VACO RISK SOLUTIONS®
Free Yourself.®

Vaco Risk Solutions' response to the City of Bryan, Texas RFP #15-048 comprises separate proposals for the City of Bryan and Bryan Texas Utilities, both of which are included in sequence in the document that follows.

VACO
RISK SOLUTIONS
Free Yourself.

Commitment to Serve

Response to Request for Proposal

Payment Card Industry (PCI) Compliance Services
RFP # 15-048

Presented: July 30, 2015

City of Bryan
Purchasing Department
1309 E. Martin Luther King St.
Bryan, TX 77803

Vaco - Houston
3200 Southwest Fwy #3030
Houston, TX 77027

713.960.9898

Vaco Risk Solutions
6000 Poplar Ave, Suite 216
Memphis, TN 38119
Dr. Suzanne Miller, Partner
901.333.2250

Table of Contents

Table of Contents 2

Letter of Introduction 3

TAB A - Qualifications and Experience 4

TAB B Rates and Expenses 9

TAB C Project Time-Line 10

TAB D Methodology 11

TAB E Vaco References 21

TAB F Certification and Acknowledgement of Any Addenda Issued 22

Appendix A Executive Summary of Management Team 26

Letter of Introduction

July 30, 2015

Vaco Risk Solutions (Vaco) is pleased to respond to Bryan, Texas' (City of Bryan) request for Qualified Security Assessor (QSA) Services for PCI Compliance Certification RFP # 15-048 (RFP), hereby incorporated by reference, including addendums.

Our proposal is a collaborative effort among Vaco Risk Solutions partners Stephen J Schaefgen and Suzanne Miller. Dr. Miller is heading our proposal team and may be contacted at 407-575-7343, or by mail at 6000 Poplar Avenue, Suite 216, Memphis, TN 38119. Vaco Risk Solutions and Vaco are two members of the Vaco Family of offices, a national staffing and services company. Vaco Risk Solutions is the successor company of the merger of Compliance and Audit Group and VCAG LLC. VCAG subsequently was renamed Vaco Risk Solutions.

Our proposal, including our named delivery team, is valid for 180 days. Vaco Risk Solutions also confirms its agreement with the provisions of the Draft Standard Form of Agreement Contract for the City of Bryan.

Our proposal consists of the sections outlined in the Table of Contents including our statement of services and delivery approach, qualifications, resources and such other items as requested by the City of Bryan in its RFP.

Along with our professional expertise, focus on project management, and overall audit efficiencies, we bring three critical distinguishing factors to your PCI compliance efforts:

1. As the 15th QSA company our dedicated Vaco PCI Team has extensive PCI DSS expertise
2. A proven fresh approach to PCI assessments based on successful engagements
3. A collaborative business partner approach providing sustainable solutions and guidance for improving efficiencies

These elements and Vaco Risk Solutions' national network of resources, provide the framework for meeting City of Bryan's assessment and certification requirements.

We look forward to the opportunity to meet City of Bryan's QSA PCI assessment and compliance needs using our proven approach, delivered by proven professionals.

Sincerely,

Suzanne Miller, Ph.D.
Partner

TAB A - Qualifications and Experience

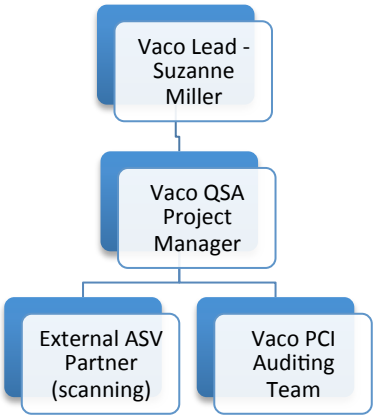
1. Vaco Risk Solutions LLC is a Premier Consulting Company. We are a specialized member of the Vaco family of companies.

   - Founded in 2002
   - Headquartered in Tennessee
   - 30 Locations Nationwide
   - 3000+ Employees
   - Over $200 Million in Annual Revenue
   - Vaco has been named as one of the *Fastest Growing Companies in America* by Inc. Magazine for eight consecutive years

Summary of Administration, Organization and Staffing of Vaco Risk Solutions, LLC

Vaco Risk Solutions (VRS) is a Limited Liability Company organized in the State of Tennessee and is an affiliated member of the Vaco LLC group of companies, which includes Vaco-Houston. VRS leadership and administration is led by partner/members including Mr. Schaefgen, president, and two partners, and Dr. Miller and Gourav Mukherjee. VRS has a team of 22 professionals including five (5) Qualified Security Assessors (QSAs).

Organization chart of people on this engagement:



2. Vaco Houston will be servicing this account.

3. In 2007 Vaco Risk Solutions (under the name of Compliance and Audit Group) became the 15th QSA Company. Vaco partners with Qualys for PCI DSS Approved Scanning Vendor (ASV) services. Our lead partner at Qualys is Mr. Paul Passey CISSP, CISM, CIPP, Technical Account Manager, Southeast US Field Operations, 1600 Bridge Parkway Redwood City, CA 94065, 919-610-0088.

4. Vaco Risk Solutions has the experience and capability to provide the following services:

    a. Initial PCI Gap Analysis
    b. Annual requirement for a PCI Pen Test
    c. Internal and external scanning
    d. PCI DSS Assessment Version 3.1 (or version current at the time of the Assessment
        - Upon successful validation of all requirements being in place, a completed SAQ or ROC (depending on the level of the merchant) will be presented to the merchant.
        - Also upon successful validation, an Attestation of Compliance (AOC) will also be presented to the merchant.
    e. Recommendations and remediation support
    f. Policy, procedure and program development
    g. Sustainment program in the form of an annual PCI compliance lifecycle (see b above)
    h. Besides performing the required scans, periodic vulnerability scans will also be performed.

5. Examples of details of PCI consulting services performed for past engagements:

    1) Vaco Risk Solutions was contracted to perform cardholder data discovery at all the newly acquired branches of a large healthcare client. Based on the results, Vaco Risk Solutions was further contracted to design a standardized process for card acceptance across all branches. Once the plan was accepted by management, Vaco Risk Solutions was able to assist with providing the needed technical resources to assist in the configuration and implement of required technology.
    2) A multi-level marketing company, required to be PCI compliant globally, needed help in reaching compliance with the 15,000 global customers who were selling products and taking credit/debit card data (acting as independent sales reps). Vaco Risk Solutions developed a strategy to bring the 15,000 global customers/independent sales reps into compliance within 6 months and sustain ongoing compliance.
    3) Vaco Risk Solutions was hired by a billion dollar charity that was unaware of the PCI requirements until their processor called. Once Vaco Risk Solutions was able to bring the organization into compliance, Vaco Risk Solutions introduced the charitable organization to other processors who were willing to dramatically reduce the interchange rate of the now compliant organization. Over $500,000 a year is being saved from this cost reduction.
    4) Vaco Risk Solutions was contracted to perform a PCI DSS Gap Analysis. During the analysis, Vaco Risk Solutions discovered that the multi-million dollar contract for outsourcing IT services required the client to complete a form booklet which outlined the PCI Compliance Services the client expected the IT company to perform. During discovery, Vaco Risk Solutions found the empty document in a file cabinet in legal. Vaco Risk Solutions was further contracted to work with the IT provider in defining and overseeing the implementation of required controls.

6. Currently, Vaco Risk Solutions performs the following PCI DSS services:

Number	PCI DSS Services (QSA)
1	PCI Gap Analysis
2	PCI Sustainment Program
3	PCI DSS Assessments
4	Vulnerability Assessments
5	Penetration Testing
6	Data Loss Prevention – eDiscovery Cardholder Data
7	Incident Response Planning
8	Policy and Procedures Development
9	Education and Training
10	Vender Management Assessments
11	Remediation Support
12	EMV Advisory Service
13	Tokenization Advisory Service
14	P2PE Advisory Services
15	Redaction Services
16	RFP Writing Service

Number	PCI DSS Services – Qualys (ASV)
1	ASV Scans
2	ASV Scans – Online help and 24x7x363 email/telephone support
3	ASV Scan- User-friendly interface
4	PCI Web Application Scanning
5	Qualys Cloud Platform - Vulnerability scanning with remediation and risk management
6	Qualys Auto-Submit - Compliance status is electronically submitted to acquiring bank

7. Project Manager and Individuals on the Vaco Engagement Team

Suzanne Miller and Kathy Brackenrich will provide QSA leadership for this project. As more fully described in their resumes in Appendix A, Dr. Miller and Ms. Brackenrich bring the following to the engagement:

1. <u>Suzanne Miller:</u>
    - Dr. Miller has performed over 210 onsite assessments for Level 1, Level 2, Level 3 and Level 4 Merchants.
    - Qualified Security Auditor (QSA)
    - Payment Card Industry Professional (PCIP)
    - Certified Information Security Manager (CISM)

- Certified Information Security Auditor (CISA)
- Certified Risk and Information Systems Controls (CRISC)
- Certified Performance Technologist (CPT)
- Certified Homeland Security (Technology) (CHS-III)

2. Kathy Brackenrich:
    - Ms. Brackenrich has performed more than 90 onsite assessments for Level 1, Level 2, Level 3 and Level 4 Merchants and will serve as project manager for the engagement.
    - Qualified Security Auditor (QSA)
    - Certified Information Security Auditor (CISA)
    - Certified Risk and Information Systems Controls (CRISC)
    - Payment Card Industry Professional (PCIP)

In addition to Dr. Miller and Ms. Brackenrich, Vaco intends to use other staff members as needed to deliver the services outlined in our approach and work plan. Members of the Vaco team who may become part of the engagement, as required, include:

- Eddie Salera, CISA, PCIP, QSA
- Michael Spiotta, PCIP, CISA
- Vicki Luckey, CIA, CISA, PCIP, CRMA
- Laury Garrett, CISA
- Matt Wagenknecht, CREA, CISSP, MCSE, MCP+1
- Gourav Mukherjee, JD, QSA, CISA, CISSP, CRISC

Key personnel identified for this project will be available for the duration of the project. No key personnel will be removed or otherwise replaced by Vaco without prior written concurrence by the City of Bryan, Texas. As noted earlier, Vaco Risk Solutions has access to the 30 offices of Vaco and a complement of resources to ensure supplemental resources are available.

8. Overview of Engagement Team

Vaco Risk Solutions methodology for performing PCI Consulting engagements is centered on a Team Approach. At Vaco Risk Solutions we believe having a team that can provide specialized expertise brings greater value to our clients without increasing costs.

Dr. Suzanne Miller, QSA will lead the Vaco PCI Team that will be assigned to this engagement. She will provide the on-site direction during the scope of the engagement. The Vaco PCI Team assigned to perform the services of this engagement are committed to the project and guaranteed by Vaco Risk Solutions except in the case of unforeseen personal events.

Vaco Risk Solutions does not use subcontractors when conducting PCI assessments and/or delivery of mitigation services. (Per Requirement 3.2.3)

Vaco Risk Solutions affirms that no employees assigned to the City of Bryan engagement have been convicted of a felony. (Per Requirement 3.2.4)

Vaco Risk Solutions welcomes the opportunity for City of Bryan to interview any of the assigned members of the proposed project team before selecting a Contractor. (Per Requirement 3.2.5)

9. Municipal Staff Support should include the following:

Support Staff	Role
Project Manager (PM)	Provide project management for the City and the departments
Department Lead	Every department lead should be the PCI overseer for the department by responding to requests, overseeing and reporting remediation efforts, attending status calls and reporting compliance issues.
IT Lead	IT lead should be the PCI overseer for the IT department by responding to requests, overseeing and reporting remediation efforts, attending status calls and reporting compliance issues.

.

10. Vaco Risk Solutions is not involved in nor has it been involved in any litigation performance or otherwise over the last five (5) years.

11. Vaco Risk Solutions has not had any contracts terminated due to non-performance over the last five (5) years.

12. Vaco Risk Solutions has not had any adverse actions sanctioned by any regulatory authorities over the last five (5) years.

TAB B Rates and Expenses

1. Vaco Risk Solutions proposed fee schedule.

	FYE 2016	FYE 2017	FYE 2018	FYE 2019	FYE 2020
Fixed Fee Price	$57,425	$49,672	$44,502	$40,366	$34,577
Administrative Fee (Consulting) *Not to exceed*	$52,925	$46,672	$41,502	$37,366	$31,576
Travel Expenses	$4,500	$3,000	$3,000	$3,000	$3,000

2. Vaco Risk Solutions' expectations concerning reimbursement for travel include flight, hotel, car rental and meals reflect the travel policy of the City of Bryan.

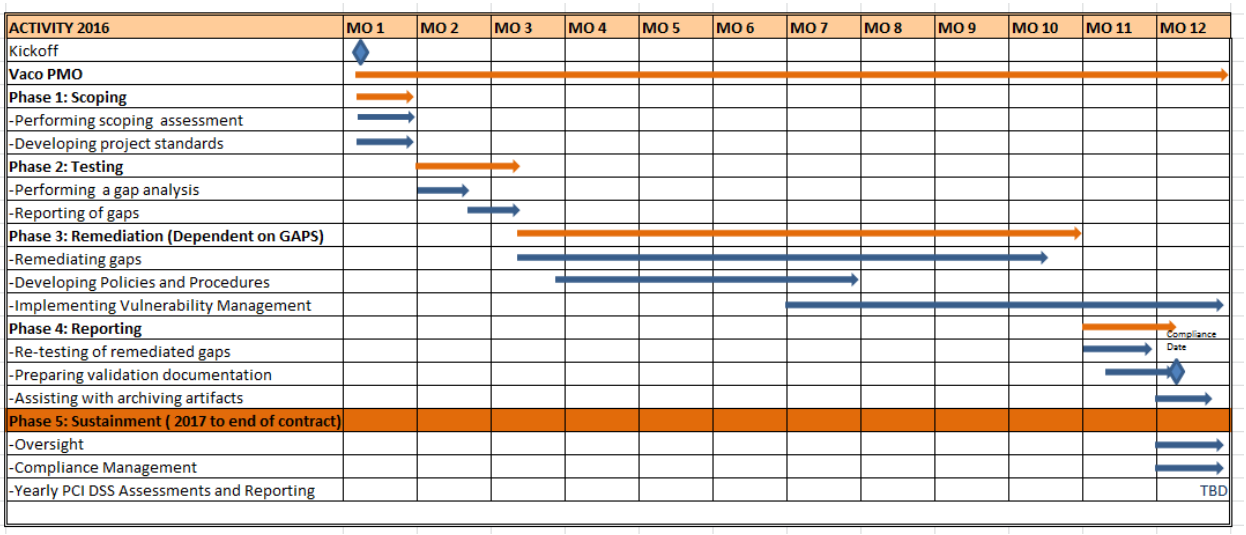
3. Vaco Risk Solutions understands prior approval by an authorized City representative is required for travel related expenses chargeable to the City.

4. Vaco Risk Solutions will not seek reimburse for charges other than approval travel expenses (See TAB B, 2).

5. Vaco Risk Solutions understands expenses not specifically listed will not be considered reimbursable.

TAB C Project Time-Line

1. Timeline for Project

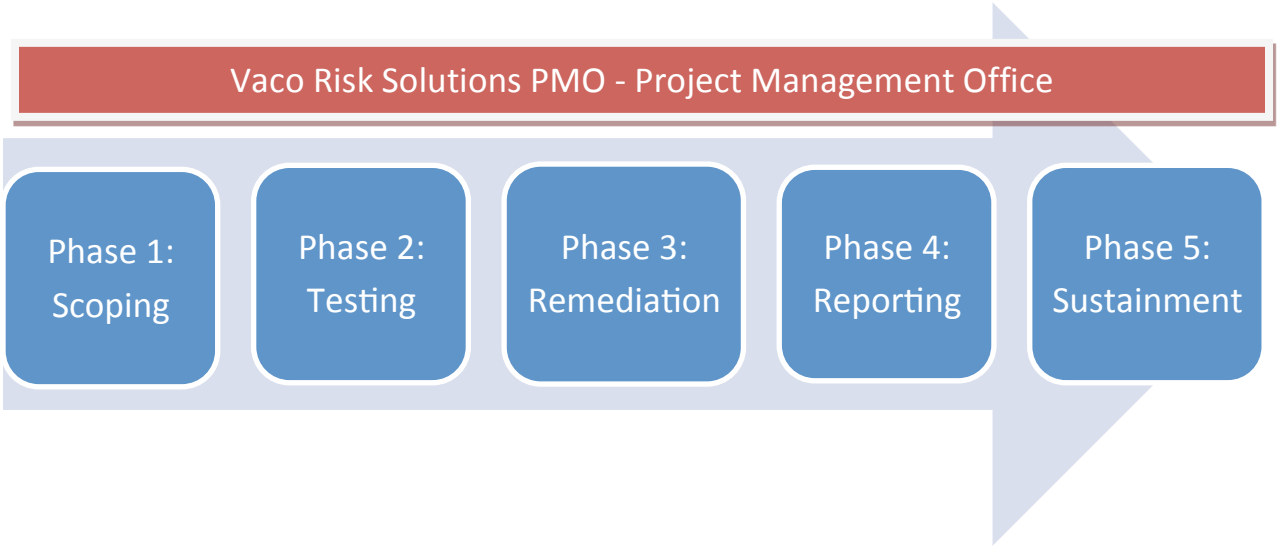


2. Phase 1 and 2 will be completed in 10 weeks. The completion of Phase 3 is dependent on the results of the gap analysis. Phase 4 will be completed in 8 weeks. Phase 5 scheduling will be addressed at the end of Phase 4.

TAB D Methodology

1. Vaco Risk Solutions PCI DSS Methodology

Based upon the scoping information provided by City of Bryan, the Vaco Risk Solutions PCI methodology that has been adapted to incorporate Vaco Risk Solutions' best practices is depicted below:



Each of the activities and phases are described in detail below.

Vaco Risk Solutions Project Management Office (PMO)

Vaco Risk Solutions PMO - Project Management Office

Vaco believes a structured and effective Project Management Office (PMO) will be a crucial element of the City of Bryan's roadmap to achieve compliance in a timely manner. The Vaco Risk Solutions PMO will plan and coordinate all aspects of the project from scoping through the planning and execution. An effective PMO requires several factors including a disciplined PMO approach, as well as a PMO leader who has extensive experience managing PCI Assessments.

The Vaco PMO will coordinate all PCI activities, resources, teams, training, communications, and document management. Vaco Risk Solutions' approach also establishes a PMO that will serve as a single point of contact for City of Bryan including updates for the Project Sponsor.

Key PMO Activities:

- Establish the PCI project office
- Create and monitor the overall PCI project plan (for all tasks and locations)
- Monitor progress, issues, milestones and deadlines for all PCI activities
- Secure resources as needed
- Coordinate and schedule activities across teams, business units and geographies

- Develop, maintain, and roll-out project tools and standard templates
- Coordinate quality assurance and risk management activities
- Establish and communicate project governance processes
- Coordinate PCI communications and change management activities
- Coordinate all training activities and materials
- Initiate knowledge sharing activities between Vaco Risk Solutions and City of Bryan

Key PMO Deliverables:

- Project plan
- Periodic status reports (e.g. weekly)
- Issue tracking reports
- Progress updates for City of Bryan's Project Sponsor
- Communications plan
- Standard document templates
- Document repository

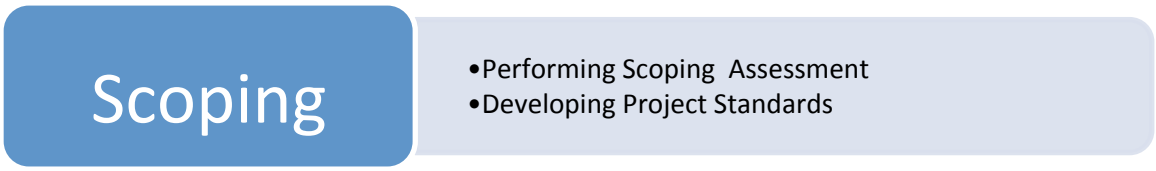
Vaco Risk Solutions' PMO methodology is based on our experience and makes use of a structured approach to coordinate PCI activities.

We believe a high level of project reporting and discipline is necessary to help ensure that any potential delays are identified and corrected as soon as possible. Therefore, the Vaco Risk Solutions PMO will provide periodic updates on the status of the project to the project sponsor.

At the conclusion of this step, the project organization, roles, and responsibilities will be clearly documented. A detailed project plan will be prepared and reviewed with City of Bryan. Project tracking and communication mechanisms will be established.

Phase 1: Scoping

We believe that the planning/scoping phase is the most important phase of the project. The key steps included in this phase are listed below and an explanation of each follows.



Task 1: Performing Scoping Assessment

We will begin by identifying and clarifying the in-scope cardholder data processes and environment. All people, departments, facilities, devices, systems, applications and databases that store, process or transmit cardholder data will be documented and defined as the cardholder data environment. These

documents will be written with the "end in mind" as the PCI standards requires the City of Bryan to attest to their cardholder data environment in each Attestation of Compliance (AOC).

Task 2: Developing Project Standards

Standardizing the assessment process across the City of Bryan will help to create time and resource efficiencies. Working with the City of Bryan, the documents for the projects will be identified and the format of the documents will be established. Additionally, the repository for the assessment documentation will be identified, and the City of Bryan will identify their team member(s) who are responsible for interfacing with and representing the departments during meetings and providing the artifacts on a timely basis. Based on our past experience we have found consistency and timeliness of meetings to be a key success factor to PCI Validation. Working with the City of Bryan, a calendar of meetings will be scheduled for the duration of the project.

At the conclusion of the planning phase, we will work with the applicable department members of the City of Bryan to finalize the approach and detailed work plan. The work plan will include the activities and timing to be performed.

The project team will present the project plan to City of Bryan project sponsor for review and approval. We believe this is an important step to ensure that the approach is appropriately documented and that there is appropriate "buy-in" from key stakeholders.

The primary deliverables for this phase are:

1. Comprehensive Work Plan for Vaco and the City of Bryan
2. Project Reporting Templates
3. Scoping Report – Identification of Validation Types (SAQs or ROCs) per Department

Phase 2: Testing

There are defined testing procedures that are required by the PCI Security Standards Council (PCI SSC).

Testing

- Performing a Gap Analysis
- Reporting of Gaps

It is important to note that we are required to test all PCI controls required per validation method as per the PCI Data Security Standard Requirements and Auditing Procedures Version 3.1. See www.pcisecuritystandards.org for a download of this document and PCI DSS version 3.1 SAQs.

For each requirement, the Vaco PCI Team will identify the artifacts that are necessary to validate compliance. The Vaco PCI Team will also be using state-of-the art assessment tools to review vulnerabilities, server policies, access controls and firewall/router settings. If during this phase, for

requirements which are found to "not be in place", Vaco will recommend actions to remediate the gaps. See Phase 3.

The Vaco PCI Team will request and review required documents. These will include documents such as: network diagrams, configuration documentation, awareness training content, and lists of terminated employees, employees' roles and responsibilities, copies of audit reports, quarterly scan reports, penetration tests, Intrusion Detection System (IDS) logs and other necessary documents.

The Vaco PCI Team is required to interview selected employees to ensure that they have an understanding of the City of Bryan's security policies and procedures. During certain interviews, the Vaco PCI Team may validate workstations or swipe devices that connect to the City of Bryan cardholder environment to ensure anti-virus, personal firewall and other access control requirements are consistent with PCI DSS requirements.

The Vaco PCI Team will visit the locations where cardholder data is processed or stored to ensure that cardholder data security procedures are consistent with written policies and adequate to protect cardholder data.

For each type of system in the card-processing environment, the Vaco PCI Team will inspect network and system configurations, firewall and router access control rules and database schemas and configuration. The Vaco PCI Team will confirm that prohibited data, such as sensitive authentication data, is not retained after authorization and that PAN (primary account number) data is encrypted during storage and over open public networks.

The Vaco PCI Team will conduct site inspections to ensure that physical security controls are adequate to protect the cardholder data. Physical media storage will also be inspected to ensure confidential data is labeled and protected in accordance with PCI DSS requirements.

The specific tasks and deliverables for Phase 2 are as follows:

Task 1: Perform a Gap Analysis

- Pre-Assessment (Gap Analysis) Activities per Department
  - Review Department's current payment card processes and data flows to identify the cardholder data environment and in-scope people, processes and technology
  - Interview Department's key staff to understand the existing controls around the cardholder data environment.
  - Walk-throughs of the Department's card-present and card-not-present payment processes at each department. Walk-throughs will include the following:
    - All people, processes and technology used to transmit, process or store cardholder data (CHD)
    - Physical location site visit(s)

- Applications that support the business processes for payment card processing and transmission
- Where subtle differences in processes and/or technology may exist for individual merchant IDs at these or other locations/properties, these will be explored by interview.
- Third party websites and gateways

➢ Evidence Gathering and Testing of the applicable requirements/sub-requirements through:
- Observation of system settings and interviews with responsible personnel
- Review of requested documentation
- Observation of processes, actions and state of in-scope components
- On-site physical review locations

Task 2: Reporting Gaps

❖ Initial Report on Compliance (IROC) -Gap Analysis Report
- ➢ Evaluate all collected information against PCI DSS 3.1 SAQ/ROC requirements and report thereon, including Compensating Controls and/or Explanations for non-Applicability, as applicable
- ➢ Provide design suggestions to reduce or manage technical scope
- ➢ Document gap analysis issues and provide prioritized remediation recommendations including detailed technical artifacts to support identified gaps
- ➢ Create the Initial Report on Compliance (IROC) and submit in electronic format to the City of Bryan

The primary deliverable for this phase is:

1. Gap Analysis Report – Executive Summary with Departmental Details

Phase 3: Remediation

During the testing phase, any requirements that are found to not be in place will require remediation. Once deficient controls are remediated, Vaco Risk Solutions will re-test these remediated controls.

The specific tasks and deliverables for Phase 3 are as follows:

Task 1: Remediating Gaps

During the remediation efforts, Vaco Risk Solutions will assist City of Bryan by providing subject matter expertise (SME) to assist with defining processes and procedures and recommending technical solutions.

Assisting with the implementing of technical solutions is not in-scope for this project. Upon request, Vaco Risk Solutions will assist the City of Bryan with staff augmentation for resource support.

- Remediation Consultation and Assistance
  - Following the IROC, Vaco Risk Solutions will:
    - Provide remediation consultation to City of Bryan's project team to assist with implementation of processes and procedures to comply with PCI DSS version 3.1 certification requirements
    - Provide remediation assistance at City of Bryan's separate request. The scope and extent of this assistance will be quoted to the Authority separate from this proposal based upon the results of the initial gap analysis produced in Phase 2.

Task 2: Developing Policies and Procedures

Vaco PCI Team will work in cooperation with the City of Bryan to develop city-wide PCI DSS policies and procedures per validation type.

Task 3: Implementing Vulnerability Management Program

- Vaco PCI Team and Qualys will initiate the Vulnerability Management Program, where applicable. This includes the following:
  - ASV external scanning
  - Penetration Testing
  - Internal scanning

The primary deliverables for this phase are:

1. PCI DSS Version 3.1 Policies and Forms Templates
2. ASV Scan Results
3. Penetration Test Results
4. Internal Scan Results

Phase 4: PCI Validation Reporting

PCI Validation Reporting

- Re-testing of Remediated Gaps
- Preparing Validation Documents (SAQ/ROC)
- Assisting with Archiving Artifacts

The Specific Tasks and Deliverables for Phase 4 are as follows:

Task 1: Re-Testing of Remediated Gaps

Following each department's successful completion of applicable remediation, Vaco Risk Solutions will:

- Perform re-testing of the remediated gaps
  - Upon successful re-testing:
    - Prepare the validation documents
    - Archive the artifacts

Task 2: Preparing Validation Documentation

- Among the other functions that are required for PCI DSS assessments, Vaco Risk Solutions will prepare the SAQs/ROC for each in-scope department at the City of Bryan. These validation documents must follow the strict guidelines of the PCI Security Standards Council. The report documents the QSA observations, results of tests and findings. Vaco Risk Solutions will provide a copy of each validation report to the City of Bryan for internal management to review and comment. Any agreed upon necessary corrections will be updated in the Final SAQs/ ROCs.
- Additionally, for each SAQ/ROC the City of Bryan is required to complete an Attestation of Compliance (AOC) as a merchant. The AOCs are to be submitted to the processor by the City of Bryan. Vaco Risk Solutions will provide City of Bryan with the required documents.
- Additionally, for each SAQ/ROC the City of Bryan is required to complete an Attestation of Compliance (AOC) as a merchant. The AOCs are to be submitted to the processor by the City of Bryan.

Task 3: Assisting with Archiving Artifacts

- Vaco Risk Solutions has a secure extranet site that allows the City of Bryan engagement team to share information and documents with the Vaco PCI Team. Because QSAs are required to retain audit work papers, evidence and PCI assessment reports for a period of not less than three (3) years, our secure site will assist us in aggregating all the required retention documents to submit to City of Bryan.

Once compliant with all in-scope requirements, primary deliverables for this phase are:

1. Validation Document (SAQs/ROCs)
2. Attestation of Compliance (signed by QSA)
3. Electronic version of the artifacts used to validate compliance

Phase 5: Sustainment and On-Going Compliance

Sustainment

- Oversight
- Compliance Management
- Yearly PCI DSS Assessments and Reporting

The main purpose of this service is to assist the City of Bryan in maintaining a secure PCI environment. By achieving a secure state, it is believed that compliance with any framework can be achieved as well as maintained. Vaco Risk Solutions will provide subject matter experts to augment the current staffing levels with the intent of assisting the City of Bryan with those activities required to maintain compliance and security.

Vaco Risk Solutions will provide oversight, compliance maintenance and yearly PCI DSS assessments and reporting. Our security expert staff will provide direction and opinion as needed, and our PCI Team will provide guidance and assist in verifying daily, weekly, monthly, bi-monthly, and annual compliance-based activities are operating effectively.

The Specific Tasks and Deliverables for Phase 5 are as follows:

Task 1: Oversight

- Vaco Risk Solutions will provide security expert staff to:
  - Provide opinion and direction where required and necessary

Task 2: Compliance Management

- Ongoing Vulnerability Management
  - ASV Scanning
  - Quarterly internal/external vulnerability analysis requirements
  - Penetration testing requirements
- Vaco Risk Solutions will review periodic evidence to verify on-going compliance where applicable for:
  - Log review
  - Anti-malware
  - File Integrity monitoring
  - Badging and Video review
  - Visitor log review
  - Vulnerability Management

    - Quarterly internal/external vulnerability analysis requirements
    - Penetration testing requirements
  - Quarterly user account review
  - Quarterly rogue wireless/networking detection
  - Vendor management
  - Change control
  - Identified threats
  - Risk management
  - Incident response management
  - Vendor due diligence

Task 3: Yearly PCI DSS Assessments and Reporting

- Vaco Risk Solutions will perform annual PCI DSS testing and validation for 4 additional years (2017, 2018, 2019 and 2020) as part of the proposed services.
  - For each year Vaco Risk Solutions will:
    - Update our understanding of the City of Bryan's payment/credit card processing environment
    - Conduct a preliminary assessment (gap analysis) per department to determine readiness for the annual PCI DSS Assessment
      - Provide the City of Bryan a gap report with the recommended remediation actions necessary to proceed with the annual PCI DSS Assessment
    - Conduct applicable PCI DSS version testing per department following applicable remediation, if necessary

The primary deliverables for this phase are:

1. Opinion Tracking Report
2. Annual Gap Analysis Report – Executive Summary with Departmental Details
3. Quarterly Sustainment Report
4. Quarterly ASV Reports
5. Quarterly Internal/External Vulnerability Reports
6. Annual Penetration Results

Once compliant with all in-scope requirements, primary deliverables for this on-going phase are:

7. Annual Validation Document (SAQs/ROCs)
8. Annual Attestation of Compliance (signed by QSA)
9. Yearly electronic version of the artifacts used to validate compliance

2. As stated in Phase 1, the type, timing and format of the progress reports will be defined in cooperation with the City of Bryan and agreed to by the City of Bryan. These will include at a minimum: status reports, remediation tracking reports and evidence request tracking reports.

3. Duties and responsibilities are defined below. Because Vaco is proposing a fixed fee, the projected hours for Vaco are not applicable.

Task	Description	City of Bryan Projected Hours -	Staff
Phase 1: 1	Performing Scoping Assessment	5	Project Manager of City
Phase 1: 2	Developing Project Standards	12	Project Manager of City
Phase 2: 1	Performing a Gap Analysis	20 8	Project Manager of City Department Leads
Phase 2: 2	Reporting of Gaps	1	PRESENTATION
Phase 3: 1	Remediating Gaps	Depends on Gaps	Depends on Gaps
Phase 3: 2	Developing Policies and Procedures	12 4	Project Manager of City Department Leads
Phase 3: 3	Implementing Vulnerability Management Program	16	IT
Phase 4: 1	Re-Testing of Remediated Gaps	6 6	Project Manager of City Department Leads
Phase 4:2	Preparing Validation Documents (SAQ/ROC)	5 1	Project Manager of City Department Leads
Phase 4:3	Assisting with Archiving Artifacts	3	Project Manager of City
Phase 5:1	Oversight	12 per year	Project Manager of City
Phase 5:2	Compliance Management	42 per year 24 per year 36 Per year	Project Manager of City Department Leads IT
Phase 5:3	Yearly PCI DSS Assessments and Reporting	20 per year 20 per year 20 per year	Project Manager of City Department Leads IT

TAB E Vaco References

Company Name/Agency and Address	Scope of Work	Contact Name and Title	Contact Email and Phone
1. Columbus Regional Airport Authority	Perform a Level 1 PCI DSS Version 3.0/3.1 Pre-Assessment; create an IROC documenting gaps and remediation plans. Currently acting as advisement for their remediation effort.	Bob Lowther, Project Manager	Phone: 614-239-6542 Email: rleffler@ColumbusAirports.com
2. Florida League of Cities - Orlando, FL	-8 years PCI DSS Subject Matter Expert Performed PCI awareness seminars for their participating cities. Speakers for Florida of Cities Conventions and the Southeast Municipalities Technology Conference. Contacted by the Florida League of Cities to perform HIPAA Privacy & Security Risk Assessment	Sherry Hilley	Phone: 407-425-9142 Fax: 407-425-9378 Email: shilley@flcities.com
3. City of New Orleans, Louisiana	Performed a comprehensive HIPAA Security Assessment for the City of New Orleans, LA	Dr. Evangeline Franklin, MD, MPH, Director of Clinical Services & Employee Health	Phone: 504-481-7824 Email: erfranklin@cityofno.com
4. FedEx - Memphis, TN	-4 years PCI DSS International consulting including Pre-Assessments, remediation plans, overseeing global remediation effort and subject matter expert for advisement	Tim Carter** ECPMO	Tim.carter@fedex.com (901) 651-6036

TAB F Certification and Acknowledgement of Any Addenda Issued

CITY OF BRYAN

PURCHASING DEPARTMENT

July 14, 2015

ADDENDUM NO. 1

Addendum to City of Bryan Request for Proposal No. 15-048

"PAYMENT CARD INDUSTRY (PCI) COMPLIANCE SERVICES"

Please be advised of the following clarifications, additions, deletions and/or changes to RFP No. 15-048 are hereby made a part of the bid documents for the above referenced project as full and as completely as though the same were included therein.

Q & A:

Q: Has the City of Bryan and or BTU performed a QSA-driven assessment in previous years?

A: No

Q: Has the City of Bryan and or BTU completed any SAQs in previous years? If yes, how many and what type?

A: No

Q: Item "A", page 10, "Intent and Scope of Work" – Is this deliverable to be acknowledged as a full, formalized risk-assessment per PCI DSS requirement 12.2?

A: Yes

Q: Item "B", page 11, "Intent and Scope of Work" – Is there a remediation timeline and budget currently approved and available, or will a budget be approved and timeline created based on these findings?

A: Timeline and budget for remediation will be created based on these findings.

Q: Item "E", page 11, "Intent and Scope of Work" – Is this item assuming that the entire City of Bryan environment will be covered under a single SAQ D, or is there a possibility for multiple SAQs?

A: Multiple SAQ's will be an inevitability.

Q: Is completion of the SAQ(s) assumed to be completed by the City of Bryan with advisory assistance, or will the winning bidder be completing the SAQ?

1309 E. Martin Luther King St. • Bryan, TX 77803
(979) 209-5500 • Fax: (979) 209-5507
http://www.bryantx.gov/departments/?name=purchasing

A: The winning bidder shall provide assistance in the completion of each SAQ.

Q: How many devices are within the CDE of the City of Bryan? And BTU?

A: Refer to fig 1 and Fig 2 in the RFP specs.

Q: How many network segments exist outside of the CDE of the City of Bryan? And BTU? (i.e user, VOIP, Wireless, Admin, etc)?

A: City of Bryan - 0 and BTU – 0. CDE is on same network segment as all network devices.

Q: How many applications are on the Internet that accept credit card payments for the City of Bryan? And BTU? How do these sites handle payment transactions?

A: City of Bryan - 5 and BTU – 1. Pass CHD to third party processor/gateway. Then a code is received for payment status.

Q: How many applications on the internal networks (of the City of Bryan, And BTU) accept credit card payments? How do these applications handle payment transactions?

A: There are 8 applications. Cardholder data (CHD) is passed to third party credit card processors/gateways. A code is returned with the status of the payment.

Q: How many user levels are there inside these applications (i.e. user, admin, power user, customer, partner, etc)?

A: Most applications conform to the following user levels: Administrator, Finance Team, Finance Manger, CSR Team, CSR Manager, and Customer.

Q: Item "5" Page 11 What is the current state of the existing Policies and Procedures in general?

A: Nonexistent.

Q: Approximately how many P&Ps are anticipated to need to be created?

A: Individual policies and procedures should be created for each application that accepts credit cards.

Q: Would it be acceptable to the City if the proposing vendor would have a sub-contractor who is a QSA/ASV?

A: It is the City of Bryan/BTU preference that there are no third party arrangements for this service.

Purchasing Department
1309 E. Martin Luther King St. • Bryan, TX 77803
(979) 209-5500 • Fax: (979) 209-5507

VACO
Free Yourself.

END OF ADDENDUM

This addendum shall be signed and included with your response package as acknowledgement of the addendum. Failure to acknowledge and submit any addenda may be cause for the bid to be rejected. The City's decision to accept or reject a bid due to a failure to acknowledge and submit addenda shall be final.

Suzanne H. Miller, PHD
Vendor Acknowledgement Signature

Karen Sonley
Karen Sonley, Buyer
City of Bryan - Purchasing

Purchasing Department
1309 E. Martin Luther King St. • Bryan, TX 77803
(979) 209-5500 • Fax: (979) 209-5507

VACO
Free Yourself.

CERTIFICATION AND AUTHORIZATION

CERTIFICATION and AUTHORIZATION:

The undersigned certifies that he has fully read **RFP # 15-048** and understands this "Request for Proposal" and has full knowledge of the scope, quantity, and quality of the services to be furnished and intends to adhere to the provisions described herein. The undersigned also affirms that they are duly authorized to submit this proposal, that this proposal has not been prepared in collusion with any other Vendor, and that the contents of this proposal have not been communicated to any other Vendor prior to the official opening of this proposal. Additionally, the undersigned affirms that the firm is willing to sign the enclosed Exhibit A, Standard Form of Agreement Contract.

By submitting a proposal, the vendor certifies that neither he, nor any co-owner of the organization submitting this proposal, is related to a member of the City Council of the City of Bryan within the first, second, or third degree of consanguinity (blood) or affinity (marriage).

Signed By: Suzanne H. Miller, PhD Title: PARTNER

Typed Name: SUZANNE MILLER, PHD Company Name: VACO RISK SOLUTIONS, LLC

Phone No.: 321 282-8516 Fax No.: 901 333-2252

Email: DRMILLER@VACO.COM

Bid Address: 6000 POPLAR AVE, ST. 216 MEMPHIS TN 38119
P.O. Box or Street City State Zip

Order Address: 6000 POPLAR AVE., ST. 216 MEMPHIS TN 38119
P.O. Box or Street City State Zip

Remit Address: 6000 POPLAR AVE., ST. 216 MEMPHIS TN 38119
P.O. Box or Street City State Zip

Federal Tax ID No.: 46-1270591

Date: 7-29-2016

END OF RFP #15-048

Appendix A Executive Summary of Management Team

1. Suzanne Miller, Ph.D. – Partner Lead
2. Kathy Brackenrich – QSA Project Manager

Suzanne H. Miller, Ph.D.

VACO Free Yourself.

Suzanne H. Miller, Ph.D., CHS-III, CPT, CISM, CRISC, CISA, PCI-QSA

Partner

AREAS OF PRACTICE

Information systems auditing, regulatory compliance (HIPAA, HITECH, SOX and GLBA), frameworks (CobiT, COSO, NIST, and ISO27005-2011), PCI DSS, IT general controls (ITGC), application controls (AC), IT entity-level controls, segregation of duties, information security curriculum development, policy and procedure development, controls documentation and implementation, business process engineering (BPE), system development life cycle (SDLC), IT process improvement, mitigation, business contingency plans, risk management, computer forensics, data mining

INDUSTRY LINES

Publicly Traded Companies, Healthcare, Hospitality, Manufacturing, Service Industry, Real Estate, Education, Telecommunications, Law Enforcement and Correctional, Logistics, Auto Dealerships, Insurance, Governments - State, County and Local

COMPUTER APPLICATIONS

-Accounting *(PeopleSoft, SAP, Oracle Financials, Great Plains, Solomon, MAPIC, Sage, MACC, Lawson, FoodStar)*
-Reporting Tools *(FRX, Crystal Report Writer, Touchpoint)*
-CRM *(Siebel, PeopleSoft, Front Page)*
-Tools *(ACL, Qualys, NetIQ, Sekchek, Bindview, LAN Manager, Tripwire, Remedy, Turnover, Bsafe, Crypto, Endevor, UC4, Lotus Notes, HEAT, Track-It, MS Office Suite, COGNOS Business Intelligent Suite, Symantec Suite, Hyperion, SPSS, EnCase, dd, Ghost, eAudit+)*
-Operating Systems *(Windows, UNIX, OS400, AIX UNIX, Linux, RACF)*
-Databases *(SQL, DB2, Oracle, Foxbase/Foxpro, Access)*
- Additional Applications *(ERP, LMS, EMR EHR, Education Record Keeping Management Systems, Hospital/ Medical/Lab/Radiology/EMS Systems)*

EDUCATION/QUALIFICATIONS

BS, University of Tennessee, Mathematics Education
MS, University of Missouri, Mathematics Education
Ph.D.-Candidate, University of Michigan, Mathematics
Ph.D., Oregon State University, Computer Science Education

PROFESSIONAL EXPERIENCE

Dr. Miller has extensive and successful experience in risk-based, cost effective information security mentoring and guidance for organizations. She has strong leadership and extensive management skills in mitigating companies for PCI/SOX/HIPAA/Red Flag Rule compliance by re-structuring control designs/implementation, process re-engineering, workforce education and development of IT Governance (business owners); Particular strength in working with management to turn around HITECH/SOX/PCI projects that are in jeopardy.

PRINCIPAL AREAS OF PRACTICE

Dr. Suzanne Miller uses her expertise in information security and regulatory compliance to help companies align their IT governance, risk management and compliance activities. Her areas of expertise are:

- Performing gap analyses, readiness assessment and pre-assessment in collaboration with an organizations internal audit team; including identification of control weaknesses, development of remediation plans and lead for the mitigation efforts
- Developing of remediation plans using a risk-based, step-by-step approach
- Mentoring and guiding organizations through customized compliance solutions which are specifically defined for the client's environment
- Working with functional groups in the creation of policies, procedures and/or guidelines to ensure the privacy and security of company sensitive information
- Leading corporate-wide security awareness initiative through the use of business owners and education programs
- Cross-walking SOX, HIPAA, PCI and/or other requirements to eliminate duplication of effort.

Additionally, Dr. Miller is the co-author of the *HIPAA Security Toolkit*, *TurboPCI Easy Workbooks* and the *CPA PCI Resource Manual*.

MAJOR PROJECTS

Large Healthcare/Research Provider

- Brought in to "fast track" and lead PCI compliance for a publicly-traded company
- Performed initial PCI Readiness Assessment and developed a Remediation Plan
- Aligned with stakeholders to identify compliance solutions by facilitating workshops and obtaining stakeholder commitment to agreed upon solutions
- Worked with the processor to develop a partnership with the organization in an effort to reduce fines and extend mandate deadlines
- Oversaw the compliance project which brought the organization from being 30% compliant to 100% in 4 months

Manufacturing Company- Medical Devices

Contracted to oversee the planning, designing and implementation of IT SOX project.
Performed all phases of IT Sarbanes-Oxley (SOX) 404 projects. Worked with corporate headquarters to define corporate-wide IT controls that align with SOX and HIPAA, oversaw the implementation of the controls and process re-engineering, developed control matrix, developed policies and procedures, developed test plans and conducted controls testing activities, developed and coordinated remediation plans
Completed project ahead of schedule and under budget
Due to contract extension, leveraged SOX work to perform a PCI gap analysis and develop a remediation plan
Mentored and guided the organization through the remediation and annual PCI compliance reporting

Logistics Company – International Fortune 50 Company

- Brought in to develop and implement a PCI Global compliance plan by working directly with processors and brands
- Designed and implemented a cross-cultural discovery methodology to identify global business processes that have access to or impact the security of cardholder data
- Designed and implemented a cross-cultural gap analysis to identify global PCI gaps
- Developed in cooperation with management a global remediation strategy

Large Hospitality Organization

- Restructured the analysis division to incorporate data warehousing and data mining
- Implemented end-to-end process management systems in conjunction with reengineering the data flow
- Implemented a SDLC (System Development Life Cycle) methodology to design, develop and implement a global contact management system for Latin America and Ritz Carlton Divisions which was 60% less than outside vendors and was rolled out ahead of schedule

Certified Information Security Manager (CISM) - Information Systems Audit and Control Association (ISACA)
Certified Information Security Auditor (CISA) - Information Systems Audit and Control Association (ISACA)
Certified Risk and Information Systems Controls (CRISC) - Information Systems Audit and Control Association (ISACA)
Certified Performance Technologist (CPT) - International Society for Performance Improvement (ISPI) Certified Homeland Security (Technology) (CHS-III) – American College of Forensic Examiners International (ACFEI)
Qualified Security Auditor (QSA) – PCI Security Standards Council (PCI SSC)

Kathy Brackenrich

VACO
Free Yourself.

Kathy Brackenrich QSA, PCIP, CISA, CRISC

Compliance

Areas of Practice

Project Management, Resource Management, Information Security scoping and assessing, PCI validation requirements, Information Security management, Policy and Procedure review and development, controls documentation, mitigation, Risk Management Remediation Management, System Development Life Cycle (SDLC), Disaster Recovery/Business Continuity, IT Governance frameworks (COBIT)

Industry Lines

Global Transportation, Retailers, Healthcare, Fundraising, Consumer Services, Manufacturing

Computer Applications

Tools *(Qualys, Sekchek, MS Office Suite, BaseCamp)*
Operating Systems *(Windows, AS400, Unix Linux)*
Databases *(SQL, Access, Quickbase)*

Education

BS, Arkansas State University
Management Information Systems

Qualifications

Certified Information Security Auditor (CISA) Certified Risk and Information Systems Controls (CRISC), Qualified Security Auditor (QSA), Payment Card Industry Professional (PCIP)

Professional Experience

- QSA, PCIP, CISA, CRISC certified senior professional with 15+ years' experience in IS security and risk management services.
- Experienced in Sarbanes-Oxley, PCI-DSS, Operational audits, Information Technology audits, Financial Statement audits, internal audits, external audits, business analysis and requirements gathering, project management familiarity with HIPPA, FISMA.
- Knowledgeable of relevant professional standards including COSO, COBIT, ISO/IEC 27001:2005, PCI DSS.
- Knowledgeable of business process in the retail, manufacturing, logistic services, financial services, telecommunications, e-commerce and government industries.

Principal Areas of Practice

Kathy conducts information security and regulatory compliance assessments and audits. Her areas of expertise consist of the following:

- Serving as Project Manager for compliance assessments
- Maintaining Budget to Actuals for each project
- Mentoring and assisting team members in various types of assessments
- Planning and performing information system audits, special reviews and testing
- Performing detailed testing, analysis, and validation of systems, processes and controls
- Coordinating interviews and artifact gathering schedules between team members and client
- Compiling accurate documentation of test results for submission to client
- Identifying and presenting control weaknesses to the audit team and client
- Developing of remediation plans using a risk-based approach
- Creating standard policies and procedures for Compliance Assessments
- Leading and participating in special projects
- Cross-walking SOX, HIPAA, PCI and/or other requirements to eliminate duplication of effort

Major Projects

Major Store Retailer

PCI DSS engagement for Level 1 Merchant, 850 Locations

Global Non-Profit Organization

PCI DSS engagement for Level 2 Merchant

Global Transportation

PCI DSS engagement for Level 1 Merchant, 571 Locations

Consumer Services

PCI DSS engagement for Level 2 Merchant, 650 Locations

Certified Information Security Auditor (CISA) - Information Systems Audit and Control Association (ISACA)
Certified Risk and Information Systems Controls (CRISC) - Information Systems Audit and Control Association (ISACA)
Qualified Security Auditor (QSA) – PCI Security Standards Council (PCI SSC)
Payment Card Industry Professional (PCIP) - PCI Security Standards Council (PCI SSC)

VACO RISK SOLUTIONS
Free Yourself.

Commitment to Serve

Response to Request for Proposal

Payment Card Industry (PCI) Compliance Services
RFP # 15-048

Presented: July 30, 2015

Bryan Texas Utilities (BTU)
Purchasing Department
1309 E. Martin Luther King St.
Bryan, TX 77803

Vaco Risk Solutions - Houston
3200 Southwest Fwy #3030
Houston, TX 77027

713.960.9898

Vaco Risk Solutions
6000 Poplar Ave, Suite 216
Memphis, TN 38119
Dr. Suzanne Miller, Partner
901.333.2250

Table of Contents

Table of Contents 2

Letter of Introduction 3

TAB A - Qualifications and Experience 4

TAB B Rates and Expenses 9

TAB C Project Time-Line 10

TAB D Methodology 11

TAB E Vaco References 21

TAB F Certification and Acknowledgement of Any Addenda Issued 22

Appendix A Executive Summary of Management Team 26

Letter of Introduction

July 30, 2015

Vaco Risk Solutions (Vaco) is pleased to respond to Bryan, Texas' (City of Bryan) request for Qualified Security Assessor (QSA) Services for PCI Compliance Certification RFP # 15-048 (RFP), hereby incorporated by reference, including addendums.

Our proposal is a collaborative effort among Vaco Risk Solutions partners Stephen J Schaefgen and Suzanne Miller. Dr. Miller is heading our proposal team and may be contacted at 407-575-7343, or by mail at 6000 Poplar Avenue, Suite 216, Memphis, TN 38119. Vaco Risk Solutions and Vaco are two members of the Vaco Family of offices, a national staffing and services company. Vaco Risk Solutions is the successor company of the merger of Compliance and Audit Group and VCAG LLC. VCAG subsequently was renamed Vaco Risk Solutions.

Our proposal, including our named delivery team, is valid for 180 days. Vaco Risk Solutions also confirms its agreement with the provisions of the Draft Standard Form of Agreement Contract for the City of Bryan.

Our proposal consists of the sections outlined in the Table of Contents including our statement of services and delivery approach, qualifications, resources and such other items as requested by the City of Bryan in its RFP.

Along with our professional expertise, focus on project management, and overall audit efficiencies, we bring three critical distinguishing factors to your PCI compliance efforts:

1. As the 15th QSA company our dedicated Vaco PCI Team has extensive PCI DSS expertise
2. A proven fresh approach to PCI assessments based on successful engagements
3. A collaborative business partner approach providing sustainable solutions and guidance for improving efficiencies

These elements and Vaco Risk Solutions' national network of resources, provide the framework for meeting City of Bryan's assessment and certification requirements.

We look forward to the opportunity to meet City of Bryan's QSA PCI assessment and compliance needs using our proven approach, delivered by proven professionals.

Sincerely,

Suzanne M. Miller, PhD

Suzanne Miller, Ph.D.
Partner

TAB A - Qualifications and Experience

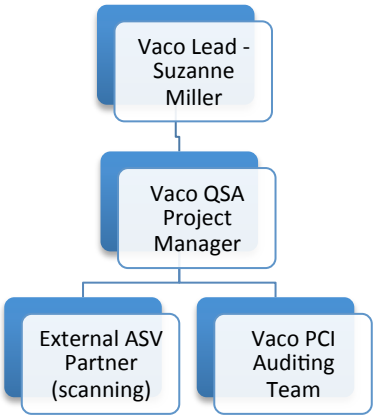
1. Vaco Risk Solutions LLC is a Premier Consulting Company. We are a specialized member of the Vaco family of companies.

   - Founded in 2002
   - Headquartered in Tennessee
   - 30 Locations Nationwide
   - 3000+ Employees
   - Over $200 Million in Annual Revenue
   - Vaco has been named as one of the *Fastest Growing Companies in America* by Inc. Magazine for eight consecutive years

Summary of Administration, Organization and Staffing of Vaco Risk Solutions, LLC

Vaco Risk Solutions (VRS) is a Limited Liability Company organized in the State of Tennessee and is an affiliated member of the Vaco LLC group of companies, which includes Vaco-Houston. VRS leadership and administration is led by partner/members including Mr. Schaefgen, president, and two partners, and Dr. Miller and Gourav Mukherjee. VRS has a team of 22 professionals including five (5) Qualified Security Assessors (QSAs).

Organization chart of people on this engagement



2. Vaco Houston will be servicing this account.

3. In 2007 Vaco Risk Solutions (under the name of Compliance and Audit Group) became the 15th QSA Company. Vaco partners with Qualys for PCI DSS Approved Scanning Vendor (ASV) services. Our lead partner at Qualys is Mr. Paul Passey CISSP, CISM, CIPP, Technical Account Manager, Southeast US Field Operations, 1600 Bridge Parkway Redwood City, CA 94065, 919-610-0088.

4. Vaco Risk Solutions has the experience and capability to provide the following services:

    a. Initial PCI Gap Analysis
    b. Annual requirement for a PCI Pen Test
    c. Internal and external scanning
    d. PCI DSS Assessment Version 3.1 (or version current at the time of the Assessment
        - Upon successful validation of all requirements being in place, a completed SAQ or ROC (depending on the level of the merchant) will be presented to the merchant.
        - Also upon successful validation, an Attestation of Compliance (AOC) will also be presented to the merchant.
    e. Recommendations and remediation support
    f. Policy, procedure and program development
    g. Sustainment program in the form of an annual PCI compliance lifecycle (see b above)
    h. Besides performing the required scans, periodic vulnerability scans will also be performed.

5. Examples of details of PCI consulting services performed for past engagements:

    1) A multi-level marketing company, required to be PCI compliant globally, needed help in reaching compliance with the 15,000 global customers who were selling products and taking credit/debit card data (acting as independent sales reps). Vaco Risk Solutions developed a strategy to bring the 15,000 global customers/independent sales reps into compliance within 6 months and sustain ongoing compliance.
    2) Vaco Risk Solutions was hired by a billion dollar charity that was unaware of the PCI requirements until their processor called. Once Vaco Risk Solutions was able to bring the organization into compliance, Vaco Risk Solutions introduced the charitable organization to other processors who were willing to dramatically reduce the interchange rate of the now compliant organization. Over $500,000 a year is being saved from this cost reduction.
    3) Vaco Risk Solutions was contracted to perform a PCI DSS Gap Analysis. During the analysis, Vaco Risk Solutions discovered that the multi-million dollar contract for outsourcing IT services required the client to complete a form booklet which outlined the PCI Compliance Services the client expected the IT company to perform. During discovery, Vaco Risk Solutions found the empty document in a file cabinet in legal. Vaco Risk Solutions was further contracted to work with the IT provider in defining and overseeing the implementation of required controls.

6. Currently, Vaco Risk Solutions performs the following PCI DSS services:

Number	PCI DSS Services (QSA)
1	PCI Gap Analysis
2	PCI Sustainment Program
3	PCI DSS Assessments
4	Vulnerability Assessments
5	Penetration Testing
6	Data Loss Prevention – eDiscovery Cardholder Data
7	Incident Response Planning
8	Policy and Procedures Development
9	Education and Training
10	Vender Management Assessments
11	Remediation Support
12	EMV Advisory Service
13	Tokenization Advisory Service
14	P2PE Advisory Services
15	Redaction Services
16	RFP Writing Service

Number	PCI DSS Services – Qualys (ASV)
1	ASV Scans
2	ASV Scans – Online help and 24x7x363 email/telephone support
3	ASV Scan- User-friendly interface
4	PCI Web Application Scanning
5	Qualys Cloud Platform - Vulnerability scanning with remediation and risk management
6	Qualys Auto-Submit - Compliance status is electronically submitted to acquiring bank

7. Project Manager and Individuals on the Vaco Engagement Team

Suzanne Miller and Kathy Brackenrich will provide QSA leadership for this project. As more fully described in their resumes in Appendix A, Dr. Miller and Ms. Brackenrich bring the following to the engagement:

1. <u>Suzanne Miller:</u>
    - Dr. Miller has performed over 210 onsite assessments for Level 1, Level 2, Level 3 and Level 4 Merchants.
    - Qualified Security Auditor (QSA)
    - Payment Card Industry Professional (PCIP)
    - Certified Information Security Manager (CISM)

- Certified Information Security Auditor (CISA)
- Certified Risk and Information Systems Controls (CRISC)
- Certified Performance Technologist (CPT)
- Certified Homeland Security (Technology) (CHS-III)

2. Kathy Brackenrich:
    - Ms. Brackenrich has performed more than 90 onsite assessments for Level 1, Level 2, Level 3 and Level 4 Merchants and will serve as project manager for the engagement.
    - Qualified Security Auditor (QSA)
    - Certified Information Security Auditor (CISA)
    - Certified Risk and Information Systems Controls (CRISC)
    - Payment Card Industry Professional (PCIP)

In addition to Dr. Miller and Ms. Brackenrich, Vaco intends to use other staff members as needed to deliver the services outlined in our approach and work plan. Members of the Vaco team who may become part of the engagement, as required, include:

- Eddie Salera, CISA, PCIP, QSA
- Michael Spiotta, PCIP, CISA
- Vicki Luckey, CIA, CISA, PCIP, CRMA
- Laury Garrett, CISA
- Matt Wagenknecht, CREA, CISSP, MCSE, MCP+1
- Gourav Mukherjee, JD, QSA, CISA, CISSP, CRISC

Key personnel identified for this project will be available for the duration of the project. No key personnel will be removed or otherwise replaced by Vaco without prior written concurrence by the BTU. As noted earlier, Vaco Risk Solutions has access to the 30 offices of Vaco and a complement of resources to ensure supplemental resources are available.

8. Overview of Engagement Team

Vaco Risk Solutions methodology for performing PCI Consulting engagements is centered on a Team Approach. At Vaco Risk Solutions we believe having a team that can provide specialized expertise brings greater value to our clients without increasing costs.

The Vaco PCI Team assigned to perform the services of this engagement are committed to the project and guaranteed by Vaco Risk Solutions except in the case of unforeseen personal events.

9. Municipal Staff Support should include the following:

Support Staff	Role
Project Manager (PM)	Provide project management for the BTU
Department Lead	Every department lead should be the PCI overseer for the department by responding to requests, overseeing and reporting remediation efforts, attending status calls and reporting compliance issues.
IT Lead	IT lead should be the PCI overseer for the IT department by responding to requests, overseeing and reporting remediation efforts, attending status calls and reporting compliance issues.

.

10. Vaco Risk Solutions is not involved in nor has it been involved in any litigation performance or otherwise over the last five (5) years.

11. Vaco Risk Solutions has not had any contracts terminated due to non-performance over the last five (5) years.

12. Vaco Risk Solutions has not had any adverse actions sanctioned by any regulatory authorities over the last five (5) years.

TAB B Rates and Expenses

1. Vaco Risk Solution proposed fee schedule.

	FYE 2016	FYE 2017	FYE 2018	FYE 2019	FYE 2020
Fixed Fee Price	$53,704	$44,776	$41,310	$38,536	$34,654
Administrative Fee (Consulting) *Not to exceed*	$49,204	$41,776	$38,310	$35,536	$31,654
Travel Expenses	$4,500	$3,000	$3,000	$3,000	$3,000

2. Vaco Risk Solutions' expectations concerning reimbursement for travel include flight, hotel, car rental and meals reflect the travel policy of the City of Bryan.

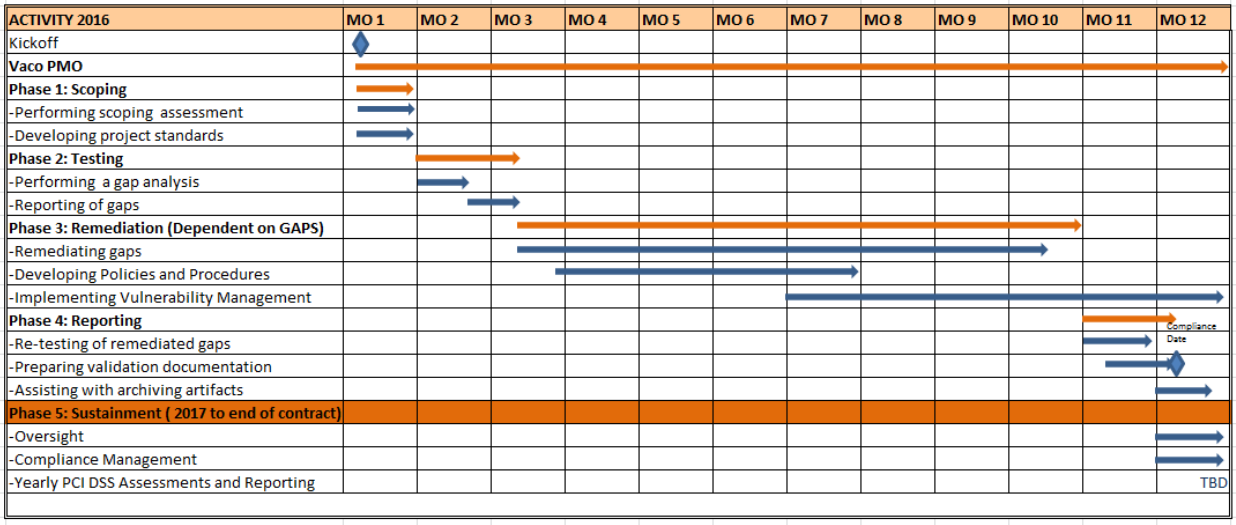
3. Vaco Risk Solutions understands prior approval by an authorized City representative is required for travel related expenses chargeable to the City.

4. Vaco Risk Solutions will not seek reimburse for charges other than approval travel expenses (See TAB B, 2).

5. Vaco Risk Solutions understands expenses not specifically listed will not be considered reimbursable.

TAB C Project Time-Line

1. Timeline for Project

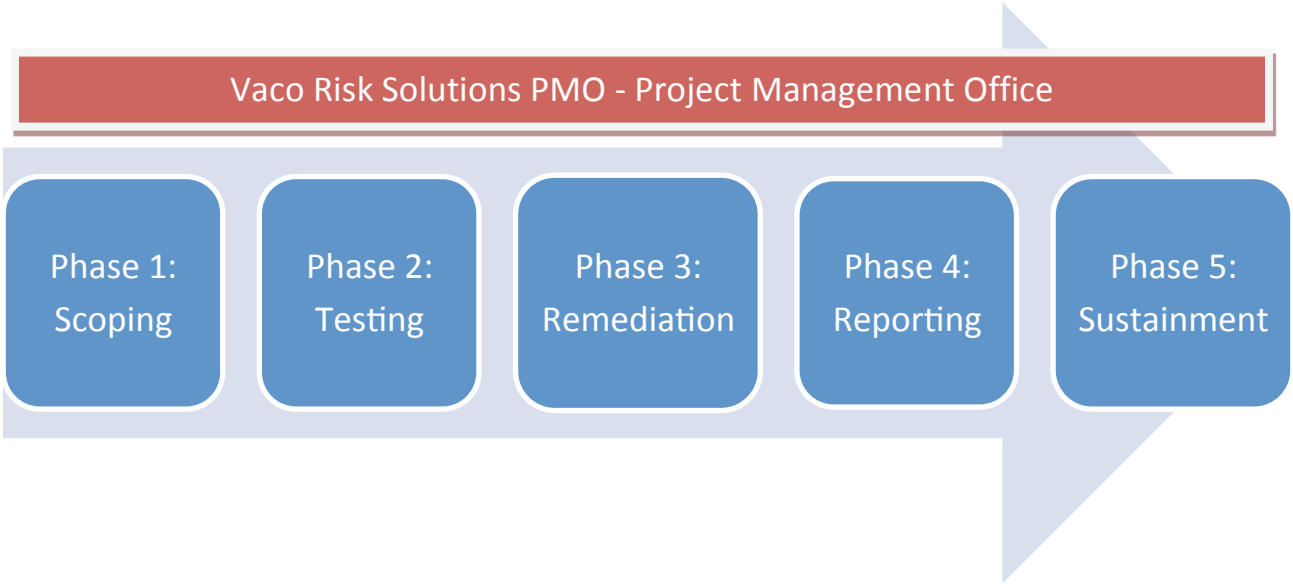


2. Phase 1 and 2 will be completed in 10 weeks. The completion of Phase 3 is dependent on the results of the gap analysis. Phase 4 will be completed in 8 weeks. Phase 5 scheduling will be addressed at the end of Phase 4.

TAB D Methodology

1. Vaco Risk Solutions PCI DSS Methodology

Based upon the scoping information provided by BTU, the Vaco Risk Solutions PCI methodology that has been adapted to incorporate Vaco Risk Solutions' best practices is depicted below:



Each of the activities and phases are described in detail below.

Vaco Risk Solutions Project Management Office (PMO)

Vaco Risk Solutions PMO - Project Management Office

Vaco believes a structured and effective Project Management Office (PMO) will be a crucial element of the BTU's roadmap to achieve compliance in a timely manner. The Vaco Risk Solutions PMO will plan and coordinate all aspects of the project from scoping through the planning and execution. An effective PMO requires several factors including a disciplined PMO approach, as well as a PMO leader who has extensive experience managing PCI Assessments.

The Vaco PMO will coordinate all PCI activities, resources, teams, training, communications, and document management. Vaco Risk Solutions' approach also establishes a PMO that will serve as a single point of contact for BTU including updates for the Project Sponsor.

Key PMO Activities:

- Establish the PCI project office
- Create and monitor the overall PCI project plan (for all tasks and locations)
- Monitor progress, issues, milestones and deadlines for all PCI activities
- Secure resources as needed

- Coordinate and schedule activities across teams, business units and geographies
- Develop, maintain, and roll-out project tools and standard templates
- Coordinate quality assurance and risk management activities
- Establish and communicate project governance processes
- Coordinate PCI communications and change management activities
- Coordinate all training activities and materials
- Initiate knowledge sharing activities between Vaco Risk Solutions and BTU

Key PMO Deliverables:

- Project plan
- Periodic status reports (e.g. weekly)
- Issue tracking reports
- Progress updates for BTU's Project Sponsor
- Communications plan
- Standard document templates
- Document repository

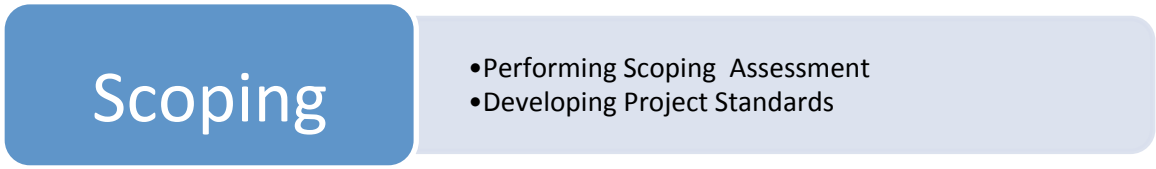
Vaco Risk Solutions' PMO methodology is based on our experience and makes use of a structured approach to coordinate PCI activities.

We believe a high level of project reporting and discipline is necessary to help ensure that any potential delays are identified and corrected as soon as possible. Therefore, the Vaco Risk Solutions PMO will provide periodic updates on the status of the project to the project sponsor.

At the conclusion of this step, the project organization, roles, and responsibilities will be clearly documented. A detailed project plan will be prepared and reviewed with BTU. Project tracking and communication mechanisms will be established.

Phase 1: Scoping

We believe that the planning/scoping phase is the most important phase of the project. The key steps included in this phase are listed below and an explanation of each follows.



Task 1: Performing Scoping Assessment

We will begin by identifying and clarifying the in-scope cardholder data processes and environment. All people, departments, facilities, devices, systems, applications and databases that store, process or transmit cardholder data will be documented and defined as the cardholder data environment. These

documents will be written with the "end in mind" as the PCI standards requires the BTU to attest to their cardholder data environment in each Attestation of Compliance (AOC).

Task 2: Developing Project Standards

Standardizing the assessment process across the BTU will help to create time and resource efficiencies. Working with the BTU, the documents for the projects will be identified and the format of the documents will be established. Additionally, the repository for the assessment documentation will be identified, and the BTU will identify their team member(s) who are responsible for interfacing with and representing the departments during meetings and providing the artifacts on a timely basis. Based on our past experience we have found consistency and timeliness of meetings to be a key success factor to PCI Validation. Working with the BTU, a calendar of meetings will be scheduled for the duration of the project.

At the conclusion of the planning phase, we will work with the applicable department members of the BTU to finalize the approach and detailed work plan. The work plan will include the activities and timing to be performed.

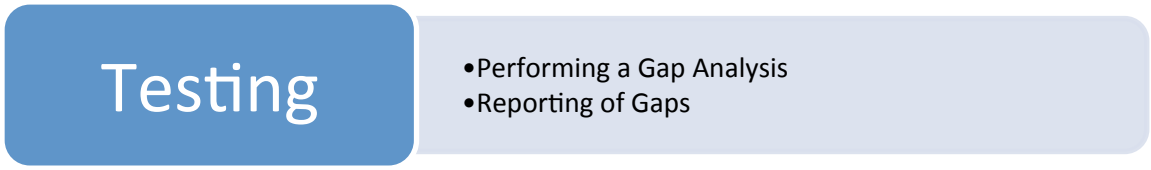
The project team will present the project plan to BTU project sponsor for review and approval. We believe this is an important step to ensure that the approach is appropriately documented and that there is appropriate "buy-in" from key stakeholders.

The primary deliverables for this phase are:

1. Comprehensive Work Plan for Vaco and the BTU
2. Project Reporting Templates
3. Scoping Report – Identification of Validation Types (SAQs or ROCs) per Department

Phase 2: Testing

There are defined testing procedures that are required by the PCI Security Standards Council (PCI SSC).



It is important to note that we are required to test all PCI controls required per validation method as per the PCI Data Security Standard Requirements and Auditing Procedures Version 3.1. See www.pcisecuritystandards.org for a download of this document and PCI DSS version 3.1 SAQs.

For each requirement, the Vaco PCI Team will identify the artifacts that are necessary to validate compliance. The Vaco PCI Team will also be using state-of-the art assessment tools to review vulnerabilities, server policies, access controls and firewall/router settings. If during this phase, for

requirements which are found to "not be in place", Vaco will recommend actions to remediate the gaps. See Phase 3.

The Vaco PCI Team will request and review required documents. These will include documents such as: network diagrams, configuration documentation, awareness training content, and lists of terminated employees, employees' roles and responsibilities, copies of audit reports, quarterly scan reports, penetration tests, Intrusion Detection System (IDS) logs and other necessary documents.

The Vaco PCI Team is required to interview selected employees to ensure that they have an understanding of the BTU's security policies and procedures. During certain interviews, the Vaco PCI Team may validate workstations or swipe devices that connect to the BTU cardholder environment to ensure anti-virus, personal firewall and other access control requirements are consistent with PCI DSS requirements.

The Vaco PCI Team will visit the locations where cardholder data is processed or stored to ensure that cardholder data security procedures are consistent with written policies and adequate to protect cardholder data.

For each type of system in the card-processing environment, the Vaco PCI Team will inspect network and system configurations, firewall and router access control rules and database schemas and configuration. The Vaco PCI Team will confirm that prohibited data, such as sensitive authentication data, is not retained after authorization and that PAN (primary account number) data is encrypted during storage and over open public networks.

The Vaco PCI Team will conduct site inspections to ensure that physical security controls are adequate to protect the cardholder data. Physical media storage will also be inspected to ensure confidential data is labeled and protected in accordance with PCI DSS requirements.

The specific tasks and deliverables for Phase 2 are as follows:

Task 1: Perform a Gap Analysis

- Pre-Assessment (Gap Analysis) Activities per Department
  - Review Department's current payment card processes and data flows to identify the cardholder data environment and in-scope people, processes and technology
  - Interview Department's key staff to understand the existing controls around the cardholder data environment.
  - Walk-throughs of the Department's card-present and card-not-present payment processes at each department. Walk-throughs will include the following:
    - All people, processes and technology used to transmit, process or store cardholder data (CHD)
    - Physical location site visit(s)

- Applications that support the business processes for payment card processing and transmission
- Where subtle differences in processes and/or technology may exist for individual merchant IDs at these or other locations/properties, these will be explored by interview.
- Third party websites and gateways

➢ Evidence Gathering and Testing of the applicable requirements/sub-requirements through:
- Observation of system settings and interviews with responsible personnel
- Review of requested documentation
- Observation of processes, actions and state of in-scope components
- On-site physical review locations

Task 2: Reporting Gaps

❖ Initial Report on Compliance (IROC) -Gap Analysis Report
- ➢ Evaluate all collected information against PCI DSS 3.1 SAQ/ROC requirements and report thereon, including Compensating Controls and/or Explanations for non-Applicability, as applicable
- ➢ Provide design suggestions to reduce or manage technical scope
- ➢ Document gap analysis issues and provide prioritized remediation recommendations including detailed technical artifacts to support identified gaps
- ➢ Create the Initial Report on Compliance (IROC) and submit in electronic format to the BTU

The primary deliverable for this phase is:

1. Gap Analysis Report – Executive Summary with Departmental Details

Phase 3: Remediation

During the testing phase, any requirements that are found to not be in place will require remediation. Once deficient controls are remediated, Vaco Risk Solutions will re-test these remediated controls.

The specific tasks and deliverables for Phase 3 are as follows:

Task 1: Remediating Gaps

During the remediation efforts, Vaco Risk Solutions will assist BTU by providing subject matter expertise (SME) to assist with defining processes and procedures and recommending technical solutions. Assisting with the implementing of technical solutions is not in-scope for this project. Upon request, Vaco Risk Solutions will assist the BTU with staff augmentation for resource support.

- Remediation Consultation and Assistance
  - Following the IROC, Vaco Risk Solutions will:
    - Provide remediation consultation to BTU's project team to assist with implementation of processes and procedures to comply with PCI DSS version 3.1 certification requirements
    - Provide remediation assistance at BTU's separate request. The scope and extent of this assistance will be quoted to the Authority separate from this proposal based upon the results of the initial gap analysis produced in Phase 2.

Task 2: Developing Policies and Procedures

Vaco PCI Team will work in cooperation with the BTU to develop city-wide PCI DSS policies and procedures per validation type.

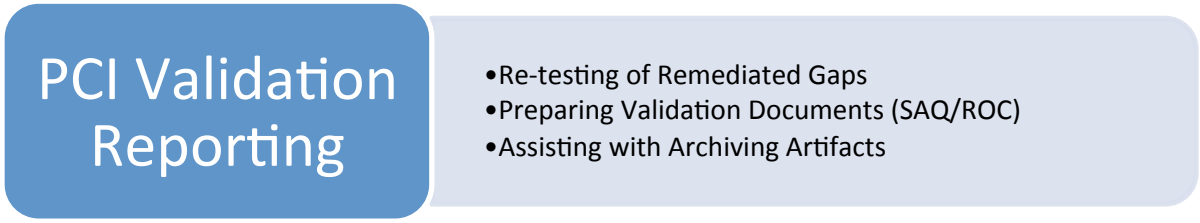
Task 3: Implementing Vulnerability Management Program

- Vaco PCI Team and Qualys will initiate the Vulnerability Management Program, where applicable. This includes the following:
  - ASV external scanning
  - Penetration Testing
  - Internal scanning

The primary deliverables for this phase are:

1. PCI DSS Version 3.1 Policies and Forms Templates
2. ASV Scan Results
3. Penetration Test Results
4. Internal Scan Results

Phase 4: PCI Validation Reporting



The Specific Tasks and Deliverables for Phase 4 are as follows:

Task 1: Re-Testing of Remediated Gaps

Following each department's successful completion of applicable remediation, Vaco Risk Solutions will:

- Perform re-testing of the remediated gaps
  - Upon successful re-testing:
    - Prepare the validation documents
    - Archive the artifacts

Task 2: Preparing Validation Documentation

- Among the other functions that are required for PCI DSS assessments, Vaco Risk Solutions will prepare the SAQ/ROC for the BTU. These validation documents must follow the strict guidelines of the PCI Security Standards Council. The report documents the QSA observations, results of tests and findings. Vaco Risk Solutions will provide a copy of each validation report to the BTU for internal management to review and comment. Any agreed upon necessary corrections will be updated in the Final SAQ/ ROC.
- Additionally, for each SAQ/ROC the BTU is required to complete an Attestation of Compliance (AOC) as a merchant. The AOCs are to be submitted to the processor by the BTU. Vaco Risk Solutions will provide BTU with the required documents.
- Additionally, for each SAQ/ROC the BTU is required to complete an Attestation of Compliance (AOC) as a merchant. AOCs are to be submitted to the processor by the BTU.

Task 3: Assisting with Archiving Artifacts

- Vaco Risk Solutions has a secure extranet site that allows the BTU engagement team to share information and documents with the Vaco PCI Team. Because QSAs are required to retain audit work papers, evidence and PCI assessment reports for a period of not less than three (3) years, our secure site will assist us in aggregating all the required retention documents to submit to BTU.

Once compliant with all in-scope requirements, primary deliverables for this phase are:

1. Validation Document (SAQs/ROCs)
2. Attestation of Compliance (signed by QSA)
3. Electronic version of the artifacts used to validate compliance

Phase 5: Sustainment and On-Going Compliance

The main purpose of this service is to assist the BTU in maintaining a secure PCI environment. By achieving a secure state, it is believed that compliance with any framework can be achieved as well as

maintained. Vaco Risk Solutions will provide subject matter experts to augment the current staffing levels with the intent of assisting the BTU with those activities required to maintain compliance and security.

Vaco Risk Solutions will provide oversight, compliance maintenance and yearly PCI DSS assessments and reporting. Our security expert staff will provide direction and opinion as needed, and our PCI Team will provide guidance and assist in verifying daily, weekly, monthly, bi-monthly, and annual compliance-based activities are operating effectively.

The Specific Tasks and Deliverables for Phase 5 are as follows:

Task 1: Oversight

- Vaco Risk Solutions will provide security expert staff to:
  - Provide opinion and direction where required and necessary

Task 2: Compliance Management

- Ongoing Vulnerability Management
  - ASV Scanning
  - Quarterly internal/external vulnerability analysis requirements
  - Penetration testing requirements
- Vaco Risk Solutions will review periodic evidence to verify on-going compliance where applicable for:
  - Log review
  - Anti-malware
  - File Integrity monitoring
  - Badging and Video review
  - Visitor log review
  - Vulnerability Management
    - Quarterly internal/external vulnerability analysis requirements
    - Penetration testing requirements
  - Quarterly user account review
  - Quarterly rogue wireless/networking detection
  - Vendor management
  - Change control
  - Identified threats
  - Risk management
  - Incident response management
  - Vendor due diligence

Task 3: Yearly PCI DSS Assessments and Reporting

- Vaco Risk Solutions will perform annual PCI DSS testing and validation for 4 additional years (2017, 2018, 2019 and 2020) as part of the proposed services.
  - For each year Vaco Risk Solutions will:
    - Update our understanding of the BTU's payment/credit card processing environment
    - Conduct a preliminary assessment (gap analysis) to determine readiness for the annual PCI DSS Assessment
      - Provide the BTU a gap report with the recommended remediation actions necessary to proceed with the annual PCI DSS Assessment
    - Conduct applicable PCI DSS version testing following applicable remediation, if necessary

The primary deliverables for this phase are:

1. Opinion Tracking Report
2. Annual Gap Analysis Report – Executive Summary with Departmental Details
3. Quarterly Sustainment Report
4. Quarterly ASV Reports
5. Quarterly Internal/External Vulnerability Reports
6. Annual Penetration Results

Once compliant with all in-scope requirements, primary deliverables for this on-going phase are:

7. Annual Validation Document (SAQ/ROC)
8. Annual Attestation of Compliance (signed by QSA)
9. Yearly electronic version of the artifacts used to validate compliance

2. As stated in Phase 1, the type, timing and format of the progress reports will be defined in cooperation with the BTU and agreed to by the BTU. These will include at a minimum: status reports, remediation tracking reports and evidence request tracking reports.

3. Duties and responsibilities are defined below. Because Vaco is proposing a fixed fee, the projected hours for Vaco are not applicable.

Task	Description	BTU Projected Hours -	Staff
Phase 1: 1	Performing Scoping Assessment	5	Project Manager of BTU
Phase 1: 2	Developing Project Standards	12	Project Manager of BTU
Phase 2: 1	Performing a Gap Analysis	20 8	Project Manager of BTU Department Leads
Phase 2: 2	Reporting of Gaps	1	PRESENTATION
Phase 3: 1	Remediating Gaps	Depends on Gaps	Depends on Gaps
Phase 3: 2	Developing Policies and Procedures	12 4	Project Manager of BTU Department Leads
Phase 3: 3	Implementing Vulnerability Management Program	16	IT
Phase 4: 1	Re-Testing of Remediated Gaps	6 6	Project Manager of BTU Department Leads
Phase 4:2	Preparing Validation Documents (SAQ/ROC)	5 1	Project Manager of BTU Department Leads
Phase 4:3	Assisting with Archiving Artifacts	3	Project Manager of BTU

Phase 5:1	Oversight	12 per year	Project Manager of BTU
Phase 5:2	Compliance Management	42 per year 24 per year 36 Per year	Project Manager of BTU Department Leads IT
Phase 5:3	Yearly PCI DSS Assessments and Reporting	20 per year 20 per year 20 per year	Project Manager of BTU Department Leads IT

TAB E Vaco References

Company Name/Agency and Address	Scope of Work	Contact Name and Title	Contact Email and Phone
1. Columbus Regional Airport Authority	Perform a Level 1 PCI DSS Version 3.0/3.1 Pre-Assessment; create an IROC documenting gaps and remediation plans. Currently acting as advisement for their remediation effort.	Bob Lowther, Project Manager	Phone: 614-239-6542 Email: rleffler@ColumbusAirports.com
2. Florida League of Cities - Orlando, FL	-8 years PCI DSS Subject Matter Expert Performed PCI awareness seminars for their participating cities. Speakers for Florida of Cities Conventions and the Southeast Municipalities Technology Conference. Contacted by the Florida League of Cities to perform HIPAA Privacy & Security Risk Assessment	Sherry Hilley	Phone: 407-425-9142 Fax: 407-425-9378 Email: shilley@flcities.com
3. City of New Orleans, Louisiana	Performed a comprehensive HIPAA Security Assessment for the City of New Orleans, LA	Dr. Evangeline Franklin, MD, MPH, Director of Clinical Services & Employee Health	Phone: 504-481-7824 Email: erfranklin@cityofno.com
4. FedEx - Memphis, TN	-4 years PCI DSS International consulting including Pre-Assessments, remediation plans, overseeing global remediation effort and subject matter expert for advisement	Tim Carter** ECPMO	Tim.carter@fedex.com (901) 651-6036

TAB F Certification and Acknowledgement of Any Addenda Issued

PURCHASING DEPARTMENT

July 14, 2015

ADDENDUM NO. 1

Addendum to City of Bryan Request for Proposal No. 15-048

"PAYMENT CARD INDUSTRY (PCI) COMPLIANCE SERVICES"

Please be advised of the following clarifications, additions, deletions and/or changes to RFP No. 15-048 are hereby made a part of the bid documents for the above referenced project as full and as completely as though the same were included therein.

Q & A:

Q: Has the City of Bryan and or BTU performed a QSA-driven assessment in previous years?

A: No

Q: Has the City of Bryan and or BTU completed any SAQs in previous years? If yes, how many and what type?

A: No

Q: Item "A", page 10, "Intent and Scope of Work" – Is this deliverable to be acknowledged as a full, formalized risk-assessment per PCI DSS requirement 12.2?

A: Yes

Q: Item "B", page 11, "Intent and Scope of Work" – Is there a remediation timeline and budget currently approved and available, or will a budget be approved and timeline created based on these findings?

A: Timeline and budget for remediation will be created based on these findings.

Q: Item "E", page 11, "Intent and Scope of Work" – Is this item assuming that the entire City of Bryan environment will be covered under a single SAQ D, or is there a possibility for multiple SAQs?

A: Multiple SAQ's will be an inevitability.

Q: Is completion of the SAQ(s) assumed to be completed by the City of Bryan with advisory assistance, or will the winning bidder be completing the SAQ?

1309 E. Martin Luther King St. • Bryan, TX 77803
(979) 209-5500 • Fax: (979) 209-5507
http://www.bryantx.gov/departments/?name=purchasing

A: The winning bidder shall provide assistance in the completion of each SAQ.

Q: How many devices are within the CDE of the City of Bryan? And BTU?

A: Refer to fig 1 and Fig 2 in the RFP specs.

Q: How many network segments exist outside of the CDE of the City of Bryan? And BTU? (i.e user, VOIP, Wireless, Admin, etc)?

A: City of Bryan - 0 and BTU – 0. CDE is on same network segment as all network devices.

Q: How many applications are on the Internet that accept credit card payments for the City of Bryan? And BTU? How do these sites handle payment transactions?

A: City of Bryan - 5 and BTU – 1. Pass CHD to third party processor/gateway. Then a code is received for payment status.

Q: How many applications on the internal networks (of the City of Bryan, And BTU) accept credit card payments? How do these applications handle payment transactions?

A: There are 8 applications. Cardholder data (CHD) is passed to third party credit card processors/gateways. A code is returned with the status of the payment.

Q: How many user levels are there inside these applications (i.e. user, admin, power user, customer, partner, etc)?

A: Most applications conform to the following user levels: Administrator, Finance Team, Finance Manger, CSR Team, CSR Manager, and Customer.

Q: Item "5" Page 11 What is the current state of the existing Policies and Procedures in general?

A: Nonexistent.

Q: Approximately how many P&Ps are anticipated to need to be created?

A: Individual policies and procedures should be created for each application that accepts credit cards.

Q: Would it be acceptable to the City if the proposing vendor would have a sub-contractor who is a QSA/ASV?

A: It is the City of Bryan/BTU preference that there are no third party arrangements for this service.

Purchasing Department
1309 E. Martin Luther King St. • Bryan, TX 77803
(979) 209-5500 • Fax: (979) 209-5507

VACO
Free Yourself.

END OF ADDENDUM

This addendum shall be signed and included with your response package as acknowledgement of the addendum. Failure to acknowledge and submit any addenda may be cause for the bid to be rejected. The City's decision to accept or reject a bid due to a failure to acknowledge and submit addenda shall be final.

Suzanne H. Miller, PHD
Vendor Acknowledgement Signature

Karen Sonley
Karen Sonley, Buyer
City of Bryan - Purchasing

Purchasing Department
1309 E. Martin Luther King St. • Bryan, TX 77803
(979) 209-5500 • Fax: (979) 209-5507

VACO
Free Yourself.

CERTIFICATION AND AUTHORIZATION

CERTIFICATION and AUTHORIZATION:

The undersigned certifies that he has fully read **RFP # 15-048** and understands this "Request for Proposal" and has full knowledge of the scope, quantity, and quality of the services to be furnished and intends to adhere to the provisions described herein. The undersigned also affirms that they are duly authorized to submit this proposal, that this proposal has not been prepared in collusion with any other Vendor, and that the contents of this proposal have not been communicated to any other Vendor prior to the official opening of this proposal. Additionally, the undersigned affirms that the firm is willing to sign the enclosed Exhibit A, Standard Form of Agreement Contract.

By submitting a proposal, the vendor certifies that neither he, nor any co-owner of the organization submitting this proposal, is related to a member of the City Council of the City of Bryan within the first, second, or third degree of consanguinity (blood) or affinity (marriage).

Signed By: Suzanne H. Miller, PhD Title: PARTNER

Typed Name: SUZANNE MILLER, PHD Company Name: VACO RISK SOLUTIONS, LLC

Phone No.: 321 282-8516 Fax No.: 901 333-2252

Email: DRMILLER@VACO.COM

Bid Address: 6000 POPLAR AVE, ST. 216 MEMPHIS TN 38119
P.O. Box or Street City State Zip

Order Address: 6000 POPLAR AVE., ST. 216 MEMPHIS TN 38119
P.O. Box or Street City State Zip

Remit Address: 6000 POPLAR AVE., ST. 216 MEMPHIS TN 38119
P.O. Box or Street City State Zip

Federal Tax ID No.: 46-1270591

Date: 7-29-2016

END OF RFP #15-048

Appendix A Executive Summary of Management Team

1. Suzanne Miller, Ph.D. – Partner Lead
2. Kathy Brackenrich – QSA Project Manager

Suzanne H. Miller, Ph.D.

VACO Free Yourself.

Suzanne H. Miller, Ph.D., CHS-III, CPT, CISM, CRISC, CISA, PCI-QSA

Partner

AREAS OF PRACTICE

Information systems auditing, regulatory compliance (HIPAA, HITECH, SOX and GLBA), frameworks (CobiT, COSO, NIST, and ISO27005-2011), PCI DSS, IT general controls (ITGC), application controls (AC), IT entity-level controls, segregation of duties, information security curriculum development, policy and procedure development, controls documentation and implementation, business process engineering (BPE), system development life cycle (SDLC), IT process improvement, mitigation, business contingency plans, risk management, computer forensics, data mining

INDUSTRY LINES

Publicly Traded Companies, Healthcare, Hospitality, Manufacturing, Service Industry, Real Estate, Education, Telecommunications, Law Enforcement and Correctional, Logistics, Auto Dealerships, Insurance, Governments - State, County and Local

COMPUTER APPLICATIONS

-Accounting *(PeopleSoft, SAP, Oracle Financials, Great Plains, Solomon, MAPIC, Sage, MACC, Lawson, FoodStar)*
-Reporting Tools *(FRX, Crystal Report Writer, Touchpoint)*
-CRM *(Siebel, PeopleSoft, Front Page)*
-Tools *(ACL, Qualys, NetIQ, Sekchek, Bindview, LAN Manager, Tripwire, Remedy, Turnover, Bsafe, Crypto, Endevor, UC4, Lotus Notes, HEAT, Track-It, MS Office Suite, COGNOS Business Intelligent Suite, Symantec Suite, Hyperion, SPSS, EnCase, dd, Ghost, eAudit+)*
-Operating Systems *(Windows, UNIX, OS400, AIX UNIX, Linux, RACF)*
-Databases *(SQL, DB2, Oracle, Foxbase/Foxpro, Access)*
- Additional Applications *(ERP, LMS, EMR EHR, Education Record Keeping Management Systems, Hospital/ Medical/Lab/Radiology/EMS Systems)*

EDUCATION/QUALIFICATIONS

BS, University of Tennessee, Mathematics Education
MS, University of Missouri, Mathematics Education
Ph.D.-Candidate, University of Michigan, Mathematics
Ph.D., Oregon State University, Computer Science Education

PROFESSIONAL EXPERIENCE

Dr. Miller has extensive and successful experience in risk-based, cost effective information security mentoring and guidance for organizations. She has strong leadership and extensive management skills in mitigating companies for PCI/SOX/HIPAA/Red Flag Rule compliance by re-structuring control designs/implementation, process re-engineering, workforce education and development of IT Governance (business owners); Particular strength in working with management to turn around HITECH/SOX/PCI projects that are in jeopardy.

PRINCIPAL AREAS OF PRACTICE

Dr. Suzanne Miller uses her expertise in information security and regulatory compliance to help companies align their IT governance, risk management and compliance activities. Her areas of expertise are:

- Performing gap analyses, readiness assessment and pre-assessment in collaboration with an organizations internal audit team; including identification of control weaknesses, development of remediation plans and lead for the mitigation efforts
- Developing of remediation plans using a risk-based, step-by-step approach
- Mentoring and guiding organizations through customized compliance solutions which are specifically defined for the client's environment
- Working with functional groups in the creation of policies, procedures and/or guidelines to ensure the privacy and security of company sensitive information
- Leading corporate-wide security awareness initiative through the use of business owners and education programs
- Cross-walking SOX, HIPAA, PCI and/or other requirements to eliminate duplication of effort.

Additionally, Dr. Miller is the co-author of the *HIPAA Security Toolkit*, *TurboPCI Easy Workbooks* and the *CPA PCI Resource Manual*.

MAJOR PROJECTS

Large Healthcare/Research Provider

- Brought in to "fast track" and lead PCI compliance for a publicly-traded company
- Performed initial PCI Readiness Assessment and developed a Remediation Plan
- Aligned with stakeholders to identify compliance solutions by facilitating workshops and obtaining stakeholder commitment to agreed upon solutions
- Worked with the processor to develop a partnership with the organization in an effort to reduce fines and extend mandate deadlines
- Oversaw the compliance project which brought the organization from being 30% compliant to 100% in 4 months

Manufacturing Company- Medical Devices

Contracted to oversee the planning, designing and implementation of IT SOX project.
Performed all phases of IT Sarbanes-Oxley (SOX) 404 projects. Worked with corporate headquarters to define corporate-wide IT controls that align with SOX and HIPAA, oversaw the implementation of the controls and process re-engineering, developed control matrix, developed policies and procedures, developed test plans and conducted controls testing activities, developed and coordinated remediation plans
Completed project ahead of schedule and under budget
Due to contract extension, leveraged SOX work to perform a PCI gap analysis and develop a remediation plan
Mentored and guided the organization through the remediation and annual PCI compliance reporting

Logistics Company – International Fortune 50 Company

- Brought in to develop and implement a PCI Global compliance plan by working directly with processors and brands
- Designed and implemented a cross-cultural discovery methodology to identify global business processes that have access to or impact the security of cardholder data
- Designed and implemented a cross-cultural gap analysis to identify global PCI gaps
- Developed in cooperation with management a global remediation strategy

Large Hospitality Organization

- Restructured the analysis division to incorporate data warehousing and data mining
- Implemented end-to-end process management systems in conjunction with reengineering the data flow
- Implemented a SDLC (System Development Life Cycle) methodology to design, develop and implement a global contact management system for Latin America and Ritz Carlton Divisions which was 60% less than outside vendors and was rolled out ahead of schedule

Certified Information Security Manager (CISM) - Information Systems Audit and Control Association (ISACA)
Certified Information Security Auditor (CISA) - Information Systems Audit and Control Association (ISACA)
Certified Risk and Information Systems Controls (CRISC) - Information Systems Audit and Control Association (ISACA)
Certified Performance Technologist (CPT) - International Society for Performance Improvement (ISPI) Certified Homeland Security (Technology) (CHS-III) – American College of Forensic Examiners International (ACFEI)
Qualified Security Auditor (QSA) – PCI Security Standards Council (PCI SSC)

Kathy Brackenrich

VACO
Free Yourself.

Kathy Brackenrich
QSA, PCIP, CISA, CRISC
Compliance

Areas of Practice

Project Management, Resource Management, Information Security scoping and assessing, PCI validation requirements, Information Security management, Policy and Procedure review and development, controls documentation, mitigation, Risk Management Remediation Management, System Development Life Cycle (SDLC), Disaster Recovery/Business Continuity, IT Governance frameworks (COBIT)

Industry Lines

Global Transportation, Retailers, Healthcare, Fundraising, Consumer Services, Manufacturing

Computer Applications

Tools *(Qualys, Sekchek, MS Office Suite, BaseCamp)*
Operating Systems *(Windows, AS400, Unix Linux)*
Databases *(SQL, Access, Quickbase)*

Education

BS, Arkansas State University
Management Information Systems

Qualifications

Certified Information Security Auditor (CISA) Certified Risk and Information Systems Controls (CRISC), Qualified Security Auditor (QSA), Payment Card Industry Professional (PCIP)

Professional Experience

- QSA, PCIP, CISA, CRISC certified senior professional with 15+ years' experience in IS security and risk management services.
- Experienced in Sarbanes-Oxley, PCI-DSS, Operational audits, Information Technology audits, Financial Statement audits, internal audits, external audits, business analysis and requirements gathering, project management familiarity with HIPPA, FISMA.
- Knowledgeable of relevant professional standards including COSO, COBIT, ISO/IEC 27001:2005, PCI DSS.
- Knowledgeable of business process in the retail, manufacturing, logistic services, financial services, telecommunications, e-commerce and government industries.

Principal Areas of Practice

Kathy conducts information security and regulatory compliance assessments and audits. Her areas of expertise consist of the following:

- Serving as Project Manager for compliance assessments
- Maintaining Budget to Actuals for each project
- Mentoring and assisting team members in various types of assessments
- Planning and performing information system audits, special reviews and testing
- Performing detailed testing, analysis, and validation of systems, processes and controls
- Coordinating interviews and artifact gathering schedules between team members and client
- Compiling accurate documentation of test results for submission to client
- Identifying and presenting control weaknesses to the audit team and client
- Developing of remediation plans using a risk-based approach
- Creating standard policies and procedures for Compliance Assessments
- Leading and participating in special projects
- Cross-walking SOX, HIPAA, PCI and/or other requirements to eliminate duplication of effort

Major Projects

Major Store Retailer

PCI DSS engagement for Level 1 Merchant, 850 Locations

Global Non-Profit Organization

PCI DSS engagement for Level 2 Merchant

Global Transportation

PCI DSS engagement for Level 1 Merchant, 571 Locations

Consumer Services

PCI DSS engagement for Level 2 Merchant, 650 Locations

Certified Information Security Auditor (CISA) - Information Systems Audit and Control Association (ISACA)
Certified Risk and Information Systems Controls (CRISC) - Information Systems Audit and Control Association (ISACA)
Qualified Security Auditor (QSA) – PCI Security Standards Council (PCI SSC)
Payment Card Industry Professional (PCIP) - PCI Security Standards Council (PCI SSC)