated damages, then Vendor shall pay to TXDPS any remaining liquidated damages within fifteen (15) calendar days following receipt of written notice of the amount due.

**5. BOX CHECKED IF THIS SECTION 5 APPLICABLE TO THIS PR.  CRIMINAL HISTORY BACKGROUND CHECK:**

- A. Vendor shall have its project personnel – as specifically identified by TXDPS -- submit to TXDPS a fingerprint-based Criminal History Background Investigation, if required by TXDPS, at the Vendor's expense. To facilitate this Criminal History Background Investigation, each person shall complete TXDPS' Vendor Background Information form (HR-22), which shall be provided by TXDPS.
- B. If TXDPS requires a fingerprint-based Criminal History Background Investigation, Vendor will not allow personnel to work on the project who have not successfully completed TXDPS' fingerprint-based Criminal History Background Investigation and who do not otherwise maintain TXDPS' security clearance. TXDPS has the right to prevent the Vendor's personnel from gaining access to TXDPS' building(s) and computer systems if TXDPS determines that such personnel do not pass the background check or fail to otherwise maintain TXDPS security clearance.
- C. When required, the Vendor's Project Manager shall provide the following to TXDPS' Project Manager within 21 calendar days of receiving this PO: a) the completed Vendor Background Information form (HR-22) for all proposed personnel; and b) acceptable fingerprints for all proposed personnel.
- D. Throughout the term of this PO, TXDPS may require Vendor personnel to submit an annual TXDPS fingerprinted-based Criminal History Background Investigation to TXDPS.
- E. Throughout the term of this PO, Vendor shall promptly notify TXDPS of any activity or action by the Vendor's personnel that may affect that individual's ability to continue to work under this PO.

**6. NOTICE:**

Any written notices required under this PO will be by hand delivery to Vendor's office address specified on Page 1 of this PO or by U.S. Mail, certified, return receipt requested, to TXDPS, 5805 N. Lamar Blvd., Austin, Texas 78752. Notice will be effective on receipt by the affected party. Either party may change the designated notice address in this Section by written notification to the other party.

**7. INFORMATION TECHNOLOGY REQUIREMENTS AND STANDARDS:**

Vendor represents and warrants that it shall comply with all technology, security, accessibility, warranty, maintenance, confidentiality, testing and other standards, policies and procedures of TXDPS and the State of Texas that are applicable to Vendor in its performance of this PO as such standards, policies, and procedures are amended by TXDPS or the State throughout the term of this PO, including any renewal or optional periods. The Information Resource Manager designated by TXDPS shall assist Vendor in reviewing these standards, policies and procedures and identifying those that are applicable to Vendor in its performance of this PO. Vendor shall comply with TXDPS standards and requirements wherever they are applicable to this PO. TXDPS shall have the sole right to waive specific requirements if, in its sole judgment doing so would mitigate costs or risks or significantly improve the installed and configured solution. If required for this PR, additional requirements are included as Appendices to this PR.

- A. **System Security and Access**, if required for this PR, this information is provided as Appendix A to this PR.
- B. **System Architecture and TXDPS IT Requirements**, if required for this PR, this information is provided as Appendix B to this PR.

**8. TEXAS PUBLIC INFORMATION ACT:**

The Confidentiality Clause included in Vendor's DIR Contract (generally located in Section 8) of Appendix A, DIR Standard Terms and Conditions for Deliverables Based Information Technology Services (DBITS) Contracts, is modified to include the following sentence. Vendor shall make any information created or exchanged with the state pursuant to this PO, and not otherwise exempted from disclosure under the Texas Public Information Act, available in a format that is accessible by the public at no additional charge to the state. TXDPS requires such information to be available in Arial format.

**9. U.S. DEPARTMENT OF HOMELAND SECURITY'S E-VERIFY SYSTEM**

By entering into this Contract, the Contractor certifies and ensures that it utilizes and will continue to utilize, for the term of this Contract, the U.S. Department of Homeland Security's E-Verify system to determine the eligibility of:

- All persons employed to perform duties within Texas, during the term of the Contract; and
- All persons (including subcontractors) assigned by the Respondent to perform work pursuant to the Contract, within the United States of America.

The Contractor shall provide, upon request of (agency name), an electronic or hardcopy screenshot of the confirmation or tentative non-confirmation screen containing the E-Verify case verification number for attachment to the Form I-9 for the three most recent hires that match the criteria above, by the Contractor, and Contractor's subcontractors, as proof that this provision is being followed.

**If this certification is falsely made, the Contract may be immediately terminated, at the discretion of the state and at no fault to the state, with no prior notification. The Contractor shall also be responsible for the costs of any re-solicitation that the state must undertake to replace the terminated Contract.**

**10. VENDOR AFFIRMATIONS TO TXDPS:**

Signing a response to this PR with a false statement or otherwise providing TXDPS with a false statement is a material breach of contract and shall void this PO, and Vendor shall be removed from all bid lists. During the term of this PO, Vendor shall, for itself and on behalf of its subcontractors, promptly disclose to TXDPS all changes that occur to the foregoing certifications, representations and warranties. Vendor covenants to fully cooperate in the development and execution of resulting documentation necessary to maintain an accurate record of the certifications, representations and warranties. By signature hereon affixed, Vendor hereby certifies that:

- A. Vendor has not given, offered to give, nor intends to give at any time hereafter any economic opportunity, future employment, gift, loan, gratuity, special discount, trip, favor, or service to a public servant in connection with this PO.
- B. The Vendor certifies that it is not currently delinquent in the payment of any franchise tax owed the State of Texas and are not ineligible to receive payment under §231.006(d), Texas Family Code, regarding child support, and that the individual or business entity named in this PO is not ineligible to receive the specified payment and acknowledges that this PO may be terminated and payment may be withheld if this certification is inaccurate. Furthermore, any Vendor subject to §231.006, Gov't Code, shall include names and Social Security numbers of each person with at least 25% ownership of the business entity submitting this PO. This information must be provided prior to award. Enter the Name & Social Security Numbers for each person below:

Name: Mai Chanyarlak	██████████	██████████
Name: Nathan Chanyarlak	██████████	██████████
Name: Jerry D. Sanders Jr.	██████████	██████████

- B. Under §2155.004, Gov't Code, Vendor certifies that the individual or business entity named in this Offer is not ineligible to receive a PO and acknowledges that this PO may be terminated and payment withheld if this certification is inaccurate. §2155.004 prohibits a person or entity from receiving a state contract if they received compensation for participating in preparing the solicitation or specifications for this PO.
- C. As required by §2252.903, Gov't Code, Vendor agrees that any payments due under this PO shall be directly applied towards eliminating any debt or delinquency including, but not limited to, delinquent taxes, delinquent student loan payments, and delinquent child support, until the debt is paid in full. Vendor shall comply with rules adopted by TXDPS under §§403.055, 403.0551, 2252.903, Gov't Code and other applicable laws and regulations regarding satisfaction of debts or delinquencies to the State of Texas.
- D. Pursuant to §669.003, Gov't Code, TXDPS may not issue a PO to a person who employs a current or former executive head of any state agency until four years has passed since that person was the executive head of the state agency. Vendor certifies that it does not employ any person who was the executive head of any state agency in the past four years. If Vendor does employ a person who was the executive head of a state agency, provide the following information:

Name of Former Executive:

\_\_\_\_\_

Name of State Agency:

\_\_\_\_\_

Date of Separation from State Agency:

\_\_\_\_\_

Position with Vendor:

\_\_\_\_\_

Date of Employment with Vendor:

\_\_\_\_\_

- A. In accordance with §2155.4441, Gov't Code, Vendor agrees that during the performance of this PO it shall purchase products and materials produced in Texas when they are available at a price and time comparable to products and materials produced outside this state.

- B. Vendor certifies that the entity and its principals are eligible to participate in this transaction and have not been subjected to suspension, debarment, or similar ineligibility determined by any federal, state or local governmental entity and that Vendor is in compliance with the State of Texas statutes and rules relating to procurement and that Vendor is not listed on the federal government's terrorism watch list as described in Executive Order 13224. Entities ineligible for federal procurement are listed at <http://www.epls.gov>.
- C. Sections 2155.006 and 2261.053, Gov't Code, prohibit state agencies from awarding contracts to any person who, in the past five years, has been convicted of violating a federal law or assessed a penalty in connection with a contract involving relief for Hurricane Rita, Hurricane Katrina, or any other disaster, as defined by §418.004, Gov't Code, occurring after September 24, 2005. Under §2155.006, Gov't Code, Vendor certifies that the individual or business entity named in this PO is not ineligible to receive a PO and acknowledges that this PO may be terminated and payment withheld if this certification is inaccurate.
- D. Vendor represents and warrants that payment to Vendor and the Vendor's receipt of appropriated or other funds under this PO are not prohibited by §556.005 or §556.008, Gov't Code, relating to the prohibition of using state funds for lobbying activities.
- E. Vendor represents and warrants that it has no actual or potential conflicts of interest in providing the requested items to TXDPS under this PO, if any, and that the Vendor's provision of the requested items under this PO, if any, would not reasonably create an appearance of impropriety.
- F. Vendor certifies that it, nor anyone acting for it, has violated the antitrust laws of the United States or the State of Texas, nor communicated directly or indirectly to any competitor or any other person engaged in such line of business for the purpose of obtaining an unfair price advantage.
- G. Vendor certifies that to the best of its knowledge and belief, there are no suits or proceedings pending or threatened against or affecting it, which if determined adversely to it will have a material adverse effect on its ability to fulfill its obligations under this PO.
- H. To the extent applicable to the scope of this PO, Vendor hereby certifies that it is in compliance with Subchapter Y, Chapter 361, Health and Safety Code related to the Computer Equipment Recycling Program and its rules, 30 TAC Chapter 328.
- N. Vendor certifies for itself and its subcontractors that it has identified all current or former, within the last five (5) years, employees of the State of Texas assigned to work on the TXDPS PO 20% or more of their time and has disclosed them to TXDPS and has disclosed or does not employ any relative of a current or former state employee within two (2) degrees of consanguinity, and, if these facts change during the course of this PO, Vendor certifies it shall disclose for itself and on behalf of subcontractors the name and other pertinent information about the employment of current and former employees and their relatives within two (2) degrees of consanguinity.

**APPENDIX A**  
**SYSTEM SECURITY AND ACCESS**

**PRICING REQUEST (PR)**  
**ISSUED BY TXDPS**  
**TO DIR DBITS VENDORS**

**SYSTEM SECURITY AND ACCESS****Information Technology Standards**

The Contractor represents and warrants that it shall comply with all technology, security, accessibility, warranty, maintenance, confidentiality, testing and other standards, policies and procedures of the Department and the State of Texas that are applicable to the Contractor in its performance of this Contract as such standards, policies, and procedures are amended by the Department or the State throughout the term of this Contract, including any renewal or optional periods. The Information Resource Manager designated by the Department shall assist the Contractor in reviewing these standards, policies and procedures and identifying those that are applicable to the Contractor in its performance of this Contract.

**Cloud Security**

The Contractor shall comply with the current Cloud Security Alliance's (CSA) Cloud Control Matrix (CCM) security requirements for Contractor hosted services or applications that are included as part of Contractor's solution. Information pertaining to CSA <https://cloudsecurityalliance.org/> and CCM information may be found at <https://cloudsecurityalliance.org/research/ccm/>.

**User Security**

- A. Account Management: Establish and administer user accounts in accordance with role-based scheme and shall track and monitor role assignment.
- B. Account Management: Automatically audit account creations, modifications, disabling and termination actions with notification to the Department's personnel.
- C. Prevent multiple concurrent active sessions for one user identification.
- D. Enforce a limit of no more than 3 consecutive invalid access attempts by a user.
- E. Automatically lock the account/node for a 15 minute time period unless released by the Department's Administrator.
- F. Prevent further access to the system by initiating a session lock after a maximum of thirty (30) minutes of inactivity, and the session lock shall remain in effect until the user reestablishes access using appropriate identification and authentication procedures.
- G. Ensure all users shall be uniquely identified.
- H. Force users to follow the secure password attributes, below, to authenticate a user's unique ID. The secure password attributes shall:
  - 1) Be a minimum length of twelve characters;
  - 2) Not be a dictionary word or proper name;
  - 3) Not be the same as the User ID;
  - 4) Expire within a maximum of ninety (90) calendar days;
  - 5) Not be identical to the previous ten (10) passwords;
  - 6) Not be transmitted in the clear text outside the secure location;
  - 7) Not be displayed in clear text when entered; and
  - 8) Never be displayed in clear text on the screen.
  - 9) Must contain two number, two symbols, two upper and two lower case characters.

**System Security**

- A. Provide audit logs that enable tracking of activities taking place on the system.
- B. Audit logs must track successful and unsuccessful system log-on attempts.
- C. Audit logs must track successful and unsuccessful attempts to access, create, write, delete or change permission on a user account, file, directory or other system resource.

- D. Audit logs must track successful and unsuccessful attempts to change account passwords.
- E. Audit logs must track successful and unsuccessful actions by privileged accounts.
- F. Audit logs must track successful and unsuccessful attempts for users to access, modify, or destroy the audit log.
- G. Provide the following content to be included with every audited event:
  - 1) Date and time of the event;
  - 2) The component of the information system (e.g. software component, hardware component) where the event occurred;
  - 3) IP address;
  - 4) Type of event;
  - 5) User/subject identity; and
  - 6) Outcome (success or failure) of the event.
- H. Provide real-time alerts to appropriate Department officials in the event of an audit processing failure. Alert recipients and delivery methods must be configurable and manageable by the Department's System Administrators.
- I. Undergo vulnerability scan/penetration testing conducted by the Department or the Texas Department of Information Resources. The Contractor shall remediate legitimate vulnerabilities and system/application shall not be accepted until all vulnerability issues are resolved at no cost to the Department.
- J. Notifications shall display an approved system use notification message or banner before granting access to the system. The notification shall state:
  - 1) Users are accessing a Department system;
  - 2) System usage shall be monitored, recorded and subject to audit;
  - 3) Unauthorized use of the system is prohibited and subject to criminal and civil penalties; and
  - 4) A description of the authorized use of the system.
- K. The Contractor shall implement and use management and maintenance applications and tools, appropriate fraud prevention and detection, and data confidentiality/protection/encryption technologies for endpoints, servers and mobile devices. This must include mechanisms to identify vulnerabilities and apply security patches.
- L. The Contractor shall establish and maintain a continuous security program as part of the Services. The security program must enable the Organization (or its selected third party) to:
  - 1) Define the scope and boundaries, policies, and organizational structure of an information security management system;
  - 2) Conduct periodic risk assessments to identify the specific threats to and vulnerabilities of the Organization due to the Services, subject to the terms, conditions and procedures;
  - 3) Implement appropriate mitigating controls and training programs, and manage resources; and
  - 4) Monitor and test the security program to ensure its effectiveness. The Contractor shall review and adjust the security program in light of any assessed risks.

#### Physical Access Controls

- A. The Contractor shall restrict physical access to the system(s) containing the Department's data to authorized personnel with appropriate clearances and access authorizations.
- B. The Contractor shall enforce physical access authorizations for all physical access points to the facility where information system resides;
- C. The Contractor shall verify individual access authorizations before granting access to the facility containing the information system;
- D. The Contractor shall control entry to the facility containing the information system using physical access devices and guards; and
- E. The Contractor shall change combinations and keys when keys are lost, combinations are compromised, or individuals are transferred or terminated.
- F. The Department and the Contractor shall collaborate on security monitoring and incident response, define points of contact on both sides, establish monitoring and response procedures, set escalation thresholds, and conduct training. The Contractor shall, at the

request of the Department or, in the absence of any request from the Department, at least quarterly, provide the department with a report of the incidents that it has identified and taken measures to resolve.

### Data Security

- A. If the Contractor or any subcontractors require access to the Department's network; the Department's data; or the network processing, transporting, or storing of the Department's data (may at the Department's discretion), the Contractor shall be required to sign the CJIS Security Addendum, and all of the Contractor's employees requiring access to the Department's network shall sign the FBI Certification to the CJIS Security Addendum and complete a fingerprint based background check.
- B. The Contractor's solution shall protect against an employee falsely denying having performed a particular action (non-repudiation).
- C. Require the Contractor, subcontractor, and their staff to obtain and provide proof of PII certifications for its employees accessing the Department's data at the request of the Department.
- D. Comply with relevant federal and state statutes and rules, and the Department's policies, and standards, including but not limited to CJIS requirements.
- E. Data shall not be exported to an external location without the permission of the Department.
- F. In the event of any impermissible disclosure, loss or destruction of Confidential Information, the receiving Party must immediately notify the disclosing Party and take all reasonable steps to mitigate any potential harm or further disclosure, loss or destruction of such Confidential Information.

### Encryption

The system shall protect the confidentiality of the Department's information. All data transmitted outside or stored outside the secure network shall be encrypted. When cryptography (encryption) is employed within information systems, the system shall perform all cryptographic operations using Federal Information Processing Standard (FIPS) PUB140-2 validated cryptographic modules with approved modes of operation. The system shall produce, control, and distribute symmetric cryptographic keys using NIST-approved key management technology and processes. The key management process is subject to audit by the Department. Bcrypt shall be used to mitigate against brute force attacks.

- A. Wireless: The following requirements specifies the minimum set of security measures required on WLAN-enabled portable electronic devices (PEDs) that transmit, receive, process, or store PII or confidential information:
  - 1) Personal Firewall: WLAN-enabled PED shall use personal firewalls or run a Mobile Device Management system that facilitates the ability to provide firewall services.
  - 2) Anti-Virus Software: Anti-virus software shall be used on wireless ECMS-capable PEDs or run a Mobile Device Management System that facilitates the ability to provide anti-virus services.
  - 3) Encryption of PII or confidential data-in-transit via WLAN-enabled PEDs, systems and technologies will be implemented in a manner that protects the data end-to-end. All systems components within a WLAN that wirelessly transmit PII or confidential information shall have cryptographic functionality that is validated under the National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program as meeting requirements per Federal Information Processing Standards (FIPS) Publication 140-2. Encryption shall be a minimum of 128 bit.
  - 4) Data-at-Rest: Data at rest encryption shall be implemented in a manner that protects PII and confidential information stored on WLAN enabled PEDs by requiring that the PED must be powered on and credentials successfully authenticated in order for the data to be deciphered. Data-at-rest encryption shall include the encryption of individual files, portions of the file system (e.g., directories or partitions), or the entire drive (e.g. hard disks, on-board memory cards, memory expansion cards). In recognition of the increased risk of unauthorized access to PII or confidential information in the event that a PED is lost or stolen and the inherently mobile nature of these devices, encryption shall be provided for data-at-rest on all WLAN enabled PEDs that is validated as meeting FIPS 140-2.
  - 5) WLAN Infrastructure: WLAN infrastructure systems may be composed of either stand-alone (autonomous) access points (AP) or thin APS that are centrally controlled by a WLAN controller.
  - 6) Validated Physical Security: APs used in the WLANS should not be installed in unprotected environments due to an increased risk of tampering and/or theft.
- B. Mobile Device Management Requirement. Mobile Device Management (MDM) facilitates the implementation of sound security controls for mobile devices and allows for centralized oversight of configuration control, application usage, and device protection and recovery. MDM shall include the following core features:
  - 1) The ability to push security policies to managed devices;
  - 2) The ability to query the device for its configuration information;
  - 3) The ability to modify device configuration as required;
  - 4) Security functionality that ensures the authenticity and integrity of the transaction in the three categories above;

- 5) Asset management (track/enable/disable) mobile devices being managed via the MDM server;
- 6) The ability to manage proxy access to network resources via the connection of the mobile device to the MDM server;
- 7) The ability to query devices being managed on the status of security policy compliance and to implement a specified mediation function based on compliance status;
- 8) The ability to download and store mobile device audit records;
- 9) The ability to receive alerts and other notifications from managed mobile devices;
- 10) The ability to receive alerts and other notifications from managed mobile devices;
- 11) The ability to generate audit record reports from mobile device audit records; and
- 12) Application management (application white list) for applications installed on managed mobile devices.

#### **Secure Erasure Of Hard Disk Capability**

All equipment provided to the Department by the Contractor that is equipped with hard disk drives (i.e. computers, telephones, printers, fax machines, scanners, multifunction devices, etc.) shall have the capability to securely erase data written to the hard drive prior to final disposition of such equipment, either at the end of the equipment's useful life or the end of the related services agreement for such equipment, in accordance with 1 TAC §202.

#### **Data Center Location Requirements**

The data center must be located in the continental United States of America.

#### **Access to Internal Department Network and Systems**

As a condition of gaining remote access to any internal Department network and systems, the Contractor shall comply with Department policies and procedures. The Department's remote access request procedures shall require the Contractor to submit a Remote Access Request form for the Department's review and approval.

- A. Remote access technologies provided by the Contractor shall be approved by the Department's CISO.
- B. Individuals who are provided with access to the Department network may be required to attend or review the Department's Security Awareness Training on an annual basis.
- C. The Contractor shall secure its own connected systems in a manner consistent with Department requirements.
- D. The Department reserves the right to audit the security measures in effect on the Contractor's connected systems without prior warning.
- E. The Department also reserves the right to immediately terminate network and system connections not meeting such requirements.

#### **FBI CJIS Security Addendum**

The Contractor shall execute an originally signed CJIS Security Addendum which can be downloaded from <http://www.txdps.state.tx.us/securityreview>. Additionally, a CJIS Security Addendum Certification shall be signed by each employee performing duties related to this project prior to final Contract award. Each original Certification shall include an original signature of the employee and the Contractor's representative. Non-compliance by Respondent will be cause for termination of contract negotiations and the Department may elect to enter into negotiations with the next highest evaluated Offer.

#### **Criminal History Background Checks**

- A. The Contractor shall have its project personnel submit to the Department a fingerprint-based Criminal History Background Investigation, if required by the Department, at the Contractor's expense. To facilitate this Criminal History Background Investigation, each person shall complete the Department's Vendor Background Information form (HR-22), which shall be provided by the Department.
- B. If the Department requires a fingerprint-based Criminal History Background Investigation, the Contractor shall not allow personnel to work on the project who have not successfully completed the Department's fingerprint-based Criminal History Background Investigation and who do not otherwise maintain the Department's security clearance. The Department has the right to prevent the Contractor's personnel from gaining access to the Department's building(s) and computer systems if the Department determines that such personnel do not pass the background check or fail to otherwise maintain the Department security clearance.

- C. When required, the Contractor's Project Manager shall provide the following to the Departments Project Manager within 10 calendar days of executing this Contract:
- 1) the completed Vendor Background Information form (HR-22) for all proposed personnel; and acceptable fingerprints for all proposed personnel.
  - 2) Throughout the term of this Contract, the Department may require the Contractor personnel to submit an annual Department fingerprinted-based Criminal History Background Investigation to the Department.
  - 3) Throughout the term of this Contract, the Contractor shall promptly notify the Department of any activity or action by the Contractor's personnel that may affect that individual's ability to continue to work under this Contract

#### Department Information Protection Policies, Standards & Guidelines

- A. Contractor, its employees, and any subcontractors shall comply with all applicable Department Information Protection Policies, Standards & Guidelines and any other Department requirements that relate to the protection or disclosure of Department Information. Department Information includes all data and information
- 1) submitted to Contractor by or on behalf of the Department,
  - 2) obtained, developed, produced by the Contractor in connection with this Contract,
  - 3) communicated verbally whether intentionally or unintentionally, or
  - 4) to which the Contractor has access in connection with the services provided under this Contract.
- B. Such Department Information may include taxpayer, vendor, and other state agency data held by the Department.
- C. As used herein, the terms "Sensitive" and "Confidential" information shall have the meanings set forth in the Department's Information Protection Policies, Standards & Guidelines.
- D. All waiver requests shall be processed in accordance with the Department's Information Protection Policies, Standards & Guidelines Waiver Policy.
- E. The Department reserves the right to audit the Contractor's compliance with the Department's Information Protection Policies, Standards & Guidelines
- F. The Department reserves the right to take appropriate action to protect the Department's network and information including the immediate termination of system access.
- G. The Contractor shall ensure that any confidential Department Information in the custody of the Contractor is properly sanitized or destroyed when the information is no longer required to be retained by the Department or the Contractor in accordance with this Contract.
- H. Electronic media used for storing any confidential Department Information shall be sanitized by clearing, purging or destroying in accordance with NIST Special Publication 800-88 Guidelines for Media Sanitization. The Contractor shall maintain a record documenting the removal and completion of all sanitization procedures with the following information:
- 1) Date and time of sanitization/destruction,
  - 2) Description of the item(s) and serial number(s) if applicable,
  - 3) Inventory number(s), and
  - 4) Procedures and tools used for sanitization/destruction.
- I. No later than sixty (60) days from contract expiration or termination or as otherwise specified in this Contract, the Contractor shall complete the sanitization and destruction of the data and provide to the Department all sanitization documentation.

#### Disclosure of Security Breach

Without limitation on any other provision of this Contract regarding information security or security breaches, the Contractor shall provide notice to the Department's Project Manager and the CISO as soon as possible following the Department's discovery or reasonable belief that there has been unauthorized exposure, access, disclosure, compromise, or loss of sensitive or confidential Department information ("Security Incident").

- A. Within twenty-four (24) hours of the discovery or reasonable belief of a Security Incident, the Contractor shall provide a written report to the CISO detailing the circumstances of the incident, which includes at a minimum:
- 1) A description of the nature of the Security Incident;
  - 2) The type of Department information involved;
  - 3) Who may have obtained the Department information;

- 4) What steps the Contractor has taken or shall take to investigate the Security Incident;
  - 5) What steps the Contractor has taken or shall take to mitigate any negative effect of the Security Incident; and
  - 6) A point of contact for additional information.
- B. Each day thereafter until the investigation is complete, the Contractor shall provide the CISO with a written report regarding the status of the investigation and the following additional information as it becomes available:
- 1) Who is known or suspected to have gained unauthorized access to the Department's information;
  - 2) Whether there is any knowledge if the Department information has been abused or compromised;
  - 3) What additional steps the Contractor has taken or shall take to investigate the Security Incident;
  - 4) What steps the Contractor has taken or shall take to mitigate any negative effect of the Security Incident; and
  - 5) What corrective action the Contractor has taken or shall take to prevent future similar unauthorized use or disclosure.
- C. The Contractor shall confer with the CISO regarding the proper course of the investigation and risk mitigation. The Department reserves the right to conduct an independent investigation of any Security Incident, and should the Department choose to do so, the Contractor shall cooperate fully by making resources, personnel, and systems access available to the Department and the Department's authorized representative(s).
- D. Subject to review and approval of the CISO, the Contractor shall, at its own cost, provide notice that satisfies the requirements of applicable law to individuals whose personal, confidential, or privileged data were compromised or likely compromised as a result of the Security Incident. If the Department, in its sole discretion, elects to send its own separate notice, then all costs associated with preparing and providing notice shall be reimbursed to the Department by the Contractor. If the Contractor does not reimburse such costs within thirty (30) calendar days of the Department's written request, the Department shall have the right to collect such costs.

#### Cyber Insurance Requirement

The Contractor will maintain sufficient cyber insurance to cover any and all losses, security breaches, privacy breaches, unauthorized distributions, or releases or uses of any data transferred to or accessed by Contractor under or as a result of this Contract.

- A. This insurance shall provide sufficient coverage(s) for the Contractor, the Department, and affected third parties for the review, repair, notification, remediation and other response to such events, including but not limited to, breaches or similar incidents under Chapter 521, Texas Business and Commerce Code.
- B. The Department may, in its sole discretion, confer with the Texas Department of Insurance to review such coverage(s) prior to approving them as acceptable under this Contract.
- C. The Contractor shall obtain modified coverage(s) as reasonably requested by the Department within ten (10) calendar days of the Contractor's receipt of such request from the Department.

#### Representations And Warranties Related To Software

If any software is provided under this Contract, the Contractor represents and warrants each of the following:

- A. The Contractor has sufficient right, title, and interest in the Software to grant the license required.
- B. Contract terms and conditions included in any "clickwrap", "browsewrap", "shrinkwrap", or other license agreement that accompanies any Software, including but not limited to Software Updates, Software Patch/Fix, or Software Upgrades, provided under this Contract are void and have no effect unless the Department specifically agrees to each licensure term in this Contract.
- C. The Software provided under this Contract does not infringe upon or constitute a misuse or misappropriation of any patent, trademark, copyright, trade secret or other proprietary right;
- D. Software and any Software Updates, Software Maintenance, Software Patch/Fix, and Software Upgrades provided under this Contract shall not contain viruses, malware, spyware, key logger, back door or other covert communications, or any computer code intentionally designed to disrupt, disable, harm, or otherwise impede in any manner, including aesthetical disruptions or distortions, the operation of the computer program, or any other associated software, firmware, hardware, or computer system, (including local area or wide-area networks), in a manner not intended by its creator(s); and
- E. Software provided under this Contract does not and will not contain any computer code that would disable the Software 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 mechanism (sometimes referred to as "time bombs", "time locks", or

“drop dead” devices) or that would permit the Contractor to access the Software to cause such disablement or impairment (sometimes referred to as “trap door” devices”).

**Rights to Data, Documents and Computer Software (State Ownership)**

- A. Any biographic data, demographic data, image data inclusive of fingerprints, photograph and signatures or any other data or metadata in any form acquired or accessed by the Contractor in the performance of its obligations under this Contract shall be the exclusive property of the State of Texas and all such data shall be delivered to the Department by the Contractor upon completion, termination, or cancellation of this Contract.
- B. The Contractor shall not use, willingly allow, or cause to have such data used for any purpose other than the performance of the Contractor’s obligations under this Contract without the prior written consent of the Department.
- C. The ownership rights described herein shall include, but not be limited to, the right to copy, publish, display, transfer, prepare derivative works, or otherwise use the works.
- d. The Contractor shall provide, at no additional charge, appropriate licenses for the Department to use and access, as necessary for the Department to use and access the turnkey solution during the term of the lease, the Contractor’s pre-existing software or other intellectual or proprietary property that the Contractor determines is necessary to facilitate the performance of the Contractor’s obligations under this Contract.

**APPENDIX B**  
**SYSTEM ARCHITECTURE AND IT REQUIREMENTS**

**PRICING REQUEST (PR)**  
**ISSUED BY TXDPS**  
**TO DIR DBITS VENDORS**

**INFORMATION TECHNOLOGY (IT) REQUIREMENTS**

The Contractor shall comply with the following standards and requirements wherever they are applicable to this Contract. The Department shall have the sole right to waive specific requirements if in its sole judgment doing so would mitigate costs or risks or significantly improve the installed and configured solution.

**Environment Standards**

The COTS Software shall be hosted within Contractor's computing infrastructure or within the Departments' IT infrastructure. The Contractor shall provide a complete hardware and software inventory including any servers required, an architectural diagram, security diagram, network diagram, network usage assessment, and communications port diagram of the complete overall system and narrative describing requested diagrams and any API and Web service components, and the recommended workstation configuration if any. The Contractor shall also itemize all assumed capabilities and minimum hardware and software requirements of any Department IT related systems required to access or support contractor's product or system. The Respondent must provide copies of the 508 compliance VPAT documentation for all components of the proposed system.

A. Contractor Hosted COTS Software:

1. Any applicable server hardware shall identify:
  - a. The processor requirements;
  - b. The memory requirements;
  - c. Operating system details and dependencies; and
  - d. Data storage requirements.
2. All workstation recommendations shall identify:
  - a. The processor requirements;
  - b. Display requirements;
  - c. The memory requirements;
  - d. Operating system details and dependencies;
  - e. Data storage requirements; and
  - f. Any support applications required such as Internet Explorer, Adobe PDF Reader etc.
3. Peripherals required:
  - a. Printers;
  - b. Scanners; and
  - c. Fax.

- B. The Respondents system must support the following
- a. DPS issued desktop or laptop PCs:
    - i. Windows 7
    - ii. Internet Explorer 8 or greater
    - iii. Firefox 27 or greater
  - b. DPS issued Mobile Devices
    - i. IOS version 7 or greater
    - ii. iPhone 4s or greater
    - iii. iPad 3 or greater
  - c. Publicly owned desktop or laptops PCs
    - i. Windows 7 or greater
    - ii. Mac OS X 10.6.8 or greater

- iii. Internet Explorer 8 or greater
- iv. Safari 10.6.4 or greater
- v. Firefox 27 or greater
- d. Publicly owned mobile devices, phones and tablets
  - i. Using IOS 7 or greater
  - ii. Using Android 4.1 or greater

C. The Department Hosted COTS Software:

The Contractor shall follow the Department's hosting standards for any software and hardware that is hosted within the Department Data Centers. The Contractor hosted software and hardware are not required to meet these requirements. However, the Contractor hosted software and hardware shall meet these standards prior to migrating from the Contractor hosted to the Department hosted.

The existing Department infrastructure framework supports several industry standard products and platforms. The Contractor shall identify the products required to properly support the contracted solution.

1. The Contractor shall identify:
  - a. Required hardware platforms and operating system to support the proposed solution:
    - i. The processor requirements;
    - ii. The memory requirements;
    - iii. Operating system details and dependencies; and
    - iv. Data storage requirements.
  - b. Required application server platforms:
    - i. The processor requirements;
    - ii. The memory requirements;
    - iii. Operating system details and dependencies; and
    - iv. Data storage requirements.
  - c. Required web server platforms:
    - v. The processor requirements;
    - vi. The memory requirements;
    - vii. Operating system details and dependencies; and
    - viii. Data storage requirements.
  - d. Any required support services such as email servers etc.:
    - ix. The processor requirements;
    - x. The memory requirements;
    - xi. Operating system details and dependencies; and
    - xii. Data storage requirements.
2. The Department's IT infrastructure only allows the following database platforms:
  - a. Contractor SQL Server 2012
  - b. DB2 9.7.2 on Distributed (AIX and LINUX)
  - c. Oracle on a case by case basis
3. The Department's IT infrastructure report services are supported with Crystal Reports.

### Communication Standards

The COTS Software shall support integration with other Department systems utilizing standard web services or provide API tools that can be incorporated into the Department's applications or secure file transfer protocol with data encryption.

### Network Topography

- A. The Department utilizes a combination of public and private TCP/IP network resources. All internal communications between client resources, other systems, and system services shall be through this network.
- B. The Respondent shall include in its Offer an estimate on the amount of bandwidth or formulas to calculate usage required to support the number of expected internal DPS Users and volume of work. The Offer must also provide information on how they will provide adequate network capacity for DPS Users and External Users.
- C. The Respondents system use standard TCP/IP network access ports. The system must be accessible on Port 80 for standard Web Browser access and Port 443 for Secure Web Browser support.

#### **Workstation installed software**

If the software solution is client based and needs to be installed on each computer, the Contractor shall provide the client software in a MSI format so that the install can be packaged to operate as a silent install for Windows based systems. OS X applications must support Apple Application installation package standards. Any software required for mobile devices must be available from the appropriate App store based on the device operating system. Mobile device software must also be compatible with Mobile Device Management software distribution tools.

#### **MAINTENANCE AND SUPPORT**

##### **Contractor Hosted COTS Software Services**

The Contractor shall provide COTS Software that includes and may not be limited to all hardware and software maintenance and support, upgrades to equipment to meet and maintain performance service levels, backup hardware and Internet connections in accordance within Section C.11.1, Cloud Security.

##### **Department Hosted COTS Software**

The Contractor shall provide a software maintenance solution to include, but may not be limited to provide:

- A. Support for the COTS Software to include software changes that the Contractor develops for the Department under this Contract shall be managed through the Service Level Agreement.
- B. Preventative scheduled and unscheduled system diagnosis and correction of faults as well as modification of the software to maintain the service level performance of the COTS Software.
- C. Web-based support portal for the Department to report minor problems shall be available twenty-four (24) hours per day, seven (7) days per week, and three-hundred-sixty-five (365) days a year with a searchable knowledge base for known issues. Response to reported problems shall be managed as defined in the Service Level Agreement.
- D. Maintenance services to resolve usability problems to include but may not be limited to bugs, security issues, and installation of software updates and major software releases.
- E. New software versions or releases at no additional cost to the Department occurring in the normal maintenance yearly support as Offered in Section B.2, Pricing Schedules.

##### **Software Updates**

The Contractor shall provide periodic system software updates that shall incorporate corrections of any defects, and enhancements to the system's software.

- A. COTS Software updates released by the Contractor shall be installed by the Contractor during periods during the maintenance window mutually agreed upon by the Department and the Contractor as defined in the Service Level Agreements.
- B. Updates to Documentation or manuals resulting from system software updates shall be provided or made available on demand to the Department.

##### **Hardware**

- A. The Contractor shall provide maintenance services for hardware equipment owned by the Contractor installed to support a Contractor's Hosted COTS Software.

- B. The Contractor shall provide notice to the Department a minimum of five (5) business days prior to scheduled maintenance including length of anticipated downtime plus the description or purpose of scheduled maintenance. The Contractor shall provide notice to The Department and employees prior to unscheduled maintenance where possible including length of anticipated downtime plus the description or purpose of unscheduled maintenance.

1. Preventive Maintenance

The Contractor shall provide preventive maintenance services in order to maintain the system in good condition and working order on a mutually agreeable scheduled basis. The preventive maintenance schedule is to be based on the Contractor's and the Departments' mutual agreement of the particular service required for each system component, it being understood that this schedule shall be oriented to avoid periods when the system is expected to have the heaviest use.

During the term of this Contract, the Department may, by providing five (5) calendar days prior written notice, select any alternative period of maintenance coverage whether or not such alternative represents an increase or decrease in service.

2. Remedial Maintenance

The Contractor shall provide remedial maintenance to the system on a twenty-four (24) hour per day, seven (7) day per week basis, with a response time of no more than one (1) hour for each incident.

### SERVICE OUTAGE ESCALATION AND COMMUNICATION

The Contractor shall provide a detailed communication plan that specifies how the Contractor shall be contacted in the event of a system outage. If the solution is hosted by the Contractor, the Contractor shall provide its notification and escalation process as part of the communication plan.

### SERVICE LEVEL STANDARDS

The purpose of these Service Level Standards is to ensure that the proper elements are in place to provide the Department employees with the optimal level of system performance. The Service Level Standards define the terms, conditions, requirements, responsibilities, and obligations of the Department, employees, and the Contractor.

#### System Production Control

The Contractor shall schedule production management such as batch processing, job scheduling, automated import/exports, etc. at a minimum of once every twenty-four (24) hours, seven (7) days per week and three hundred sixty-five (365) days per year. The production control schedule shall be mutually agreed upon by both the Contractor and the Department and shall be oriented around periods when the system is expected to have the lightest use.

#### System Support

The Contractor shall support all software licensed to the Department for use during the term of this Contract. The Contractor shall provide toll-free telephone, or e-mail accessibility to the Department for the system, Monday through Friday, 8:00 a.m. to 6:00 p.m., Central Time, excluding State or federal holidays. A list of the Departments holiday schedule is available upon request. These days and times may change at the discretion of the Department. The Contractor shall provide the capability for the Department and employees to leave a message for occasions outside of that time period.

A. System support for the Department and employees includes responsibilities such as:

1. New Department or employee training;
2. System configuration;
3. Record contribution methodologies or practices;
4. System navigation;
5. Data query or export procedures;
6. Search criteria, best practices, parameters, etc.; and
7. Troubleshooting for system hardware, system software, network, etc.

B. System support for the Department and employee excludes responsibilities such as:

1. Record content;

2. Record quality;
3. Record interpretation;
4. Employee administration (including new accounts, password creation or resets);
5. Non-system software owned, purchased, installed, developed or utilized by the Department or the Department's hardware; and
6. The Departments/User's ISP or other internal method of access.

## System Performance

### Basic Requirements

#### A. Basic Requirements

In addition to the office hours uptime requirements, as defined in Section C.16.2.3, System Rate Calculation, the Contractor agrees to maintain optimal system performance twenty-four (24) hours per day, seven (7) days per week, three hundred sixty-five (365) days per year at a rate of 99.5% (hereafter referred to as the "Rate") as calculated by Rate Calculation below. The Contractor is cautioned to quickly resolve the source or sources of failure. Inability to meet or exceed the Rate in any twelve (12) month period may at the Department's sole discretion result in the following actions:

1. First Remedy: Verbal warning.
2. Second Remedy: Written warning added to the Contract File Folder as stated in accordance with Section H.3, Further Opportunity to Cure, of this Contract.
3. Continuing Remedy: The Department may consider exercising the Contract remedies, which may include termination as stated in accordance with Section H.4, Termination, of this Contract.

### Rate of Calculation

#### B. Rate Calculation

The Contractor shall measure the rate of system performance by the amount of downtime during a calendar month. This metric gauges the system performance as a percentage of available hours tracked to the quarter of an hour (rounded). The rate of system performance shall be measured and monitored as follows:

Available hours equal total number of hours in a month (24 hours x number of days in the month) minus the actual amount of time spent to the quarter of an hour for scheduled maintenance for the hosted application.

Downtime is the total number of hours (rounded to the quarter hour) during which the solution is not in operation.

System Performance Rate equals available hours Downtime divided by available hours.

**Example** for the month of January:

Available time per month was 744 hours (31 days X 24 hours)

Downtime per month was 3.75 hours (start 1:00 am - end 4:40 am)

$744.00 - 3.75 = 740.25$

$740.25 \div 744 = 99.5\%$

### Reports

For Vendor hosted solutions, the Vendor shall report both system performance Rate and average Response Time of the system by 5:00 pm CST Monday following the last business day of the month throughout the life of an active Change Order. Reports may be made available through the system or distributed to the Department's Contract Monitor.

### Data Backups

The Vendor or system shall perform backups on all system Records once every twenty-four (24) hours, seven (7) days per week, and three hundred sixty-five (365) days per year to facilitate data and system restoration in the event of any failures, including but not limited to, hardware. The data backup schedule shall be mutually agreed upon by both the Vendor and the Department and shall be oriented around periods when the system is expected to have the lightest use.

### Contact Persons

The Vendor's point of contact for maintenance and service levels shall be the Division and ITD Project Managers. The Departments' primary point of contact shall be the Departments' Contract Administrator in accordance with this Contract in Section {X}, Contract Administrator.

- A. The vendor will comply with the Disaster Recovery Plan.

**Hardware and Software Refresh**

The Vendor shall provide hardware and software refresh plans to address end of support or end of life products. The plan shall also address system and application patches and implementation methodology and schedule. Refresh of hardware and software will be at the sole discretion of the Department.

**ADA Compliance**

The Respondent represents and warrants that it will comply with the requirements of the Americans with Disabilities Act (ADA).

**TESTING REQUIREMENTS, IMPLEMENTATION AND ACCEPTANCE**

All testing activities shall include the following but not be limited to:

**Implementation and Acceptance**

TXDPS will work closely with the Respondent to insure each phase of this project is complete; however, completion of any one phase specified in this RFO does not constitute full completion and acceptance of the project's requirements.

**Unit Testing:**

- A. Respondent shall provide a listing of test cases based on the requirements of this solicitation, the Implementation Plan, Project Plan and Schedule and in direct coordination with TXDPS Project Manager.
- B. Respondent shall also provide TXDPS with the results of the Unit test cases that were executed to completion.
- C. Based on the outcome of successful unit testing, Respondent shall advance to the next step of System Testing. Successful unit testing shall be defined as 100% pass rate of all defined unit test cases with no outstanding issues/defects. Respondent shall perform all these tests in a development environment.

**System Testing:**

- A. Respondent shall provide to TXDPS for review and approval by TXDPS QA testing staff, documented test cases that shall be performed during Respondent system testing to validate the successful migration and installation of the software package before any System Testing begins.
- B. Respondent shall be responsible for performing system testing in the Respondent QA Environment and provide test results to TXDPS.
- C. Respondent shall log all defects found during the System Testing in the agreed upon defect tracking application.
- D. Respondent shall investigate any defects found during System Testing and participate in Defect Triage meetings with TXDPS to determine defect outcome and resolution.
- E. Respondent shall provide defect fixes in the timeframe as defined in SLA.
- F. Respondent shall demonstrate all components of the Application Software are performing as defined in the System Test cases and Business Requirements, including interfaces with other systems (Baseline Interfaces), in the specified System Hardware, Operating Software and Network Environment (System Environment).

**Performance/Load Testing:**

Performance/Load Testing will be performed by TXDPS in coordination with the Respondent in instances where internal metrics (network load, etc.) cannot be captured by the Respondent. TXDPS will also help coordinate internal resources to provide oversight and assistance when necessary.

- A. Respondent shall provide documented test cases to TXDPS that shall be performed during Respondent performance and load testing to validate the successful performance of the software package.
- B. Respondent shall capture the average data throughput for solution and the maximum number of concurrent users before service degradation to ensure user traffic does not have an adverse effect the TXDPS network and provide these results to TXDPS.
- C. Respondent shall be responsible for conducting performance and load testing that will demonstrate their system is capable of meeting metrics as defined by TXDPS.

- D. Respondent shall provide performance and load test results to TXDPS for review and approval.
- E. Based on the outcome of successful performance and load testing, Respondent shall advance to the next step of System Integration Testing. Successful performance testing shall be defined as 100% pass rate of all defined test cases with no outstanding issues/defects. Respondent shall perform all these tests in a production-like environment.

**Integration Testing:**

TXDPS shall perform System Integration Testing independently or jointly with the Respondent, following successful completion and documentation of Respondent and TXDPS System Testing. Successful completion is defined as 100% pass rate of all defined System Test cases with no outstanding issues/defects.

- A. Respondent shall provide assistance during the System Integration Testing process by providing technical and QA resources that will answer questions and provide clarifications and/or fixes to any issues encountered during the System Integration Testing cycle. This support can be performed remotely or in person at the TXDPS facility. Remote support shall consist of, but is not limited to, remote server control mechanisms, WebEx review sessions, telephone conference calls and email exchanges. System Integration Testing will focus on the integration and interaction with other TXDPS systems, external systems, or third party components and shall be based on the TXDPS requirements as well as the Respondent System Design Specification.
- B. The vendor must provide a User Acceptance Testing environment upon successful completion of System Integration Testing.
- C. TXDPS shall log all defects found during the System Integration Testing in the agreed upon defect tracking application.
- D. Respondent shall investigate any defects and participate in Defect Triage meetings with TXDPS to determine defect outcome and resolution.
- E. Respondent shall provide a documented response to the documented defect in the agreed upon defect tracking application.
- F. Respondent shall provide defect fixes in the timeframe as defined in SLA.
- G. Respondent shall provide Release Notes containing an open issues log for each test iteration.
- H. At TXDPS' sole discretion, test cases may be modified or added to ensure completeness, accuracy and quality of the delivered software package as defined in business and technical documentation.
- I. Based on the successful outcome of System Integration Testing, TXDPS shall advance to User Acceptance Testing (UAT). Successful System Integration Testing shall be defined in the Test Plan documentation created by TXDPS.
- J. System Integration testing shall not be considered successful if outstanding Severity one (1) or Severity two (2) defects pending resolution remain.

**User Acceptance Testing (UAT):**

- A. Following successful completion of the System Integration Testing, or System Test for Contractor Hosted systems, TXDPS shall coordinate and execute UAT in the Contractor's (UAT) environment.
- B. UAT shall be performed by TXDPS end users based on UAT test cases created by TXDPS.
- C. TXDPS shall notify Respondent of any defects found during User Acceptance Testing of the Software Solution.
- D. Respondent shall investigate any defects and participate in Defect Triage meetings with TXDPS to determine defect outcome and resolution.
- E. Respondent shall provide defect fixes in the timeframe as defined in the SLA.
- F. If the number of defect failures prevents all systems from operating as described above, the TXDPS may reject the entire final software package.
- G. If all criteria is not met as defined in the TXDPS Quality Assurance Entry and Exit Criteria document (Exhibit ##), or the respondent's solution does not meet the defined business requirements, the TXDPS may reject the final software solution.

**Final Acceptance:**

Final acceptance of the Software Solution shall not occur until ninety (90) business days after the review period, to include thirty (30) days failure free operation of the system and delivery of all required documentation.

**Failure Resolution:**

Upon failure of any test within the control of the Respondent shall submit a report describing the nature of the failure and the actions to be taken to remedy the situation prior to any modification or replacement of the system, within ten (10) business days. TXDPS shall provide written approval or denial within five (5) business days. If a system requires modification, the fault shall be corrected and the test repeated until successfully completed.

- A. Major discrepancies that will substantially delay receipt and acceptance of the system shall be sufficient cause for rejection of the system. Failure to satisfy the requirements of any test is considered a defect and the system shall be subject to rejection by TXDPS. Any rejected software package may be offered again for retest provided all noncompliance has been corrected.
- B. Resolution of System Integration Test Failure. If the software package fails the System Integration Test, Respondent shall correct the fault and then TXDPS will repeat the Systems Integration Test until successfully completed.
- C. Resolution of Final Acceptance Test Failure. If a defect within the system is detected during the Final Acceptance Test, TXDPS shall document the failure. Respondent will be required to research, document and correct the source of failure. Once corrective measures are taken, TXDPS shall monitor the point of failure until a consecutive thirty (30) calendar day period free of defects is achieved.

**Retest**

Respondent and TXDPS shall mutually agree to re-test per C.17 Testing Requirements, Implementation, and Acceptance, as determined by the environment where the issue is to be addressed. If the system downtime exceeds seventy-two (72) hours or system has not operated for thirty (30) consecutive days free of defects within the ninety (90) day period, TXDPS may extend the test period by an amount of time equal to the greater of the downtime in excess of seventy-two (72) hours or the number of days required to complete the performance requirement of an individual point of failure.

**DEPARTMENT RECORDS AND DATA RETENTION**

- A. Upon conclusion of this Contract, including management transition to the Department or another Contractor, all agency data and reports and the complete, certified set of fully, properly documented, and commented application programming files and logs developed by the Contractor specifically for this Contract shall revert to the Department. This shall include customized code, data and images, data and images indices, data and image indexing or analysis, and logging tools and information not present in Contractor's product as normally initially delivered to other clients.
- B. Agency records shall be labeled and delivered in a manner satisfactory to the Department. The Contractor shall comply with additional instructions pertaining to Department records as detailed in Section H.55, Books and Records, of this Contract.
- C. In the event the Contractor requires copies of any records after conclusion of this Contract or this Contract's expiration and Facility management transition, the Department shall furnish copies to the Contractor at the Contractor's expense.
- D. Records shall be maintained in accordance with the Department's Records Retention Schedule as detailed in Section E.2, Inspection by State Employees.

**Attachment C**

**STATEMENT OF WORK**

**FOR**

**A Pricing Request (PR)**

**TITLE**

**TXDPS Texas Gang Intelligence Index (TX Gang)**

**TECHNOLOGY CATEGORIES**

***Deliverables Based Information Technology Services (DBITS)***

*Application Development*

*Technology Upgrade/Migration and Transformation*

*Application Maintenance and Support*

**DIR Vendor Name**

CBM Archives Co., LLC

**DIR Vendor Contract Numbers (list all applicable DIR Master Contract Numbers)**

**DIR-SDD- 1966**

**Date Issued: 6/09/15**

**Response must be received on or before 6/30/2015 by 1:00 P.M.**

## 1. Introduction

TXDPS issues this Statement of Work (SOW) under this PR number 405-15-R012836 for services under the Department of Information (DIR) Deliverables Based Information Technology (DBITS) Master Contracts for a TXDPS Crime Records Service (CRS) application.

Chapter 61 of the Texas Code of Criminal Procedure mandates that the TXDPS create and maintain a statewide gang intelligence database operated in accordance with Title 28 of the Code of Federal Regulations Chapter 23. This database is provided at no cost to law enforcement and criminal justice agencies throughout Texas for the purposes of maintaining a central gang intelligence source. Any law enforcement agency collecting gang intelligence in Texas, any sheriff's office in a county with a population of greater than 100,000, and any police department jurisdiction with a population of more than 50,000 are required to submit gang data to the TXDPS-provided gang database. The database was officially created in 1999 as the Texas Gang Intelligence Index ("TX Gang" or "the System"), and has been through three major iterations in that time, each of which has had an increase in participation and scope. TX Gang has become, and is continuing to grow as, a major resource in both the Texas and national gang intelligence communities. Currently, the Crime Records Service (CRS) of the Law Enforcement Support (LES) division oversees and maintains the database.

TX Gang serves as an effective investigative, analytical, and statistical criminal investigative resource by providing the tools necessary to identify, relate, and track gangs, gang members, and their activities and by allowing for the sharing of data across multiple local, state, and national jurisdictions. The primary objectives of TX Gang are receipt, storage, and sharing of essential criminal investigative information related to gangs and gang members. It is the intent of TXDPS to issue a Purchase Order (PO) for maintenance and support tasks, and accompanying Change Orders for application development needs as identified.

## 2. Scope - Technical Environment and Identified Application Enhancement Projects

- A. The Vendor shall provide continuous maintenance services for the TXDPS' TX Gang related software utilized by the TXDPS for the System to include, but not be limited to, preventive and remedial maintenance and enhancement services for upgrades, refreshes, enhancements, customization, test and acceptance, and other related services.
- B. The Vendor's services for the System shall be an open solution to allow for customization and enhancements to meet all CJIS security requirements.
- C. Enhancement services: The TXDPS will assign and then issue Change Order Plan(s) as incorporated in Exhibit I, Change Order Template, for additional services to include but not be limited to customization, enhancements, and other related services. The Contract Monitor shall work with the Vendor to prepare the COP(s). The Contract Monitor shall submit a requisition to Procurement and Contract Services to finalize the modification to this Contract.

Examples of factors requiring application enhancement include but are not limited to:

- Open Records Requests
- Mandated Legislative Changes

405-15-R025523  
Attachment C - SOW  
TXDPS Texas Gang Intelligence Index (TX Gang)  
Application Development, Maintenance & Support,  
Technology Upgrade/Migration and Transformation

- FBI Program Specific Changes through its Technical Operational Update documents
- FBI Audit
- TXDPS Audit
- TXDPS Administrative Mandates
- TXDPS Internal Data Aggregation Mandates (Web Services)
- TXDPS IT and Infrastructure Design Mandates
- TXDPS CRS Tertiary Programs (Texas Crime Information Center / National Crime Information Center / Texas Law Enforcement Telecommunications System)
- Oversight board requirements

The Vendor shall provide continual application development and support services through enhancements and software updates plus support services contracted through its DIR Master Contract. Support services shall include:

- System analysis
- Scope assessment
- Specification development
- Programming
- Web based services
- Data import and export processes
- Interfaces
- System Infrastructure
- Report generation
- Testing and quality assurance
- Implementation
- Documentation of new features and functionality
- Technical support
- Database design
- Support code framework ensuring the system meets all compliance requirements with Title 1 Texas Administrative Code chapters 206 and 213
- 24x7x365 maintenance of the System
- Maintenance and patching of software
- Preventative and routine maintenance to include but not be limited to patching of servers and other relevant commercial software such as Microsoft SQL Server

## 2.1 Technical Environment

**2.1.1 Software Environment:** Operating System(s): Red Hat Enterprise Linux Server release 5.4;  
Application Server: Tomcat 7.0.23

**2.1.2 Hardware:** Cisco UCS Server (production); Cisco UCS Server (development/test)

**2.1.3 Database Environment:** DB2 v9.7.0.2 and any subsequent releases

**2.1.4 Programming Languages:** Java 1.6.0\_2; stored procedures (see database environment); JavaScript; Tapestry 5.1

**2.1.5 User accessibility:** will be on a 24x7x365 basis, with at least 99.5% availability via approved platforms. Web based access will be available regardless of user platform, but at a minimum will support all common browser configurations.

**2.1.6 Data throughput:** Data transmitted from TX Gang will meet NIEM 2.1 standards with an anticipated upgrade to 3.0 within twelve (12) calendar months of its release. Future iterations of the NIEM standard will also be supported.

## **2.2. Application Development and / or Enhancement Change Orders**

Application development or technology upgrade/migration and transformation tasks will be governed by issuing task specific Change Orders (Exhibit 1). Each Change Order will be negotiated and agreed to by both parties. Change Orders will be officiated by signatures of the Vendor, the TXDPS Division's Contract Monitor (CM) or assigned designee, requesting the work, and the TXDPS Procurement & Contract Services (P&CS) Contract Administrator, and will be incorporated into this Contract. The TXDPS CM or assigned designee will initiate this process by providing the Vendor with a draft Change Order for update and negotiations. Once the TXDPS CM or assigned designee and the Vendor have determined and agreed to all deliverables and updated the draft Change Order accordingly, the draft Change Order will be forwarded to the TXDPS Contract Administrator for scope and pricing verification. Once all identified groups concur, the TXDPS Contract Administrator will facilitate final signatures to incorporate the Change Order into this Contract. No work is authorized without an approved and executed Change Order as provided to the Vendor by the TXDPS Contract Administrator.

### **2.2.1 Change Order Format and Methodology**

The format of the Change Order will not be altered by either the TXDPS Division CM or assigned designee or the Vendor. The TXDPS Division CM or assigned designee and the Vendor shall only update applicable deliverable language, provide pertinent project information and background necessary to explain the project tasks and scope, and update all Change Order tables as the project progresses.

Change Orders will be issued for any and all application customizations, updates, and/or modifications, to include but not be limited to: alterations of software, programming, documentation, and other applications or services beyond those originally stated within this SOW for standard maintenance and hosting requirements as detailed within this Contract.

## **3. Maintenance and Support Requirements**

The Vendor shall provide maintenance and support for the TX Gang application will need to meet the following criteria. Please refer to Section 7 of this SOW for service level requirements.

### **3.1 Application Hosting Requirements for Vendor Hosted Applications**

The Vendor shall comply with all Terms and Conditions of this Contract and shall:

405-15-R025523  
Attachment C - SOW  
TXDPS Texas Gang Intelligence Index (TX Gang)  
Application Development, Maintenance & Support,  
Technology Upgrade/Migration and Transformation

- Provide each application with a separate test and redundant production environment to mitigate application downtime.
- Allow an unlimited number of unique remote Administrator Access Users for the production and test environments for each application.
- Provide TXDPS Administrator Access Users capabilities to maximize administration of each application, including but not limited to the creation, modification, and removal of users, groups, and roles and permissions management.
- Coordinate and obtain written approval from the TXDPS' Project Manager for requirements necessary to providing and maintain the Administrator roles-based accounts. The Vendor shall ensure accounts meet TXDPS standards.
- Provide web based access to all applications by users and Administrator Access Users.
- Provide web-based access independent of user platform, but at a minimum, support Internet Explorer 8, other common web browsers, and common mobile devices to include, but not be limited to, iPhone, iPad, Android, and IOS devices.
- Ensure user access to applications support web based protocols and not require a fat client for system administration and / or user operations.
- Provide data archiving to comply with statutory requirements as defined in the State Library requirements and the TXDPS Records Retention schedule.
- Provide full and indelible audit logs as requested by TXDPS for all operations performed within each application to include, but not be limited to, compliance with the most up to date version of the CJIS Security Policy, including auditing, accountability, access control, identification and authentication. Reference Section 12.1 of this SOW for CJIS details and Section 13 of this SOW for documentation required with the PR response.
- Include data security features within each application that protect the security and privacy of personally identifiable information (PII) and which comply with the storage and dissemination of reports involving juveniles, victims, suspects, and sex-offenders as required by statute.
- Ensure, and provide documentation within its PR response, that all applications comply with the current Cloud Security Alliance's (CSA) Cloud Control Matrix (CCM) security requirements for Vendor hosted applications. Information pertaining to CSA <https://cloudsecurityalliance.org/> and CCM information may be found at <https://cloudsecurityalliance.org/research/ccm/>.
- Provide an updated hardware (HW) and software (SW) inventory as changes are made, including any servers and network technology required and, as requested by TXDPS, an architectural diagram of the complete overall system, to demonstrate compliance with CSA CCM, and provide specific detail related to:
  - a. the processor requirements;
  - b. the memory requirements;
  - c. operating system details and dependencies; and
  - d. data storage requirements.

### 3.2 Data Backups

The Vendor shall perform backups of all applications daily, for the term of this Contract.

- 3.2.1** The data backups will be performed at a mutually agreed upon time outside the hours of 8:00 A.M. to 5:00 P.M. CT. Exceptions to this schedule require prior written consent from the TXDPS CM. The TXDPS CM will have one (1) business day to respond to exception requests.

- 3.2.2 Automatic notification of backup failures will be sent to the application TXDPS' Project Manager.
- 3.2.3 The Vendor shall perform backups on all applications and application data once every twenty-four (24) hours, seven (7) days per week, and three hundred sixty-five (365) days per year to facilitate data and system restoration in the event of any failures, including but not limited to hardware or network.
- 3.2.4 The daily data backup general operation start time shall be mutually agreed to by both the Vendor and TXDPS and will be oriented around periods when the system is expected to have the lightest use. The Vendor shall ensure no more than twenty-four (24) hours of data are at risk.
- 3.2.5 The Vendor shall ensure data and application backups allow for the complete recovery of data and application functionality up to the point of failure.
- 3.2.6 Data backup failures will be reported via email to the TXDPS' Project Manager within one (1) hour of failure.
- 3.2.7 Data backup failures will be reported on the monthly incident report.

### 3.3 Hosting Center Disaster Recovery and Disaster Recovery Plan

The Vendor shall author and design a Disaster Recovery Plan (DRP) for each hosted application.

- 3.3.1 The Vendor shall update the DRP for any enhancement.
- 3.3.2 DRP will be approved by the TXDPS IT Division, TXDPS Cyber Security, the TXDPS Division requesting the enhancement, and the TXDPS Procurement and Contract Services (P&CS) Contract Administrator. Final acceptance of the DRP will be communicated from the Contract Administrator to the Vendor via email.
- 3.3.3 The Disaster Recovery (DR) solution will reside at a secondary location.
- 3.3.4 The DRP will be reviewed and updated every six (6) months to ensure the plan reflects current priorities, processes, and execution strategies.
- 3.3.5 The Vendor shall provide its proposed DRP to the TXDPS Contract Administrator within fifteen (15) calendar days of Contract award. 3.3.6 The Vendor and TXDPS shall negotiate and agree on the initial DRP within thirty (30) calendar days of awarded of this Contract.
- 3.3.7 The Vendor and TXDPS shall negotiate and agree on the updated DRPs within ten (10) business days of submission.
- 3.3.8 **The Recovery Time Objective (RTO) is seven (7) days. The Recovery Point Objective (RPO) is less than 30 minutes. The RTO is the targeted duration of time and a service level within which a business process must be restored after a disaster (or disruption) in order to avoid unacceptable consequences associated with a break in business continuity. An RPO is defined by business continuity planning. It is the maximum targeted period in which data might be lost from an IT service due to a major incident.**

### 3.4 Transition Plan/Procedures

The Vendor, with the assistance of TXDPS, as part of the application maintenance and support requirements, shall provide a detailed plan for transitioning all applications, data, software, and documentation ("Application Data"), in whole or part, to a subsequent Vendor, TXDPS or other entity. The Vendor shall update the

405-15-R025523  
Attachment C - SOW  
TXDPS Texas Gang Intelligence Index (TX Gang)  
Application Development, Maintenance & Support,  
Technology Upgrade/Migration and Transformation

Transition Plan within fifteen (15) calendar days following any enhancement work that alters application or system design.

The Vendor shall provide, within its Offer, a detailed draft transition plan ("Transition Plan") for a ninety (90) calendar day transition period that meets industry and best practices standards and will include, at a minimum, step by step processes, timelines, involved parties' responsibilities, knowledge transfer, training and functional requirements to ensure that transition of all Application Data includes without limitation:

- Detail of all hardware (if applicable) and associated operating software requirements necessary to support all applications.
- Detail of all platform and development software necessary to support, maintain and administer all application test, application production, and application monitoring environments.
- Detail of all network hardware (if applicable) and software necessary to support, maintain and monitor all application test, application production, and application monitoring environments.
- Detail to ensure all Application Data can integrate with other TXDPS or other identified entities' systems utilizing standard web services, or provide application program interface (API) tools that can be incorporated into TXDPS or other identified entities' applications or secure file transfer protocol with data encryption.

The Vendor shall provide to TXDPS a finalized Transition Plan within thirty (30) calendar days of Contract award. TXDPS shall review the Transition Plan within fifteen (15) calendar days of submission, and shall discuss any issues, requirements or concerns with the Vendor.

As directed by TXDPS as a result of such discussions, the Vendor shall modify the Transition Plan and return the Plan to TXDPS for review and written acceptance within fifteen (15) calendar days of receipt. The fifteen (15) business day cycle, at a maximum, shall continue between TXDPS and the Vendor until it is determined the Transition Plan achieves TXDPS' satisfaction. Upon determining that the Transition Plan meets the requirements of this Contract including these provisions, TXDPS shall notify the Vendor of its written acceptance of the Transition Plan and upon such written acceptance, the Transition Plan shall be incorporated by reference into this Contract. Notice to the Vendor will be provided by the Contract Administrator via email.

TXDPS shall ensure cooperation on the part of any subsequent Vendor, other entity or TXDPS personnel, depending on the entity to which TXDPS directs that all or part of this Contract shall be transitioned; however, the Vendor shall maintain all responsibility for all tasks, deliverables and performances under this Contract during the transition period. At the end of the ninety (90) day transition period, or earlier depending on TXDPS approvals, the subsequent Vendor, other entity or TXDPS shall assume full responsibility for all tasks, deliverables and performances as directed by TXDPS.

During this Contract term, additional revisions of the Transition Plan may be required due to information, processes or issues that originally were not included or addressed in the Transition Plan. Revisions to the Transition Plan shall be processed under the same procedures as the initial Transition Plan, including provision to TXDPS for review, comment, revision, written acceptance, and incorporation into this Contract. Any enhancement activities that alter application or system design shall necessitate an update to the Transition Plan.

Knowledge transfer shall occur over the entirety of the 90-day transition period. The knowledge transfer shall take place via various methods. The Vendor shall, at a minimum, coordinate and conduct two (2) formal classroom training sessions. These sessions shall focus on the specific Transition Plan requirements and any other tasks or activities identified by the Vendor and TXDPS as needed to ensure a successful transition of

technology necessary to continue applications operations. Training sessions shall be completed no later than sixty (60) calendar days prior to the end of the transition period. The Vendor, TXDPS and the subsequent Vendor or other entity shall meet a minimum of once per week to determine if further training or knowledge transfer is required.

TXDPS shall meet with the Vendor and the subsequent Vendor or other entity to ensure all concerns and issues have been met and addressed appropriately. TXDPS shall make the determination, in its discretion, of when the transition is complete and shall provide the Vendor and the subsequent Vendor or other entity with formal written acceptance indicating such transfer of responsibilities. The formal transfer of duties shall be documented, in writing, on a TXDPS Contract Modification or Contract Amendment, to include acceptance signatures from TXDPS, the Vendor and the subsequent Vendor or other entity.

Activation of the Transition Plan approved by TXDPS under these provisions (the beginning of the ninety (90) day transition period), will begin on the Vendor's receipt of written notification from TXDPS that this Contract, in whole or in part, is being transitioned. The Vendor shall comply with these provisions and the Transition Plan. The Vendor's failure to comply with these provisions and the Transition Plan shall constitute a material breach of this Contract.

### **3.5 Software Maintenance and Support for TXDPS Owned/Hosted Applications**

The Vendor shall provide all SW maintenance and support, to meet and maintain performance service levels. Maintenance of TX Gang will include Preventative Maintenance, Remedial Maintenance and Special Maintenance as defined herein: The Vendor shall provide the following:

Maintenance, support, or implementation for existing interfaces or TXDPS required future interfaces.

Maintenance and support for all existing database features.

Provide users with a method of contacting one another within the database.

Visibility of documenting officer, entering user, and user that performs the most recent validation of the record to TX Gang users

The means to notify users of fundamental database transactions, including but not limited to additions, modifications, deletions, expirations, views, subscriptions, or other similar data changes.

Relational ties within the database for comparison of similar records.

Provide and support methods for all types of reports current to the system as well as future reports requested by the TXDPS.

Maintain up to date knowledge of the existing data set rules required for export to NCIC, TCIC, and any other TXDPS resource required.

Assurance that the database is maintained in full compliance with all applicable government laws, rules, procedures, and statutes.

Support for external agencies wishing to contribute data to TX Gang via one-time data migration or

ongoing batch upload. Support shall consist of coordinating with agencies to provide transfer specifications, field matching, and automated report emails.

Full and indelible audit logs as requested by TXDPS for all operations performed within the database to include but not be limited to compliance with the most up to date version of the CJIS Security Policy including auditing, accountability, access, control, identification and authentication.

Means for participating agencies to export their own data either en masse or singularly to both an analysis software program as well as a spreadsheet format.

Data archiving to comply with statutory requirements and TXDPS Records Retention Schedules

Assurance that records that have met legislatively mandated expiration dates are not retained past their legally mandated expiration dates by programmatically removing such records from the active record database

Provide system edits to verify the validity of a record during the life of the record, from creation to expiration

Provide a user management component that will allow local users to manage their own users (resetting passwords, etc.), as well as, provide the ability for Administrators to create and manage user accounts statewide

The Vendor will supply to TXDPS all necessary reference manuals, sample data, source documents, and any other information required to perform maintenance.

### **3.6 Preventive Maintenance**

The Vendor shall provide preventive maintenance services in order to maintain the System in good condition and working order on a mutually agreeable scheduled basis. The preventive maintenance schedule is to be based on the Vendor and TXDPS CM or assigned designee mutual agreement of the particular service required for each system component, it being understood that this schedule will be oriented around periods when the System is expected to have the lightest use and outside of the PRINCIPAL PERIOD OF OPERATION.

The PRINCIPAL PERIOD OF OPERATION coverage is Monday through Friday during the hours of 8:00 a.m. to 6:00 p.m. CST, excluding state or federal holidays.

The Vendor shall:

- A. Provide an advance notice reminder to the TXDPS' Project Manager or assigned designee at least five (5) calendar days prior to scheduled preventive maintenance activities for those activities that impact System operation.
- B. Provide the TXDPS' Project Manager or designee with email or phone notice of unscheduled preventive maintenance activities and receive approval from the TXDPS prior to services being rendered.
- C. Provide installation of patches and upgrades of all application and operating system software associated with the System, with written preauthorization of the TXDPS to keep current with FBI

CJIS and TXDPS IT Division standards. Updates to manuals resulting from System software updates will be supplied to the TXDPS free of charge.

- D. Install, without charge outside Principal Period of Operation, all mandatory changes with written preauthorization from the TXDPS.
- E. Replace faulty, malfunctioning, or end-of-life System software to maintain the current level of System functionality and operational effectiveness.

Cost for preventive maintenance services will be included in the predetermined monthly maintenance cost.

### **3.7 Remedial Maintenance**

Remedial Maintenance is defined as maintenance performed during System component failure that is performed by the Vendor on an unscheduled basis.

The Vendor shall:

- A. Provide all necessary maintenance at no cost to the TXDPS to remedy malfunctioning system hardware or software to regain full operability.
- B. If the TXDPS gives notice to the Vendor of a System failure, notification shall be considered approval to provide remedial maintenance. If the Vendor discovers a System failure, the Vendor shall notify the TXDPS according to the terms defined in the Service Level Agreement. The Vendor shall follow Critical Blocker procedures defined in the Service Level Agreement for instances of remedial maintenance.
- C. Produce a notification banner for users attempting to access the faulty System. Such notification banner shall indicate the System is down and will show an estimated time of System availability. The Vendor shall update the banner hourly, providing the current status and estimated time of System availability.

### **3.8 System Modifications and Enhancements**

System modifications and/or enhancements shall be performed by the Vendor outside the scope of Preventive or Remedial Maintenance. These activities will include but not be limited to customization, enhancements or other related services.

The Vendor shall:

- A. Perform modifications/enhancements as requested by the TXDPS if the service to be rendered is less than three (3) hours, at no additional cost to the TXDPS. Coordination of the requested services will be mutually agreed upon in writing prior to services being rendered.
- B. Complete a Change Order Plan (COP) issued by the TXDPS.
  - 1. Provide modification/enhancement services that are estimated to exceed three (3) hours by the issuance of a COP utilizing Exhibit 1, Change Order template.
  - 2. Properly fill out the COP to include the specific areas added or changed by the TXDPS. Areas may include Work Breakdown Structure ("WBS"), delivery dates, responsibilities and other critical information necessary for the services to be rendered.

3. Upon approval and signatures from the Vendor and the TXDPS PM, the COP will be forwarded to the Contract Monitor, who will secure approval and issuance from the Contract Administrator. The Contract Administrator will not approve and issue the COP until such time as all appropriate TXDPS signatories have reviewed and approved the COP request. After all signatories have reviewed and approved the COP, the Contract Administrator will initiate a Contract modification. A Contract modification is required for all COPs. No services will be rendered until the Vendor receives an approved COP from the Contract Administrator with all appropriate TXDPS signatures.
  4. Ensure all services are within scope of this Contract and have been requested at the sole discretion of the TXDPS.
  5. Abide by the terms and conditions within this Contract and not add any contractual terms and conditions to the COP.
- C. Repair defects enumerated in the COP caused by the following: acts of God; the TXDPS or its designated agent or users; neglect; misuse or abuse of the System; or use of non-recommended products or services.

### **3.9 Software Support**

The Vendor shall:

- Provide 24 x 7 x 365 monitoring of all support software necessary to administer all applications per stated SLAs.
- Provide routine patching and upgrades of all software that directly or indirectly impacts application production availability to maintain compliance with software manufacturer's versioning requirements and TXDPS IT Division standards.
  - Identify all (both reported and non-reported) software issues within one (1) hour of occurrence.
  - Begin remediation of all (both reported and non-reported) issues within one (1) hour of identification.
  - If the issue cannot be resolved in the stated timeframe, the Vendor shall contact, via email communication, the TXDPS Information Technology Division Operations Intelligence Center (ITD OIC): 1-888-377-6420 and designated TXDPS CM or assigned designee assigned to the specific application.
- Support response times and ticket detail will be submitted to the TXDPS CM or assigned designee or assigned designee with each month's per application, incident report.

### **3.10 Application, Software, Network Infrastructure Support Requirements**

The Vendor shall:

- Identify and notify TXDPS of all software, and network technology issues that arise within all dependent and independent components of all applications and technology infrastructure.
- Track software and networking issues and identify each incident via a unique designation identifier. The incident ticket will provide all information and documentation as required within Section 6.
- Assign a severity level to each incident. Severity level scale is detailed within Section 7 of this SOW.
- Report all issues encountered to the TXDPS ITD OIC, provide severity level, root cause, and estimated resolution time.

- Provide a monthly summary of all incident tickets encountered while providing application maintenance and support.
- Provide software refresh plans to address end of support or end of life products. The plans shall also address application patches and implementation methodology and proposed deployment schedules.

### **3.11 Maintenance Responsibilities of TXDPS**

#### **3.11.1 Notification**

TXDPS shall notify the Vendor's designated contact immediately upon discovery of system failure and shall permit the Vendor prompt and unfettered access to the system. TXDPS shall provide the Vendor use of necessary data communications facilities and equipment at no charge to Vendor subject only to TXDPS security regulations.

#### **3.11.2 Vendor Office and Storage**

TXDPS may provide the Vendor with a work area at no charge. The Vendor shall, at a minimum, supply field engineering materials, devices, and aids necessary to maintain the system in good working order.

#### **3.11.3 Authorized Support**

TXDPS personnel will not attempt any repair or maintenance on the System while the System is covered by this SOW unless previously agreed upon in writing by the Vendor as part of normal operator maintenance responsibilities. TXDPS will not request or allow any individual other than the Vendor's support personnel or TXDPS employees specifically approved to make any adjustment, repair or maintenance.

#### **3.11.4 Maintenance Personnel**

Depending upon the availability of TXDPS manpower and the practicability for TXDPS to do so, TXDPS will assign a person or persons (TXDPS employee(s) specifically approved) to coordinate all maintenance activities and to work with the Vendor. The Vendor shall work with said person(s). TXDPS shall bear all responsibility for any actions performed by the TXDPS employee(s), which were not directed by or requested by or under the control of the Vendor. The Vendor shall bear all responsibility for activities performed by all of its employees. Some TXDPS employees will be considered under the direction of the Vendor (for training purposes). The Vendor shall bear final responsibility for control of any TXDPS employees in training or placed under the Vendor's direction as specified by SLA(s) or separate Contract provisions. Depending upon the availability of TXDPS manpower and the practicability for TXDPS to do so, TXDPS will assign competent, trained personnel to cooperate with the Vendor. Should the Vendor feel any recommended TXDPS employee is not performing or able to perform the duties necessary for training or as specified by SLA(s) or separate contract the Vendor must submit its concerns in writing to the designated TXDPS CM or assigned designee. TXDPS personnel will be available for consultation and to answer pertinent questions as specified in the SLA.

### **4. Outsourced Services**

The prime Vendor shall ensure any subcontractors working under this Contract comply with all Contract Requirements.

## **5. Deliverable Receipt, Acceptance and Change Management**

### **5.1 Application Development or Enhancement Test, Acceptance, and Receipt.**

- All deliverables will be provided on the dates specified in each uniquely identified and approved Change Order.
- All deliverables will have a testing period of ten (10) calendar days, with acceptance contingent upon five (5) calendar days of error free operation.
- If test and acceptance is not achieved by the tenth business day, the testing period will continue until achievement of test requirements and acceptance by TXDPS. The Vendor will not be paid for any additional work provided to achieve deliverable acceptance beyond the quantity of hours originally agreed upon within the signed Change Order. If successful testing and acceptance of the identified deliverable is not achieved, payment will not be provided.
- If the deliverable cannot be provided within the agreed upon and scheduled timeframe, the Vendor is required to contact the TXDPS CM or assigned designee, per the Change Management Requirements below.

Beyond the test and acceptance period, all deliverables will have up to a ninety (90) day post-launch production quality validation period. The TXDPS CM or assigned designee and the Vendor shall monitor application performance for stability and validate that deliverables meet current and projected performance requirements. Post-launch production validation will be considered complete when both parties sign the Change Order Acceptance Form (Exhibit 2)

### **5.2 Application Maintenance and Support Acceptance and Receipt.**

The TXDPS PM or assigned designee will review the monthly summary of incident reports during the first week of each following month. If all incidents were addressed within the time frames, the TXDPS PM or assigned designee will certify all maintenance and support activities were provided within the stated requirements

### **5.3 Change Management**

- Any changes to the Change Order delivery dates shall be reviewed and approved by the TXDPS CM or assigned designee before being placed in effect.
- The Vendor's request for a revised schedule shall include the impact on: related and/or dependent tasks, overall project, resolution methodology for correcting deficiencies, and change to specific and overall timeframes.
- TXDPS shall document changes to delivery dates by the update of Change Order governance table(s) by the TXDPS CM or assigned designee and provide such documentation to the Vendor PM or assigned designee.
- Any administrative or substantive requirement changes to this SOW shall be approved by both parties in writing and documented by a TXDPS Modification of Contract form. TXDPS or the Vendor PM or assigned designee shall initiate the change process by notifying the other party in writing; email is acceptable, and by submitting a written Change Order signed by both parties, to TXDPS Contract Administrator. No work is to begin until Change Order is executed by Procurement and Contract Services.

The Vendor is hereby advised that changes to the Software Solution system will be subject to the TXDPS' Change Control Board (CCB) process. This requirement is mandatory for the Vendor hosted and the TXDPS hosted packages. The TXDPS shall initiate and manage the change control process. The purpose of the TXDPS' IT Change Management (ITCM) is to ensure that Change Requests (CRs) to the TXDPS' IT systems are properly reviewed, authorized, implemented and tracked with minimum disruption to service levels. The purpose of our change management policy is to ensure accountability, communication, transparency and visibility between IT and the Business. The Vendor shall submit a change request to the CCB detailing what is changing and where it is changing, along with test plans, test results, and communication processes for before and after a change. There are two types of change requests:

#### A. Standard CR

Standard CRs follow the 'normal' change request process. This means these changes will be approved by the CCB prior to being released to a production environment.

#### B. Emergency CR

Emergency CRs will follow an abbreviated version of the CCB process. The following are considered emergency CRs:

1. Production system down;
2. Multiple users/sites affected ;
3. Misparsing data; and
4. Security risk.

### **6. Reports and Meetings**

- For all Change Order events, the Vendor, if requested by the TXDPS, shall arrange a kickoff meeting to be held at the TXDPS Main Campus located at 5805 N. Lamar Blvd. Austin, TX 78752, at a date and time agreeable to the TXDPS at no additional cost to the TXDPS. The Vendor PM or assigned designee and TXDPS CM or assigned designee, shall attend all project meetings. The TXDPS CM shall be informed of all meetings prior to occurrence.
- The Vendor shall provide the TXDPS CM with monthly, written, progress reports for each in-process Change order and maintenance and support incident reports.
  - "Progress Reports" are monthly status summaries of Change Order progress.
  - "Incident Reports" are monthly summaries of all "incident tickets", "tickets".
- Progress and incident reports shall be submitted by 5:00 pm CST Monday following the last working day of the month throughout the life of an active Change order or this Contract term. Email submission of the reports is acceptable.
- Progress reports shall cover all work performed and completed during the month for which the progress report is provided and will present the work to be performed during the subsequent month.
- Progress reports will identify any problems encountered with that month's development, all outstanding issues with an explanation of the cause, resolution methodology, and updated Change Order governance tables.
  - Incident reports will detail: each issue encountered by incident ticket identifier, affected application(s), affected software, affected networking infrastructure, incident discovery method (e.g.

infrastructure monitoring, technical support call / email, error discovered while performing maintenance, etc.), severity level, root cause analysis findings, detailed actions taken to resolve the issue, time expended in correcting the issue, name of person reporting the issue and report method, the Vendor's staff assigned to the issue, initial response time and method, and other agreed to report details requested by the TXDPS CM.

- The Vendor shall provide a listing of all programming languages used, updated as changes are made, in development and maintenance of the applications. Languages applicable to application functionality will be identified within the Transition Plan and included in monthly maintenance reports.

## 7. Service Level Agreements – SLAs

The Vendor shall provide a service credit to TXDPS equal to one-hundred dollars (\$100.00) for failure to meet any stated SLAs. Service credits will be applied on a per-application development and / or enhancement, or application maintenance basis.

### 7.1 Definitions:

“Uptime” is defined as any period of time 24 x 7 x 365 when an application is available to the “customer base” within the stated “availability technical requirements”.

“Downtime” is defined as any period of time 24 x 7 x 365 when an application is unavailable to the “customer base” to include but not limited to: outages, unscheduled maintenance & support events, software failures, or access to application is less than the stated “availability technical requirements”.

“Technical Availability” is defined as the customer base’s application access to an application, customer base’s access to test environments, and associated information or data results and/or exports based on customer base’s interaction with any application or supporting technology.

“Customer Base” is defined as any person or representative of TXDPS, the network-accessible, or an Authorized Data Access Entity (ADAE).

“Issue” is defined as any event that results in a loss of access to an applications production environment, test environment, or supporting technology that results in an application not achieving availability or technical requirements.

“Severity Level” is a defining classification scheme for all issues with corresponding resolution times.

- Critical/blocker (system is down and non-usable – Severity 1) -- Respond within in 1 hour, fix delivered in 24 hours.
- High (system is functional but suffering from significant impact to operations – Severity 2) -- Respond in 4 hours, fix delivered in 72 hours.
- Medium (system is functional, some impact to operations – Severity 3) – Respond in 8 hours, Fix delivered in 10 days or less.
- Low (minor issue, no impact to operations – Severity 4) – Respond in 24 hours, Fixed delivered based on prioritization of planned releases.

## 7.2. Application Performance Service Levels

The Vendor shall provide application, test and production environments, uptime on a 24 x 7 x 365 basis at a rate of ninety-nine and one-half percent (99.5%) operational availability to meet customer base needs.

The Vendor shall provide the customer base with application accessibility at the following minimum requirements assuming TXDPS' hardware is fully operational:

- .05 second limit for manipulating webpage objects
- 1 second limit for navigating to, from, and between main webpage, subordinate webpages and associated hyperlinks
- 1 second limit for navigating webpage command space
- 2 second limit for submitting a data request and getting a processing acknowledgment
- 10 second limit for retrieving data from a data request

## 7.3 Rate calculation

The rate calculation will be measured as the rate of System's technical availability by the amount of downtime during a calendar month. This metric gauges the application(s) performance as a percentage of available hours tracked to the quarter of an hour (rounded). The rate of system performance will be measured and monitored as follows:

- Available hours equal total number of hours in a month (24 hours x number of days in the month) minus the actual amount of time spent to the quarter of an hour for scheduled maintenance for the hosted application.
- Downtime is the total number of hours (rounded to the quarter hour) during which the solution is not in operation.
- System Performance Rate equals available hours Downtime divided by available hours.

Example for the month of January:

Available time per month was 744 hours (31 days X 24 hours)

Downtime per month was 3.75 hours (start 1:00 am - end 4:40 am)

$744.00 - 3.75 = 740.25$

$740.25 \div 744 = 99.5\%$

### 7.3.1 Escalation Process

Inability to meet or exceed the RATE during this Contract period will result in the following actions:

First event – verbal warning

Second event – written warning added to this Contract file

Third event – Negative Vendor Performance report

TXDPS reserves the right (as per TXDPS Technical Terms and Conditions) to terminate this Contract at any time.

## 8. Training

- A. The Vendor shall provide a detailed training plan within thirty (30) calendar days after contract award for the TXDPS users to acquire the necessary skills and proficiencies. All training programs will be conducted at TXDPS Headquarters, located in Austin, Texas. Training will be interactive with an emphasis on all appropriate development skills, and users shall have the ability to ask questions of the trainer during the sessions. The schedule of training sessions will be coordinated with the TXDPS' Project Manager. The requirements of the training programs are as follows:
1. Train the Trainer:
    - a. The Train the Trainer training will be offered to selected TXDPS users to acquire the necessary information, skills, and proficiencies of the user interface and database to allow those users to train other typical users how to use the user interface and database to its fullest potential.
    - b. The training will include advanced user techniques and basic technical troubleshooting skills.
    - c. It is estimated that the TXDPS will receive a minimum of no less than eight (8) training sessions during the total potential contract term, including the Base term and each Renewal Option Periods.
  2. Developer Training:
    - a. The developer training will be provided to select TXDPS personnel who will be responsible for the daily operation and maintenance of the database.
    - b. The developer training will provide TXDPS personnel with the skills needed to integrate new data into the database.
    - c. The developer training will include data integration training designed for TXDPS personnel to be able to interface with internal and external data sources.
    - d. The developer training course will include overviews of the entity model, importing an SQL database, multi-level security related to data sources and analysis outcomes, and entity resolution.
    - e. It is estimated that the TXDPS will receive a minimum of no less than three (3) developer training sessions during each of the Base and Renewal.
- B. The Vendor's training programs will allow the TXDPS and the Vendor to jointly alter the proportion of train the trainer, analyst, developer, and certified training programs so as to maximize the overall effectiveness of the training for the TXDPS. All training sessions including any web-based sessions will be live and/or interactive.
- C. The Vendor shall scale, detail, and tie training to match the user interface and database.
- D. The Vendor shall submit to the TXDPS' Project Manager copies of the curricula and associated User Guides for trainees for acceptance by the TXDPS no less than fifteen (15) calendar days prior to the first training program for each type of training.
- E. The Vendor shall make available to the TXDPS video recorded training for each training program as a review/refresher resource for TXDPS personnel who have already completed the live training.

## 9. Reproduction of Materials

TXDPS may reproduce all documentation and printed materials provided by the Vendor. If the documentation described above is revised at any time or if the Vendor develops additional documentation for the System, the Vendor shall deliver an electronic copy of such revised or additional documentation to TXDPS at no additional cost.

## 10. Period of Performance

The term of this Contract shall be September 1, 2015, or the date of TXDPS PO issuance, through August 31, 2016.

## 11. Invoices

Invoices associated with the provided services will be submitted monthly to [APIInvoices@dps.texas.gov](mailto:APIInvoices@dps.texas.gov) for all accepted Change Order deliverables and maintenance & support requirements associated with this Contract. A copy of the submitted invoice will also be sent, via email, to the TXDPS CM or assigned designee identified for each specific application or individual Change Order. Invoices will contain all required information per the State of Texas Procurement Manual listed on the Texas Comptroller of Public Accounts website (<http://www.cpa.state.tx.us/procurement/pub/manual/2-43.pdf>).

### 11.1 Maintenance invoices shall detail:

- a. The TXDPS Purchase Order number,
- b. The TXDPS application name for which maintenance was provided,
- c. Detail of any SLAs missed for the month and the cumulative credit being applied.

### 11.2 Application development and / or enhancement invoice shall detail:

- a. The TXDPS Purchase Order Number,
- b. The assigned TXDPS Change Order Alpha Designation,
- c. Identified Service Provided by Description,
- d. Quantity of Hours Associated with the Service Provided per Service Title,
- e. Actual cost to TXDPS for the Service Provided per Service Title,
- f. Detail of any SLAs missed for the month and the cumulative credit being applied,
- g. A copy of the TXDPS Change Order Acceptance Document signed by both parties.

## 12. Additional Customer Terms and Conditions

### 12.1 FBI CJIS Security Addendum

The Vendor shall execute an original signed CJIS Security Addendum which can be downloaded from <http://txdps.state.tx.us/securityreview>. Additionally, a CJIS Security Addendum Certification shall be signed by each employee performing duties related to this project prior to working on this Contract. Each original Certification shall include an original signature of the employee and the Vendor's representative. Non-compliance by the Vendor will be cause for termination of this Contract.

The Vendor shall, prior to beginning work on this Contract, enter into the CJIS online system all Vendor employees and subcontractors who will work on this Contract (further instructions will be provided to the Vendor prior to execution of this Contract), and have those employees/subcontractors complete the CJIS online training/testing. The Vendor shall meet or exceed all requirements contained in the CJIS Security Policy.

### 12.2 Vendor Background Check Completion

The Vendor's Authorized Representative shall provide the following to the TXDPS' Contract Manager within ten (10) calendar days of executing this Contract:

- i. The completed TXDPS Contractor Background Information form (HR-22) for all proposed personnel; and
- ii. Acceptable fingerprints for all proposed personnel.

The Vendor will not allow any personnel to work on the project that have not submitted to and successfully completed a TXDPS fingerprint-based Criminal History Background Investigation. The TXDPS has the right to prevent the Vendor's personnel from gaining access to the TXDPS building(s) and computer systems if the TXDPS determines that such personnel did not pass the background check or failed to otherwise maintain a security clearance.

### **13. Vendor Requirements and Response Submission**

Respondents interested in this opportunity shall detail as part of their Pricing Request response, how they meet the following qualifications. Qualification demonstration shall include but not be limited to verifiable documentation of:

- Year of experience
- Similar in scope projects

Respondents shall also response with sufficient detail necessary to prove competency in meeting all requirements stated within this SOW.

At a minimum, the Vendor shall have demonstrated experience in each of the following:

#### **13.1 Application Language: JAVA, DB2 SQL Stored Procedures**

#### **13.2 Operating Systems**

Web based access will be available regardless of user platform, but at a minimum will support Internet Explorer 7 and higher versions, and common mobile devices to include, but not be limited to, iPhone, iPad, Android, and BlackBerry devices. Red Hat Enterprise Linux Server release 5.4; Tomcat 7.0.23

#### **13.3 SQL Technologies**

Advanced Query Analysis and Optimization  
SQL Server Linked Servers  
Supporting large scale web applications

#### **13.4 System Knowledge**

The Vendor shall have verifiable experience in the following areas:

- All technologies referenced in Section 2.1
- Working with TCIC/NCIC transactions and communications
- Export formats such as Comma Separated Value (.csv) for certain information and reports
- XML for individual gang member data
- 12 Analyst Notebook (.anb) for individual gang member data

Respondents shall provide references from three (3) projects of similar size databases that involved intelligence data regulated by the Code of Federal Regulations Title 28, Chapter I, Part 23.

405-15-R025523  
Attachment C - SOW  
TXDPS Texas Gang Intelligence Index (TX Gang)  
Application Development, Maintenance & Support,  
Technology Upgrade/Migration and Transformation

The Vendor's augmented deliverable response information shall be phrased in terms and language that can be easily understood by non-technical personnel (e.g., laypersons without subject matter expertise).

- Any acronyms used in the Respondent's response, shall be clearly detailed and spelled out.
- SOW responses shall be in the same form and fashion as provided by TXDPS through this solicitation. The PR documents including all attachments, addendas, and exhibits are to be modified using Track Changes, identifying all additions, deletions, and / or modifications from the original.
- Any Respondent-added information shall be placed within the corresponding and relevant section of this SOW.

Respondent shall provide a response narrative for each Section and Subsection in the format in which requirements are presented. Supplemental justification and / or documentation may be provided as attachments. The Respondent shall ensure that all material submitted is directly pertinent to the requirements of this SOW and shall be formatted as to the specific requirements of the SOW Sections.

Respondent shall submit in editable, public format, all required documents via email to the TXDPS Contract Administrator by the date and time listed on the SOW. Required documentation shall include:

- **1.** Cover Page - List name and address of the Respondent, date of Offer, SOW identifier, and signature of authorized official.
- **2.** Completed SOW document and Attachment A
- **3.** Respondent's Project Team Resumes:
  - Employee names
  - Employee titles
  - Employees work experiences and corresponding dates - relevant to scope of this SOW
  - Additional in-scope skills, abilities, knowledge
- **4.** Respondent's organizational chart to include phone and email contact information
- **5.** An original and signed CJIS Security Addendum - Reference Section 12.
- **6.** An FBI Certification page to the CJIS Security Addendum for each employee performing duties related to the project - Reference Section 12.
- **7.** Documentation verifying compliance with CSA CCM - Reference Section 3.1.
- **8.** Documentation verifying experience with and familiarity of working with the State's payment portal.
- **9.** Completed HUB HSP Plan

14. SOW Authorization

Vendor	Texas Department of Public Safety
By:	By: <u>Steven C. McCraw</u>
Name: <u>Jerry D. Sanders Jr.</u>	Name: <u>Steven C. McCraw</u>
Title: <u>President</u>	Title: <u>Director</u>
Date: <u>08/19/2015</u>	Date: <u>8/28/15</u>



The applications identified in this request for pricing are not cloud based and the CAIQ does not apply.

<b>Consensus Assessments Initiative Questionnaire</b>			
<b>Control Group</b>	<b>CGID</b>	<b>CID</b>	<b>Consensus Assessment Questions</b>
Independent Audits	CO-02	CO-02.2	How often do you conduct network penetration tests of your cloud service infrastructure. N/A
		CO-02.3	How often do you conduct regular application penetration tests of your cloud infrastructure? N/A
		CO-02.4	How often do you conduct internal audits? N/A
		CO-02.5	Do you conduct external audits regularly as prescribed by industry best practices and guidance? N/A
		CO-02.6	Are the results of the network penetration tests available to tenants at their request? N/A
		CO-02.7	Are the results of internal and external audits available to tenants at their request? N/A
Third Party Audits	CO-03	CO-03.1	Will you permit DPS to conduct vulnerability scans on hosted applications and your network? N/A
		CO-03.2	Do you have external third-party conduct vulnerability scans and periodic penetration tests on your applications and networks? N/A
Audit Tools Access	IS-29	IS-29.1	How do you restrict, log, and monitor access to your information security management systems? (Ex. Hypervisors, firewalls, vulnerability scanners, network sniffers, APIs, etc.) N/A
Information System Regulatory Mapping	CO-05	CO-05.1	How do you ensure customer data is logically segmented that data may be produced for a single tenant only, without inadvertently accessing another tenant's data? N/A
		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? N/A
Intellectual Property	CO-06	CO-06.1	Describe the controls you have in place to protect tenants intellectual property? N/A
<b>Data Governance</b>			

## Consensus Assessments Initiative Questionnaire

Control Group	CGID	CID	Consensus Assessment Questions
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)? N/A
Classification	DG-02	DG-02.4	Can you provide the physical location/geography of storage of a tenant's data upon request? N/A
		DG-02.5	Do you allow tenants to define acceptable geographical locations for data routing or resource instantiation? N/A
Handling / Labeling / Security Policy	DG-03	DG-03.1	Are Policies and procedures established for labeling, handling and security of data and objects which contain data? N/A
Retention Policy	DG-04	DG-04.1	Describe technical control you have in place to enforce tenant data retention policies? N/A
Secure Disposal	DG-05	DG-05.1	Describe your process for secure disposal or destruction of physical media and secure deletion or sanitization of all computer resources of DPS data once DPS has N/A
Nonproduction Data	DG-06	DG-06.1	How do you ensure production data is be replicated or used in non-production environments? N/A
Information Leakage	DG-07	DG-07.1	Describe the controls in place to prevent data leakage or intentional/accidental compromise between tenants. N/A
		DG-07.2	What a Data Loss Prevention (DLP) or extrusion prevention solution is in place for all systems which interface with your cloud service offering? N/A
<b>Facility Security</b>			
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? N/A
Unauthorized Persons Entry	FS-05	FS-05.1	How are ingress and egress points such as service areas and other points where unauthorized personnel may enter the premises, monitored, controlled or isolated from data storage and process? N/A
Asset Management	FS-07	FS-07.1	What are your procedures governing asset management and repurposing of equipment used to support DPS hosted services or data? N/A
<b>Human Resources Security</b>			

## Consensus Assessments Initiative Questionnaire

Control Group	CGID	CID	Consensus Assessment Questions
Background Screening	HR-01	HR-01.1	Are state of residency and national fingerprint-based record checks conducted on employees or contractors who have access to DPS's data, applications or the networks supporting DPS's data and or applications? <sup>Yes</sup>
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? <sup>N/A</sup>
		HR-02.2	Do you document employee acknowledgment of training they have completed? <sup>N/A</sup>
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? <sup>N/A</sup>
<b>Information Security</b>			
Management Program	IS-01	IS-01.1	Do you provide tenants with documentation describing your Information Security Management Program (ISMP)? <sup>N/A</sup>
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? <sup>N/A</sup>
Policy	IS-03	IS-03.1	Do your information security and privacy policies align with particular industry standards (ISO-27001, ISO-22307, CoBIT, etc.)? <sup>N/A</sup>
		IS-03.2	Do you have agreements which ensure your providers adhere to your information security and privacy policies? <sup>N/A</sup>
	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? <sup>N/A</sup>
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? <sup>N/A</sup>
Policy Enforcement	IS-06	IS-06.1	Is a formal disciplinary or sanction policy established for employees who have violated security policies and procedures? <sup>N/A</sup>
		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? <sup>N/A</sup>

## Consensus Assessments Initiative Questionnaire

Control Group	CGID	CID	Consensus Assessment Questions
User Access Policy	IS-07	IS-07.1	What controls do you have in place to ensure timely removal of systems access which is no longer required for business purposes? N/A
User Access Restriction /	IS-08	IS-08.1	Describe process for granting and approving access to DPS data or hosted services. N/A
User Access Revocation	IS-09	IS-09.1	Describe process for timely deprovisioning, revocation or modification of user access to the DPS data or hosted services upon any change in status of employees, contractors, customers, business partners or third parties? N/A
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)? N/A
		IS-10.2	If users are found to have inappropriate entitlements, are all remediation and certification actions recorded? N/A
Training / Awareness	IS-11	IS-11.1	Do you provide annually a formal security awareness training program for cloud-related access and data management issues for all persons with access to DPS or hosted services? N/A
	IS-12	IS-12.2	Do you benchmark your security controls against industry standards? N/A
Segregation of Duties	IS-15	IS-15.1	How do you maintain segregation of duties within your cloud service offering? N/A
Encryption	IS-18	IS-18.1	Do you have a capability to allow creation of unique encryption keys per tenant? N/A
		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)? N/A
Encryption	IS-19	IS-19.1	What encryption method and level of encryption is applied to DPS's data at rest and does it meet FIPS 140-2? N/A
		IS-19.3	For DPS data in transport, what encryption level is applied and is the cryptographic module FIPS 140-2 certified. N/A
		IS-19.4	Describe your key management procedures? N/A
Encryption Key Management			
Vulnerability / Patch Management	IS-20	IS-21.1	Describe your patch management process? N/A

## Consensus Assessments Initiative Questionnaire

Control Group	CGID	CID	Consensus Assessment Questions
Antivirus / Malicious Software	IS-21	IS-21.1	Do you have anti-malware programs installed on all systems which support DPS hosted services and data? N/A
		IS-21.2	How do you ensure that security threat detection systems which use signatures, lists, or behavioral patterns are updated across all infrastructure components which support DPS's hosted services. N/A
Incident Management	IS-22	IS-22.1	Do you have a documented security incident response plan N/A
			Do you have processes for handling and reporting of security incidents that include preparation, detection, analysis, containment eradication, and recovery? N/A
			What steps are taken to ensure all employees are made aware of the incident reporting procedures? N/A
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? N/A
Network Monitoring	IS-27	IS-27.1	List the tools used to monitor network events, detect attacks, and provide identification of unauthorized use. N/A
Source Code Access Restriction	IS-33	IS-33.1	Describe the controls in place to prevent unauthorized access to your application, program or object source code, and assure it is restricted to authorized personnel only? N/A
Utility Programs Access	IS-34	IS-34.1	How are utilities that can significantly manage virtualized partitions (ex. shutdown, clone, etc.) appropriately restricted and monitored? N/A
Release Management			
Production Changes	RM-02	RM-02.1	Do you have documented change management procedures? N/A
Quality Testing	RM-03	RM-03.1	Do you provide your tenants with documentation which describes your quality assurance process? N/A
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? N/A
		RM-04.2	Do you have controls in place to detect source code security defects for any outsourced software development activities? N/A
Unauthorized Software Installations	RM-05	RM-05.1	What controls do you have in place to restrict and monitor the installation of unauthorized software onto your systems? N/A

## Consensus Assessments Initiative Questionnaire

Control Group	CGID	CID	Consensus Assessment Questions
<b>Resiliency</b>			
Business Continuity Testing	RS-01	RS-01.1	Are Policy, process and procedures defining business continuity and disaster recovery in place to minimize the impact of a realized risk event? N/A
	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? N/A
Equipment Power Failures	RS-07	RS-07.1	How are Security mechanisms and redundancies implemented to protect equipment from utility service outages (e.g., power failures, network disruptions, etc.)? N/A
<b>Security Architecture</b>			
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? N/A
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? N/A
Password			Describe password requirements N/A
Application Security	SA-04	SA-04.2	Do you utilize an automated source-code analysis tool to detect code security defects prior to production? N/A
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? N/A
Remote User Multifactor Authentication	SA-07	SA-07.1	Describe multi-factor authentication method required for all remote user access. N/A
Segmentation	SA-09	SA-09.4	Are system and network environments logically separated to ensure protection and isolation of sensitive data? N/A
Wireless Security	SA-10	SA-10.1	Are policies and procedures established and mechanisms implemented to protect network environment perimeter and configured to restrict unauthorized traffic? N/A

## Consensus Assessments Initiative Questionnaire

Control Group	CGID	CID	Consensus Assessment Questions
		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.) N/A
		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? N/A
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? N/A
Audit Logging / Intrusion Detection	SA-14	SA-14.1	What file integrity controls and network intrusion detection (IDS) tools are deployed to help facilitate timely detection, investigation by root cause analysis and response to incidents? N/A
		SA-14.2	Is Physical and logical user access to audit logs restricted to authorized personnel? N/A

## **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	FedRAMMP	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	X	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-2D NIST SP800-53 R3 CA-2(1)D NIST SP800-53 R3 CA-7D NIST SP800-53 R3 CA-7(2)D NIST SP800-53 R3 PL-6D	PCI DSS v2.0 2.1.2.b	SIG v6.0: L1, L2, L7, L8, L11	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 DSS.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 RA-5C NIST SP800-53 R3 RA-5(1)D NIST SP800-53 R3 RA-5(2)D NIST SP800-53 R3 RA-5(3)D NIST SP800-53 R3 RA-5(9)D NIST SP800-53 R3 RA-5(8)D	NIST SP800-53 R3 CA-1D NIST SP800-53 R3 CA-2D NIST SP800-53 R3 CA-2(1)D NIST SP800-53 R3 CA-6D NIST SP800-53 R3 RA-5C NIST SP800-53 R3 RA-5(1)D NIST SP800-53 R3 RA-5(2)D NIST SP800-53 R3 RA-5(3)D NIST SP800-53 R3 RA-5(9)D NIST SP800-53 R3 RA-5(8)D	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: L2, L4, L7, L9, L11	GAPP Ref 1.2.6 GAPP Ref 1.2.7 GAPP Ref 4.2.1 GAPP Ref 9.2.7 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	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 SC-7(1)D NIST SP800-53 R3 SC-7(2)D NIST SP800-53 R3 SC-7(3)D NIST SP800-53 R3 SC-7(4)D NIST SP800-53 R3 SC-7(5)D NIST SP800-53 R3 SC-7(6)D NIST SP800-53 R3 SC-7(7)D NIST SP800-53 R3 SC-7(8)D NIST SP800-53 R3 SC-7(12)D NIST SP800-53 R3 SC-7(13)D NIST SP800-53 R3 SC-7(18)D	NIST SP800-53 R3 CA-3D NIST SP800-53 R3 SA-9C NIST SP800-53 R3 SA-9(1)D NIST SP800-53 R3 SA-12D NIST SP800-53 R3 SC-7D NIST SP800-53 R3 SC-7(1)D NIST SP800-53 R3 SC-7(2)D NIST SP800-53 R3 SC-7(3)D NIST SP800-53 R3 SC-7(4)D NIST SP800-53 R3 SC-7(5)D NIST SP800-53 R3 SC-7(6)D NIST SP800-53 R3 SC-7(7)D NIST SP800-53 R3 SC-7(8)D NIST SP800-53 R3 SC-7(12)D NIST SP800-53 R3 SC-7(13)D NIST SP800-53 R3 SC-7(18)D	PCI DSS v2.0 2.4 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-5D NIST SP800-53 R3 IR-6D NIST SP800-53 R3 SI-5D	NIST SP800-53 R3 AT-5D NIST SP800-53 R3 IR-6D NIST SP800-53 R3 SI-5D	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) 8) 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 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-1D NIST SP800-53 R3 AT-1D NIST SP800-53 R3 AU-1D NIST SP800-53 R3 CA-1D NIST SP800-53 R3 CM-1D NIST SP800-53 R3 CP-1D NIST SP800-53 R3 IA-1D NIST SP800-53 R3 IA-7D NIST SP800-53 R3 IR-1D NIST SP800-53 R3 MA-1D NIST SP800-53 R3 MP-1D NIST SP800-53 R3 PE-1D NIST SP800-53 R3 PL-1D NIST SP800-53 R3 PM-1D NIST SP800-53 R3 PS-1D NIST SP800-53 R3 RA-1D NIST SP800-53 R3 RA-2D NIST SP800-53 R3 SA-1D NIST SP800-53 R3 SA-6D NIST SP800-53 R3 SC-1D NIST SP800-53 R3 SC-13D NIST SP800-53 R3 SI-1D	NIST SP800-53 R3 AC-1D NIST SP800-53 R3 AT-1D NIST SP800-53 R3 AU-1D NIST SP800-53 R3 CA-1D NIST SP800-53 R3 CM-1D NIST SP800-53 R3 CP-1D NIST SP800-53 R3 IA-1D NIST SP800-53 R3 IA-7D NIST SP800-53 R3 IR-1D NIST SP800-53 R3 MA-1D NIST SP800-53 R3 MP-1D NIST SP800-53 R3 PE-1D NIST SP800-53 R3 PL-1D NIST SP800-53 R3 PM-1D NIST SP800-53 R3 PS-1D NIST SP800-53 R3 RA-1D NIST SP800-53 R3 RA-2D NIST SP800-53 R3 SA-1D NIST SP800-53 R3 SA-6D NIST SP800-53 R3 SC-1D NIST SP800-53 R3 SC-13D NIST SP800-53 R3 SI-1D	PCI DSS v2.0 3.1.1 PCI DSS v2.0 3.1	SIG v6.0: L1, L2, L4, L7, L9	GAPP Ref 1.2.2 GAPP Ref 1.2.4 GAPP Ref 1.2.6 GAPP Ref 1.2.11 GAPP Ref 3.2.4 GAPP Ref 5.2.1

## 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 - Intellectual Property	CO-08	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-60 NIST SP800-53 R3 SA-70 NIST SP800-53 R3 PM-50		SIG v6.0: L4	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 DSS.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 RA-2 NIST SP800-53 R3 SA-2	NIST SP800-53 R3 CA-20 NIST SP800-53 R3 CA-2 (1)0 NIST SP800-53 R3 PM-50 NIST SP800-53 R3 PS-20 NIST SP800-53 R3 RA-20 NIST SP800-53 R3 SA-20		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-20 NIST SP800-53 R3 AC-40	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-160 NIST SP800-53 R3 MP-10 NIST SP800-53 R3 MP-30 NIST SP800-53 R3 PE-160 NIST SP800-53 R3 SI-120 NIST SP800-53 R3 SC-9 (1)0	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 8.2.6		
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.  Removed the specific reference to tape and disk backup as there are other media types	No Change	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 (b)(7)(i)(A) 45 CFR 164.310 (d)(2)(iv) 45 CFR 164.308(a)(7)(i)(D) (New) 45 CFR 164.316(b)(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-20 NIST SP800-53 R3 CP-2 (1)0 NIST SP800-53 R3 CP-2 (2)0 NIST SP800-53 R3 CP-6 (1)0 NIST SP800-53 R3 CP-6 (3)0 NIST SP800-53 R3 CP-7 (1)0 NIST SP800-53 R3 CP-7 (2)0 NIST SP800-53 R3 CP-7 (3)0 NIST SP800-53 R3 CP-7 (5)0 NIST SP800-53 R3 CP-8 (1)0 NIST SP800-53 R3 CP-8 (2)0 NIST SP800-53 R3 CP-8 (3)0 NIST SP800-53 R3 CP-9 (1)0 NIST SP800-53 R3 CP-9 (3)0 NIST SP800-53 R3 SI-120 NIST SP800-53 R3 AU-110	PCI DSS v2.0 3.1 PCI DSS v2.0 3.1.1 PCI DSS v2.0 3.2 PCI DSS v2.0 3.2.2 PCI DSS v2.0 3.2.3 PCI DSS v2.0 3.2.4 PCI DSS v2.0 3.2.5 PCI DSS v2.0 3.2.6 PCI DSS v2.0 3.2.7 PCI DSS v2.0 3.2.8 PCI DSS v2.0 3.2.9 PCI DSS v2.0 3.2.10 PCI DSS v2.0 3.2.11 PCI DSS v2.0 3.2.12 PCI DSS v2.0 3.2.13 PCI DSS v2.0 3.2.14 PCI DSS v2.0 3.2.15 PCI DSS v2.0 3.2.16 PCI DSS v2.0 3.2.17 PCI DSS v2.0 3.2.18 PCI DSS v2.0 3.2.19 PCI DSS v2.0 3.2.20 PCI DSS v2.0 3.2.21 PCI DSS v2.0 3.2.22 PCI DSS v2.0 3.2.23 PCI DSS v2.0 3.2.24 PCI DSS v2.0 3.2.25 PCI DSS v2.0 3.2.26 PCI DSS v2.0 3.2.27 PCI DSS v2.0 3.2.28 PCI DSS v2.0 3.2.29 PCI DSS v2.0 3.2.30 PCI DSS v2.0 3.2.31 PCI DSS v2.0 3.2.32 PCI DSS v2.0 3.2.33 PCI DSS v2.0 3.2.34 PCI DSS v2.0 3.2.35 PCI DSS v2.0 3.2.36 PCI DSS v2.0 3.2.37 PCI DSS v2.0 3.2.38 PCI DSS v2.0 3.2.39 PCI DSS v2.0 3.2.40 PCI DSS v2.0 3.2.41 PCI DSS v2.0 3.2.42 PCI DSS v2.0 3.2.43 PCI DSS v2.0 3.2.44 PCI DSS v2.0 3.2.45 PCI DSS v2.0 3.2.46 PCI DSS v2.0 3.2.47 PCI DSS v2.0 3.2.48 PCI DSS v2.0 3.2.49 PCI DSS v2.0 3.2.50 PCI DSS v2.0 3.2.51 PCI DSS v2.0 3.2.52 PCI DSS v2.0 3.2.53 PCI DSS v2.0 3.2.54 PCI DSS v2.0 3.2.55 PCI DSS v2.0 3.2.56 PCI DSS v2.0 3.2.57 PCI DSS v2.0 3.2.58 PCI DSS v2.0 3.2.59 PCI DSS v2.0 3.2.60 PCI DSS v2.0 3.2.61 PCI DSS v2.0 3.2.62 PCI DSS v2.0 3.2.63 PCI DSS v2.0 3.2.64 PCI DSS v2.0 3.2.65 PCI DSS v2.0 3.2.66 PCI DSS v2.0 3.2.67 PCI DSS v2.0 3.2.68 PCI DSS v2.0 3.2.69 PCI DSS v2.0 3.2.70 PCI DSS v2.0 3.2.71 PCI DSS v2.0 3.2.72 PCI DSS v2.0 3.2.73 PCI DSS v2.0 3.2.74 PCI DSS v2.0 3.2.75 PCI DSS v2.0 3.2.76 PCI DSS v2.0 3.2.77 PCI DSS v2.0 3.2.78 PCI DSS v2.0 3.2.79 PCI DSS v2.0 3.2.80 PCI DSS v2.0 3.2.81 PCI DSS v2.0 3.2.82 PCI DSS v2.0 3.2.83 PCI DSS v2.0 3.2.84 PCI DSS v2.0 3.2.85 PCI DSS v2.0 3.2.86 PCI DSS v2.0 3.2.87 PCI DSS v2.0 3.2.88 PCI DSS v2.0 3.2.89 PCI DSS v2.0 3.2.90 PCI DSS v2.0 3.2.91 PCI DSS v2.0 3.2.92 PCI DSS v2.0 3.2.93 PCI DSS v2.0 3.2.94 PCI DSS v2.0 3.2.95 PCI DSS v2.0 3.2.96 PCI DSS v2.0 3.2.97 PCI DSS v2.0 3.2.98 PCI DSS v2.0 3.2.99 PCI DSS v2.0 3.2.100	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		
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 means for specific reasons.	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-60 NIST SP800-53 R3 MP-6 (4)0 NIST SP800-53 R3 PE-10	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.2.2.14,	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-110 NIST SP800-53 R3 SA-11 (1)0 NIST SP800-53 R3 CM-040	PCI DSS v2.0 6.4.3	SIG v6.0: I.2, 18	GAPP Ref 1.2.6		

## 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	GAPP (Aug 2009)				
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-8 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-8 NIST SP800-53 R3 SI-7 NIST SP800-53 R3 SI-7 (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-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-8 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: 1.2, 18	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)(9) (New)	Clause 4.2.1 e) & 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) 45 CFR 164.310 (a)(2)(i) 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-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.1.6, F.1.7, F.1.8, F.1.9, F.2.1, F.2.2, F.2.3, F.2.4, F.2.5, F.2.6, 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, F.1.4.6, 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, 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	GAPP Ref 8.2.3				

## 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 27001:2006	NIST SP800-53	FedRAMP	PCI DSS v2.0	BITS Shared Assessments AUP v5.0 / SIG v6.0	GAPP (Aug 2008)
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 attestation mechanisms shall be designed to address the requirements of legislative plurality and their results shared with tenants	X	X	X	X		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 R3 PE-7 NIST SP800-53 R3 PE-8 NIST SP800-53 R3 PE-18	NIST SP800-53 R3 PE-20 NIST SP800-53 R3 PE-2 (1) NIST SP800-53 R3 PE-30 NIST SP800-53 R3 PE-60 NIST SP800-53 R3 PE-6 (1) NIST SP800-53 R3 PE-70 NIST SP800-53 R3 PE-7 (1) NIST SP800-53 R3 PE-80 NIST SP800-53 R3 PE-180	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 9.2	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, 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	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 prevent 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-70 NIST SP800-53 R3 PE-7 (1) NIST SP800-53 R3 PE-160 NIST SP800-53 R3 PE-180		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, 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	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-10 NIST SP800-53 R3 MA-20 NIST SP800-53 R3 MA-2 (1) NIST SP800-53 R3 PE-160	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
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 repurposing of equipment and resources prior to tenant assignment or jurisdictional transport.	X	X	X	X			45 CFR 164.310 (e ) 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-170 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-10 NIST SP800-53 R3 PE-10 NIST SP800-53 R3 PE-160 NIST SP800-53 R3 PE-170	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			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 (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 responsibilities of the candidate.	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-20 NIST SP800-53 R3 PS-30	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-40 NIST SP800-53 R3 PS-60 NIST SP800-53 R3 PS-70	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 complicated	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-40 NIST SP800-53 R3 PS-50		SIG v6.0: E.6	GAPP Ref 8.2.2 GAPP Ref 10.2.5

## Cloud Controls Matrix (CCM) R1.1

Control Area	Control ID	Control Specification	Control Revisions v1.1	Cloud Service Delivery Model Applicability					Compliance Mapping									
				Scope Applicability			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)		
				SaaS	PaaS	IaaS												
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: <ul style="list-style-type: none"> <li>• Risk management</li> <li>• Security policy</li> <li>• Organization of information security</li> <li>• Asset management</li> <li>• Human resources security</li> <li>• Physical and environmental security</li> <li>• Communications and operations management</li> <li>• Access control</li> <li>• Information systems acquisition, development,</li> </ul>	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.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-10 NIST SP800-53 R3 PM-20 NIST SP800-53 R3 PM-30 NIST SP800-53 R3 PM-40 NIST SP800-53 R3 PM-50 NIST SP800-53 R3 PM-60 NIST SP800-53 R3 PM-70 NIST SP800-53 R3 PM-80 NIST SP800-53 R3 PM-90 NIST SP800-53 R3 PM-100 NIST SP800-53 R3 PM-110	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	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-11 NIST SP800-53 R3 PM-110	NIST SP800-53 R3 CM-10 NIST SP800-53 R3 PM-10 NIST SP800-53 R3 PM-110	PCI DSS v2.0 12.5	SIG v6.0: C.1	GAPP Ref 8.2.1		
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 leadership and officer 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.8.2.2	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 IA-1 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 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-10 NIST SP800-53 R3 AT-10 NIST SP800-53 R3 AU-10 NIST SP800-53 R3 CA-10 NIST SP800-53 R3 CM-10 NIST SP800-53 R3 IA-10 NIST SP800-53 R3 IR-10 NIST SP800-53 R3 MA-10 NIST SP800-53 R3 MP-10 NIST SP800-53 R3 PE-10 NIST SP800-53 R3 PL-10 NIST SP800-53 R3 PS-10 NIST SP800-53 R3 SA-10 NIST SP800-53 R3 SC-10 NIST SP800-53 R3 SI-10	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 reassessed at least annually or upon significant	No Change	X	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 (1) NIST SP800-53 R3 CM-2 (3) NIST SP800-53 R3 CM-2 (5) NIST SP800-53 R3 SA-20 NIST SP800-53 R3 SA-40 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 v6.0: L.2, L.5, L.7 L.8, L.9, L.10	SIG GAPP Ref 8.2.1 GAPP Ref 8.2.7	GAPP Ref 1.2.6 GAPP Ref 8.2.1 GAPP Ref 8.2.7			

## 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)
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 CFE 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 IR-1 NIST SP800-53 R3 MA-1 NIST SP800-53 R3 MP-1 NIST SP800-53 R3 PE-1 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.1.5	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)	No Change	X	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.6.2, H.1.1, K1.4.5,	GAPP Ref 6.1.0
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 DS 5.4	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.11.1.1 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 IA-2 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 IA-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

## 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)
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	X	COBIT 4.1 DS 5.4	45 CFR 164.308(a)(3)(i)(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(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-4C NIST SP800-53 R3 PS-5C	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
Information Security - User Access Reviews	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 tiers (IaaS, SaaS, PaaS, (DaaS, ...). Automatic or manual remediation 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)(i)(B) 45 CFR 164.308 (a)(4)(i)(C)	A.11.2.4	NIST SP800-53 R3 AC-2 NIST SP800-53 R3 AU-6 NIST SP800-53 R3 PS-6 NIST SP800-53 R3 PS-7	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-6C 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-6C NIST SP800-53 R3 PS-7C		SIG v6.0: H.2.6, H.2.7, H.2.9,	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 as 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)(i)(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-1C NIST SP800-53 R3 AT-2C NIST SP800-53 R3 AT-3C NIST SP800-53 R3 AT-4C	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 SI-5 NIST SP800-53 R3 SI-5C	NIST SP800-53 R3 SI-5C		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-3C NIST SP800-53 R3 PL-4C NIST SP800-53 R3 PM-10C NIST SP800-53 R3 PS-1C NIST SP800-53 R3 PS-6C NIST SP800-53 R3 PS-7C		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-2C NIST SP800-53 R3 AT-3C NIST SP800-53 R3 CA-1C NIST SP800-53 R3 CA-5C NIST SP800-53 R3 CA-6C NIST SP800-53 R3 CA-7C NIST SP800-53 R3 PM-10C	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

## 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)			
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)(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 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(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 6.5.7 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-2 NIST SP800-53 R3 MP-4 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				
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 DSS.8 COBIT 4.1 DSS.10 COBIT 4.1 DSS.11	45 CFR 164.312 (a)(2)(iv) 45 CFR 164.312 (e)(1) 45 CFR 164.312 (e)(2)(ii)	A.10.6.1 A.10.8.3 A.10.8.4 A.10.9.2 A.10.9.3 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-16 NIST SP800-53 R3 SC-23 NIST SP800-53 R3 SI-8 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(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(16) 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 4.2	AUP v5.0 G.4 AUP v5.0 G.15 AUP v5.0 I.3 SIG v6.0: G.10.4, G.11.1, G.11.2, G.12.1, G.12.2, G.12.4, G.12.10, G.14.18, G.14.19, G.16.2, G.16.18, G.16.19, G.17.16, G.17.17, G.18.13, G.18.14, G.19.1.1, G.20.14	GAPP Ref 6.1.1 GAPP Ref 8.2.1 GAPP Ref 8.2.5				

## 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 v6.0 / SIG v6.0	GAPP (Aug 2009)
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 (5)□ 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	SIG v6.0: L6	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 A16.1 COBIT 4.1 A13.3 COBIT 4.1 DS5.9	45 CFR 164.308 (a)(1)(i)(A) 45 CFR 164.308 (a)(1)(i)(B) 45 CFR 164.308 (a)(5)(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 (9)□ NIST SP800-53 R3 RA-5 (6)□ 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 6.1 PCI-DSS v2.0 6.2 PCI-DSS v2.0 6.3.2 PCI-DSS v2.0 6.4.5 PCI-DSS v2.0 6.5X 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	AUP v5.0: I.4 SIG v6.0: G.15.2, I.3	GAPP Ref 1.2.6 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)(i)(B)	A.10.4.1	NIST SP800-53 R3 SA-7 NIST SP800-53 R3 SC-5 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-5□ NIST SP800-53 R3 SI-7□ NIST SP800-53 R3 SI-8□ NIST SP800-53 R3 SI-5 (1)□ 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)(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-3 NIST SP800-53 R3 IR-4 NIST SP800-53 R3 IR-5 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 (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 7.2.4 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	No Change	X	X	X	X	X	COBIT 4.1 DS5.6	45 CFR 164.312 (a)(6)(i) 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 (1)□ NIST SP800-53 R3 IR-7 (2)□ NIST SP800-53 R3 IR-7 (3)□ NIST SP800-53 R3 SI-4 (2)□ NIST SP800-53 R3 SI-4 (4)□ NIST SP800-53 R3 SI-4 (6)□ 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 - 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)(i)	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

## 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)
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-6	NIST SP800-53 R3 IR-4D NIST SP800-53 R3 IR-4 (1)D NIST SP800-53 R3 IR-8D NIST SP800-53 R3 IR-8D	PCI DSS v2.0 12.9.6	SIG v6.0: J.1.2,	GAPP Ref 1.2.7 GAPP Ref 1.2.10
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 analysis output	X	X	X	X	X	COBIT 4.1 DS 5.3	45 CFR 164.310 (b)	A.7.1.3	NIST SP800-53 R3 AC-6 NIST SP800-53 R3 AC-20 NIST SP800-53 R3 PL-4	NIST SP800-53 R3 AC-8D NIST SP800-53 R3 AC-20D NIST SP800-53 R3 AC-20 (1)D NIST SP800-53 R3 AC-20 (2)D NIST SP800-53 R3 PL-4D	PCI-DSS v2.0 12.3.5	AUP v5.0 B.3, SIG v6.0: B.1.7, D.1.3.3, E.3.2, E.3.5.1, E.3.5.2	GAPP Ref 6.1.0
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-4D		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-14D NIST SP800-53 R3 AC-14 (1)D NIST SP800-53 R3 AC-21D NIST SP800-53 R3 AC-22D NIST SP800-53 R3 IA-8D NIST SP800-53 R3 AU-10D NIST SP800-53 R3 AU-10 (5)D NIST SP800-53 R3 SC-4D NIST SP800-53 R3 SC-8 (1)D NIST SP800-53 R3 SC-9D NIST SP800-53 R3 SC-9 (1)D	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.19.1.1, G.19.1.2, G.19.1.3, 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 7.2.2 GAPP Ref 8.2.1 GAPP Ref 8.2.5
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	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-9D NIST SP800-53 R3 AU-9 (2)D NIST SP800-53 R3 AU-11D NIST SP800-53 R3 AU-14D	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-7D NIST SP800-53 R3 CM-7 (1)D NIST SP800-53 R3 MA-3D NIST SP800-53 R3 MA-3 (1)D NIST SP800-53 R3 MA-3 (2)D NIST SP800-53 R3 MA-3 (3)D NIST SP800-53 R3 MA-4D NIST SP800-53 R3 MA-4 (1)D NIST SP800-53 R3 MA-4 (2)D NIST SP800-53 R3 MA-5D	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	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-20D NIST SP800-53 R3 SC-20 (1)D NIST SP800-53 R3 SC-21D NIST SP800-53 R3 SC-22D NIST SP800-53 R3 SC-23D NIST SP800-53 R3 SC-23D		AUP v5.0 C.2 SIG v6.0: C.2.6, G.9.9	GAPP Ref 8.2.2 GAPP Ref 8.2.5

## 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	GAPP (Aug 2009)
																AUP v5.0 / SIG v6.0
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 DSS.11 COBIT 4.1 DSS.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-17 (2) NIST SP800-53 R3 MP-2 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)	NIST SP800-53 R3 AC-17D 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.1.1, 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 8.4.1 PCI-DSS v2.0 6.4.2	SIG v6.0: 1.2.7.2, 1.2.9, 1.2.10, 1.2.15,	GAPP Ref 1.2.6 GAPP Ref 6.2.1
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 DSS.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 AC-6 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-19D	PCI DSS v2.0 7.1.2	SIG v6.0:H.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 SA-9 (1)	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

## 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)
Legal - Third Party Agreements	LG-02	Third party agreements that directly, or indirectly, impact the organizations 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. Assets agreements 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)(A) 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 (c)(1) (New) 45 CFR 164.312(e)(2)(ii) (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)(ii)(A) 45 CFR 164.314 (a)(2)(ii)(B) 45 CFR 164.314 (a)(2)(ii)(C) 45 CFR 164.314 (a)(2)(ii)(D) 45 CFR 164.314 (a)(2)(iii)(A) 45 CFR 164.314 (a)(2)(iii)(A)(1) 45 CFR 164.314 (a)(2)(iii)(A)(2) 45 CFR 164.314 (a)(2)(iii)(B) 45 CFR 164.314 (a)(2)(iii)(C) 45 CFR 164.314 (b)(1) 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)	A.6.2.3 A.10.2.1 A.10.8.2 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-6 NIST SP800-53 R3 SA-7 NIST SP800-53 R3 SA-9	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 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, G.16.3,	GAPP Ref 1.2.5
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.8.2.2 A.10.1.1	NIST SP800-53 R3 CM-2 NIST SP800-53 R3 CM-2 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 (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 (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 information system	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

## 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)
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(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 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 NIST SP800-53 R3 MA-6	NIST SP800-53 R3 MA-2(1) 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(1) NIST SP800-53 R3 MA-4 (2) NIST SP800-53 R3 MA-5(1) NIST SP800-53 R3 MA-6(1)		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.12.5.1 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(1) NIST SP800-53 R3 CA-2(1) NIST SP800-53 R3 CA-2(1) NIST SP800-53 R3 CA-5(1) NIST SP800-53 R3 PM-9(1) NIST SP800-53 R3 RA-1(1)	PCI DSS v2.0 12.1.2	AUP v5.0 L.2 v6.0: A.1, L.1	SIG GAPP Ref 1.2.4
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 should 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.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(1) NIST SP800-53 R3 RA-2(1) NIST SP800-53 R3 RA-3(1)	PCI DSS v2.0 12.1.2	AUP v5.0 I.1 AUP v5.0 J.4 SIG v6.0: C.2.1, I.4.1, I.5, G.15.1.3, I.3	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.14.1.2 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(1) NIST SP800-53 R3 CM-4(1)		AUP v5.0 I.4 AUP v5.0 L.2 v6.0: I.3, L.9, L.10	SIG 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(1) NIST SP800-53 R3 CP-2 (1) NIST SP800-53 R3 CP-2 (2) NIST SP800-53 R3 RA-2(1) NIST SP800-53 R3 RA-3(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, B.1.2, B.1.6, B.1.7.2, G.2, L.9, L.10	N/A

## Cloud Controls Matrix (CCM) R1.1

Control Area	Control ID	Control Specification	Control Revisions v.1.1	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 v6.0 / SIG v6.0	GAPP (Aug 2009)
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	Service Providers shall implement and communicate disaster recovery, business continuity, capacity overflow and operational redundancy plans to all dependant service iters. Service Providers shall perform failure impact analysis studies and communicate potential service impacts and reduced capacity projections to	X	X	X	X	X	COBIT 4.1 DS 2.3		A.6.2.1 A.6.3.3 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 RA-3 (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	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 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 I.2 SIG v6.0: I.1.1, I.1.2, I.2.7, 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, A17.6	45 CFR 164.306 (b)(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 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 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	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-6 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-5 NIST SP800-53 R3 SA-6 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	G.1.7, G.1, G.6, I.1, I.4.5, I.2.16, I.2.21, I.2.23, I.2.26, 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

## 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)
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 legally 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.10.2.2 A.10.2.9 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.12.5.5 A.12.6.1 A.13.1.2 A.15.2.1 A.15.2.2	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-4D 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-5C NIST SP800-53 R3 SA-5 (1)□ NIST SP800-53 R3 SA-5 (3)□ NIST SP800-53 R3 SA-8C NIST SP800-53 R3 SA-9C NIST SP800-53 R3 SA-9 (1)□ NIST SP800-53 R3 SA-10C NIST SP800-53 R3 SA-11C NIST SP800-53 R3 SA-11 (1)□ NIST SP800-53 R3 SA-12C NIST SP800-53 R3 SA-13C	PCI DSS v2.0 3.6.7 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 9.3.1 PCI DSS v2.0 10.5.2 PCI DSS v2.0 11.5 PCI DSS v2.0 12.3.1 PCI DSS v2.0 12.3.3	AUP v5.0 C.2 AUP v5.0 I.2 AUP v5.0 I.4 AUP v5.0 I.1 SIG v6.0: C.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.2.18, I.2.22.6, I.2.27.1, 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, L.7, L.9, 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.10.4.1 A.11.5.4 A.11.6.1 A.12.4.1 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-1D NIST SP800-53 R3 CM-2D 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-3D NIST SP800-53 R3 CM-3 (2)□ NIST SP800-53 R3 CM-5D NIST SP800-53 R3 CM-5 (1)□ NIST SP800-53 R3 CM-5 (5)□ NIST SP800-53 R3 CM-7D NIST SP800-53 R3 CM-7 (1)□ NIST SP800-53 R3 CM-8D 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-9D NIST SP800-53 R3 SA-6D NIST SP800-53 R3 SA-7D NIST SP800-53 R3 SI-1D NIST SP800-53 R3 SI-3D 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-4D 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-7D NIST SP800-53 R3 SI-7 (1)□	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,	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 6.2.2	

### 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 v6.0 / SIG v6.0	GAPP (Aug 2009)
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	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)(i)(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: K1.2.9, K1.2.10, K3.1	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: <ul style="list-style-type: none"> <li>• Identify critical products and services</li> <li>• Identify all dependencies, including processes, applications, business partners and third party service providers</li> <li>• Understand threats to critical products and services</li> <li>• Determine impacts resulting from planned or unplanned disruptions and how these vary over time</li> <li>• Establish the maximum tolerable period for disruption</li> <li>• Establish priorities for recovery</li> <li>• Establish recovery time objectives for resumption of critical products and services within their maximum tolerable period of disruption</li> </ul>	No Change	X	X	X	X	X		45 CFR 164.308 (a)(7)(i)(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:K2	N/A

### 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)
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: <ul style="list-style-type: none"> <li>• Defined purpose and scope, aligned with relevant dependencies</li> <li>• Accessible to and understood by those who will use them</li> <li>• Owned by a named person(s) who is responsible for their review, update and approval</li> <li>• Defined lines of communication, roles and responsibilities</li> <li>• Detailed recovery procedures, manual work-around and reference information</li> </ul>	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 164.310 (a)(2)(i) 45 CFR 164.312 (a)(2)(ii)	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 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-5 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)(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
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 a reasonable distance.	No Change	X	X	X	X			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,	N/A

## 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)
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-10 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.1.6.1, 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 taps, 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-10 NIST SP800-53 R3 PE-4C NIST SP800-53 R3 PE-13C 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.1.6.1, 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.2.6.1, 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		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-6 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 (2) 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-6C NIST SP800-53 R3 IA-8C NIST SP800-53 R3 SC-10C	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.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,	N/A

## Cloud Controls Matrix (CCM) R1.1

Control Area	Control ID	Control Specification	Control Revisions v.1.1	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)
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 leakage prevention) 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.10.9.2 A.11.1.1 A.11.6.1 A.11.4.6 A.12.3.1 A.12.5.4 A.15.1.4	NIST SP800-53 R3 AC-1 NIST SP800-53 R3 AC-4 NIST SP800-53 R3 SC-1 NIST SP800-53 R3 SC-16	NIST SP800-53 R3 AC-1 NIST SP800-53 R3 AC-4 NIST SP800-53 R3 SC-1 NIST SP800-53 R3 SC-16	PCI DSS v2.0 2.3 PCI DSS v2.0 3.4.1, 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 6.5c PCI DSS v2.0 8.3 PCI DSS v2.0 10.5.5 PCI DSS v2.0 11.5	AUP v5.0 B.1 v6.0: G.8.2.0.2, G.8.2.0.3, G.12.1, G.12.4, G.12.9, G.12.10, G.16.2, G.19.2.1, G.19.3.2, G.9.4, G.17.2, G.17.3, G.17.4, G.20.1,	SIG 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 9.2.1
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 (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.16.3, I.3	GAPP Ref 1.2.6
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.12.6.1 A.15.2.1	NIST SP800-53 R3 SI-10 NIST SP800-53 R3 SI-11 NIST SP800-53 R3 SI-12 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	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
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 B.1 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	SIG 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 B.1 SIG v6.0: H.1.1, G.9.13, G.9.20, G.9.21,	GAPP Ref 8.2.2

## 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 v5.0	GAPP (Aug 2009)	
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 (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 DSS.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 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	
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 network 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 DSS.5 COBIT 4.1 DSS.7 COBIT 4.1 DSS.8 COBIT 4.1 DSS.10	45 CFR 164.312 (e)(4)(2)(ii) 45 CFR 164.308(s)(5)(ii)(D) (New) 45 CFR 164.312(e)(1) (New) 45 CFR 164.312(e)(2)(ii) (New)	A.7.1.1 A.7.1.2 A.7.1.3 A.9.2.1 A.9.2.4 A.10.8.1 A.10.8.2 A.10.8.1 A.10.8.3 A.10.8.5 A.10.10.2 A.11.2.1 A.11.4.3 A.11.4.5 A.11.4.6 A.11.4.7 A.12.3.1 A.12.3.2		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 9.1.3	AUP v5.0 D.1 AUP v5.0 B.3 AUP v5.0 F.1 AUP v5.0 G.4 AUP v5.0 G.15 AUP v5.0 G.17 AUP v5.0 G.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	No Change	X	X	X	X	X		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 R3 SC-7 NIST SP800-53 R3 PE-4□ NIST SP800-53 R3 SC-4□ 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 v6.0: D.1.1, E.1, F.1.1, H.1.1,	SIG GAPP Ref 8.2.5	

# Cloud Controls Matrix (CCM) R1.1

Control Area	Control ID	Control Specification	Control Revisions v.1.1	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	GAPP (Aug 2009)
				AUP v5.0 G.7	SIG v6.0 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,	AUP v5.0 D.1	SIG v6.0 D.1.1, D.1.3	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.9.6.2, G.9.5.3, G.9.6.4, G.9.19, H.2.16, H.3.3, J.1, J.2, L.5, L.9, L.10	SIG v6.0 G.20.12, I.2.5	N/A
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 timelines. 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-6	NIST SP800-53 R3 AU-10 NIST SP800-53 R3 AU-80 NIST SP800-53 R3 AU-8 (1)0	PCI DSS v2.0 10.4	AUP v5.0 G.7 SIG v6.0 G.8	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-30 NIST SP800-53 R3 IA-40 NIST SP800-53 R3 IA-4 (4)0		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 DS5.6 COBIT 4.1 DS9.2	45 CFR 164.308 (a)(1)(ii)(D) 45 CFR 164.312 (b) 45 CFR 164.308(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-10 NIST SP800-53 R3 AU-20 NIST SP800-53 R3 AU-2 (3)0 NIST SP800-53 R3 AU-2 (4)0 NIST SP800-53 R3 AU-30 NIST SP800-53 R3 AU-3 (1)0 NIST SP800-53 R3 AU-40 NIST SP800-53 R3 AU-50 NIST SP800-53 R3 AU-60 NIST SP800-53 R3 AU-6 (1)0 NIST SP800-53 R3 AU-6 (3)0 NIST SP800-53 R3 AU-70 NIST SP800-53 R3 AU-7 (1)0 NIST SP800-53 R3 AU-90 NIST SP800-53 R3 AU-9 (2)0 NIST SP800-53 R3 AU-110 NIST SP800-53 R3 AU-120 NIST SP800-53 R3 AU-140 NIST SP800-53 R3 SI-40 NIST SP800-53 R3 SI-4 (2)0 NIST SP800-53 R3 SI-4 (4)0 NIST SP800-53 R3 SI-4 (5)0 NIST SP800-53 R3 SI-4 (6)0	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.9.6.2, G.9.5.3, G.9.6.4, G.9.19, H.2.16, 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 (4)0	NIST SP800-53 R3 SC-180 NIST SP800-53 R3 SC-18 (4)0		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/cem.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 uses not addresses in the copyright notice, please contact [info@cloudsecurityalliance.com](mailto:info@cloudsecurityalliance.com)

## 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

QA by the HISPI  
12/01/10

Change Order *Template*

**1. Introduction:**

TXDPS Contract 405-xx-xxxxxxx with \_\_\_\_\_ incorporates the ability to scope, detail, and administer specific application enhancement Change Orders (CO). CO will be administered per the requirements of Section 3.1 and follow the change management requirements of Section 5.3 of Statement of Work to TXDPS 405-xx-xxxxxxx. An approved CO shall set forth the specific services to be performed by (Company Name).

TXDPS Business Division Project Manager (PM) and (Company Name) shall update the following sections of this CO through cooperative negotiations. The Sections, Tables, and format of this CO shall be augmented with information specific to the particular application enhancement. Sections, Tables, and format outlined will not be modified.

**2. Scope**

*2.1. TXDPS requires (Company Name) to provide services related to Application Enhancements and Technology Upgrade / Migration and Transformation. Specific business and functional requirements will include but may not be limited to: hardware (HW) and software (SW) customizations, HW and SW upgrades, programming services, project documentation, and successful testing of each required deliverable(s) identified in this CO. All services provided by (Company Name) shall be in accord with deliverables available through named DIR contracts identified within 405-xx-xxxxxxx.*

*2.2. TXDPS has indentified the following, itemized services to be performed:*

- 2.2.1. \_\_\_\_\_*
- 2.2.2. \_\_\_\_\_*
- 2.2.3. \_\_\_\_\_*

*2.3. (Company Name) shall deliver, through updates to this CO, the project detail necessary to address information commonly found within Implementation Plan, Project Plan, Schedule, and Pricing Quotes for enhancement services related to achieving he identified deliverables. The CO will address the processes, sub-tasks, itemized costs and duration for completion of each deliverable and the Pricing will set the associated cost. Tables 1, 2, 3, and 4 are provided as the tools to clearly itemize all identified deliverables.*

2.3.1. Table 1 - Project Points of Contact and Responsibilities

Organization	Title / Responsibility	Name	Office Phone	Cell Phone	Email Address
TXDPS	Project Sponsor				
TXDPS	Project Manager				
TXDPS	Technical SME - Hardware				
TXDPS	Technical SME - Software				
TXDPS	Technical SME - Data transmission				
TXDPS	Contract Monitor				
TXDPS	Contract Administrator				

Organization	Title / Responsibility	Name	Office Phone	Cell Phone	Email Address
	Relationship Representative				
	Project Manager				
	Programmer				
	DBA				
	HW / SW SME				

2.3.2. Table 2 - Project Specific Roles & Responsibility

Table 2 – Roles and Responsibilities Matrix	Micro Assist	TXDPS
Project requirement / dependency #1		
Project requirement / dependency #2		
*primary (P)		

2.3.3. Table 3 - Project Schedule

W.O. Ref #	Deliverable Description	Date				Comments
		Due Date	Actual	Test / Review	Acceptance	
2.2.1	“Same info as is provided in section 2.2.x above”					
2.2.2						
2.2.3						

2.3.4. Table 4 - Pricing

W.O. Ref #	Deliverable - Description	Service Category / Description (e.g. Programmer) and (Company Name) Employee Name	Qty of Hours	Hourly Rate	Cost Extension
2.2.1	“Same info as is provided in section 2.2.x above”				
2.2.2					
2.2.3					

2.4. Services are not complete until all testing and acceptance is successfully completed as defined in Section 5 of the 405-xx-xxxxxxx, SOW. During the testing and acceptance period, (Company Name) shall capture and document performance issues identified by (Company Name) and / or reported by TXDPS and resolve all HW, SW, and programming defects. Time and materials used to resolve defects will not be billed to TXDPS.

2.5. Final testing and acceptance completion, and all unplanned work to achieve acceptance, will be documented within Table 3 of the final CO version.

2.6. Final acceptance will be memorialized in writing by sign-off of the CO Acceptance Document, Exhibit 2 to this document.

**3. Risk and Issue Management**

*The TXDPS PM shall update Section 3 with any and all pertinent and known risks and issue management items related to the specific application enhancement CO. (Company Name) shall add information as necessary to ensure all possible CO risks and issue management items are clearly addressed during negotiations with the TXDPS Business Division.*

The following general procedures shall be used to manage active CO issues and risks:

- 3.1. *The TXDPS PM shall identify and document project issues (current problems) and risks (potential events that impact the project).*
- 3.2. *The TXDPS PM shall assess, analyze and prioritize the impact and determine the highest priority risks and issues that will be managed actively, according to priority, by (Company Name).*
- 3.3. *(Company Name) shall plan and schedule high-priority risks and issues assigning responsibility for risk management and issue resolution in a documented risk register or issues log, as determined by TXDPS.*
- 3.4. *(Company Name) shall track and report the status of risks and issues, and communicate risk mitigation plans and issue resolutions using the risk register or issue log as determined by TXDPS.*
- 3.5. *The TXDPS PM shall monitor and control the effectiveness of the risk and issue management actions.*
- 3.6. *Active issues and risks shall be monitored and reassessed on a weekly basis by the TXDPS PM and (CompanyName). Mutually agreed upon escalation and risk management processes will be defined at the outset of the CO.*

**4. Service Levels:**

(Company Name) shall meet the following service levels for work performed under this CO. All Service Levels for this CO will meet the same standards as written in the Statement of Work Section 7.

Meantime to Resolution (MTR): Upon verbal or written notification (Company Name) shall provide the following MTR's for defect resolution.

Time and materials applied to fix (Company Name) defects will not be billed to TXDPS.

**5. Required Reporting and Communication:**

(Company Name) shall:

- 5.1. *Create and maintain a Risk and Issues Log if requested by TXDPS.*
- 5.2. *Be accountable for tracking of all technical staff hours and provide a written monthly report due by 5:00 pm CT Monday following the last working day of the month throughout the life of the Change Order reflecting current cost and total Contract usage.*
- 5.3. *Provide one (1) weekly status report and prepare and lead one (1) status meeting per week of no more than one (1) hour in duration, if requested by TXDPS.*
- 5.4. *Attend any required or requested meeting(s) or submit any requested documentation at the discretion of the TXDPS PM.*

**6. Pricing:**

(Company Name) shall identify the specific CO pricing within Table 4 above. In addition (Company Name) shall ensure:

6.1. All CO pricing is provided per a deliverable basis, identifies the Service Category, and identifies the (Company Name) employee providing the work as listed within Attachment A.

6.2. CO pricing will be a fixed / not to exceed cost of (enter total cost here).

**7. Change Order Authorization Signatures:**

\_\_\_\_\_  
TXDPS Business Representative                      Date

\_\_\_\_\_  
(Company Name) Authorized Agent                      Date

\_\_\_\_\_  
TXDPS Contract Administrator                      Date

TXGangs 405-15-R025523 Exhibit 2  
**CHANGE ORDER COMPLETION ACCEPTANCE DOCUMENT**

TEXAS DEPARTMENT OF PUBLIC SAFETY

**Section 1. General Information**

Contract # \_\_\_\_\_

Change Order Name \_\_\_\_\_

Change Order # \_\_\_\_\_

**Section 2. Vendor Acknowledgement of Change Order Completion**

*The following project deliverables, as required by Section C Scope of Work and as assigned by Subsection Change Order Plan, have been completed.*

CO Ref. #	Completed Deliverable Description

This is to acknowledge that \_\_\_\_\_ has completed this Change Order project for the Texas Department of Public Safety.

Vendor Approver Name	Title	Signature	Date

**Section 3. TXDPS Acceptance of Change Order Completion**

This document certifies that the above-referenced services from Change Order Plan # \_\_\_\_\_ have hereby been tested and accepted by the Texas Department of Public Safety.

Upon execution of this acceptance document, an invoice in the amount of \$ \_\_\_\_\_ may be submitted to the Texas Department of Public Safety.

TXDPS Approver Name	Title	Signature	Date