

**THE PORT AUTHORITY OF NY & NJ
PROCUREMENT DEPARTMENT
TWO MONTGOMERY STREET, 3RD FLOOR
JERSEY CITY, NJ 07302**

Date: March 20, 2015

ADDENDUM #1

To prospective Proposers to Request for Proposals (RFP) # 41681: Enterprise Risk Management (ERM)/Governance Risk Compliance (GRC) Software Solution

Proposals due April 10, 2015, no later than 2:00 PM

CHANGES:

1. Page 14, Section 7 (Certification of Recycled Materials Provision), first sentence of the first paragraph: Change "Attachment X" to "Attachment F".
2. Pages 84-90, Attachment H (Control Requirements Contract Checklist): Replace Attachment H with the revised Attachment H included at the end of this Addendum #1.
3. Pages 13-14, Section 6 (DBE Participation): Replace Section 6 in its entirety with the following Section 6 entitled "M/WBE Subcontracting Provisions":

"The Port Authority has a long-standing practice of making its business opportunities available to Minority Business Enterprises (MBEs) and Women-Owned Businesses (WBEs) and has taken affirmative steps to encourage such firms to seek business opportunities with the Port Authority. The successful Proposer will use good faith efforts to provide for meaningful participation by the Port Authority certified M/WBEs as defined in this document, in the purchasing and subcontracting opportunities associated with this contract, including purchase of equipment, supplies and labor services.

Minority Business Enterprise (MBE) - shall mean a business entity which is at least 51% owned and controlled by one or more members of one or more minority groups, or, in the case of a publicly held corporation, at least 51% of the stock of which is owned by one or more minority groups, and whose management and daily business operations are controlled by one or more such individuals who are citizens or permanent resident aliens.

"Minority Group" means any of the following racial or ethnic groups:

- a) Black persons having origins in any of the Black African racial groups not of Hispanic origin;
- b) Hispanic persons of Mexican, Puerto Rican, Dominican, Cuban, Central or South American culture or origin, regardless of race;
- c) Asian and Pacific Islander persons having origins in any of the original peoples of the Far East, Southeast Asia, The Indian Subcontinent, or the Pacific Islands;

- d) Native American or Alaskan native persons having origins in any of the original peoples of North America and maintaining identifiable tribal affiliations through membership and participation or community identification.

Women-Owned Business Enterprise (WBE) - shall mean a business enterprise which is at least 51% owned by one or more women, or, in the case of a publicly held corporation, at least 51% of the stock of which is owned by one or more women and whose management and daily business operations are controlled by one or more women who are citizens or permanent or resident aliens.

The Contractor shall use good faith efforts to achieve participation equivalent to 12% of the total Contract price for MBEs and 5% of the total Contract price for WBEs.

Good faith efforts to include participation by M/WBEs shall include, but not be limited to the following:

- 1) Dividing the services and materials to be procured into small portions where feasible;
- 2) Giving reasonable advance notice of specific subcontracting and purchasing opportunities to such firms as may be appropriate;
- 3) Soliciting services and materials from M/WBEs, which are certified by the Port Authority;
- 4) Ensuring that provision is made for timely progress payments to the M/WBEs and;
- 5) Observance of reasonable commercial standards of fair dealing in the respective trade or business.

Proposers are directed to use form PA3749B as the recording mechanism for the M/WBE participation Plan, which may be downloaded at <http://www.panynj.gov/business-opportunities/become-vendor.html>

The M/WBE Plan submitted by the Contractor to the Port Authority shall contain, at a minimum, the following:

- Identification of M/WBE's: Provide the names and addresses of all M/WBEs included in the Plan. If none are identified, describe the process for selecting participant firms in order to achieve the good faith goals under this Contract.
- Level of Participation: Indicate the percentage of M/WBE participation expected to be achieved with the arrangement described in the Plan.
- Scope of Work: Describe the specific scope of work the M/WBE's will perform.
- Previous M/WBE Participation: Describe any previous or current M/WBE participation, which the Proposer has utilized in the performance of its contracts.

All M/WBE subcontractors listed on the M/WBE Participation Plan must be certified by the Port Authority in order for the Contractor to receive credit toward the M/WBE goals set forth in this Contract. Please go to <http://www.panynj.gov/business-opportunities/supplier-diversity.html> to search for M/WBEs by a particular commodity or service. The Port Authority makes no representation as to the financial responsibility of such firms or their ability to perform Work under this Contract.

Proposers shall include their M/WBE Participation Plan with their proposals, to be reviewed and approved by the Authority's Office of Business Diversity and Civil Rights (OBDCR).

Proposers may request a waiver of the M/WBE participation goals set forth in this Contract by providing with its proposal, information in accordance with this provision and the provision entitled "M/WBE Good Faith Participation" in the Standard Terms and Conditions of this Contract.

4. Pages 52 to 56, Section 45 (“Disadvantaged Business Program [DBE]”): Replace Section 45 in its entirety with the following Section 45 entitled “M/WBE Good Faith Participation”:

“If specified as applicable to this Contract, the Contractor shall use every good-faith effort to provide for participation by certified Minority Business Enterprises (MBEs) and certified Women-owned Business Enterprises (WBEs) as herein defined, in all purchasing and subcontracting opportunities associated with this Contract, including purchase of equipment, supplies and labor services.

Good Faith efforts to include participation by MBEs/WBEs shall include the following:

- a. Dividing the services and materials to be procured into small portions, where feasible.
- b. Giving reasonable advance notice of specific contracting, subcontracting and purchasing opportunities to such MBEs/WBEs as may be appropriate.
- c. Soliciting services and materials, to be procured, from the Directory of MBEs/WBEs, a copy of which can be obtained on the Port Authority Website at <http://www.panynj.gov/business-opportunities/supplier-diversity.html> or by contacting the Port Authority’s Office of Business Diversity and Civil Rights at (212) 435-7819 or seeking MBEs/WBEs from other sources.
- d. Insuring that provision is made to provide progress payments to MBEs/WBEs on a timely basis.
- e. Observance of reasonable commercial standards of fair dealing in the respective trade or business.

Either prior or subsequent to Contract award, the Contractor may request a full or partial waiver of the M/WBE participation goals set forth in this Contract by providing documentation demonstrating to the Manager, for approval by the Port Authority’s Office of Business Diversity and Civil Rights, that its good faith efforts did not result in compliance with the goals set forth above because participation by eligible M/WBEs could not be obtained at a reasonable price or that such M/WBEs were not available to adequately perform as subcontractors. The Contractor shall provide written documentation in support of its request to the Manager. The documentation shall include, but not be limited to, documentation demonstrating good faith efforts as described above, which may include, proof that the Authority’s directory does not contain M/WBEs in this specific field of work, a list of organizations contacted to obtain M/WBEs, and/or a list of M/WBEs contacted and their price quotes. If approved by the Authority’s Office of Business Diversity and Civil Rights, the Manager will provide written approval of the modified or waived M/WBE Participation Plan.

Subsequent to Contract award, all changes to the M/WBE Participation Plan must be submitted via a modified M/WBE Participation Plan to the Manager for review and approval by the Authority’s Office of Business Diversity and Civil Rights. For submittal of modifications to the M/WBE Plan, Contractors are directed to use form PA3749C, which may be downloaded at <http://www.panynj.gov/business-opportunities/become-vendor.html>. The Contractor shall not make changes to its approved M/WBE Participation Plan or substitute M/WBE subcontractors or suppliers for those named in their approved plan without the Manager’s prior written approval. Unauthorized changes or substitutions, including performing the work designated for a subcontractor with the Contractor’s own forces, shall be a violation of this section. Progress toward attainment of M/WBE participation goals set forth herein will be monitored throughout the duration of this Contract.

The Contractor shall also submit to the Manager, along with invoices, the Statement of Subcontractor Payments as the M/WBE Participation Report, annexed hereto as an attachment. The Statement must include the name and business address of each M/WBE subcontractor and supplier actually involved in the Contract, a description of the work performed and/or product or service supplied by each such

subcontractor or supplier, the date and amount of each expenditure, and such other information that may assist the Manager in determining the Contractor’s compliance with the foregoing provisions.

If, during the performance of this Contract, the Contractor fails to demonstrate good faith efforts in carrying out its M/WBE Participation Plan and the Contractor has not requested and been granted a full or partial waiver of the M/WBE participation goals set forth in this Contract, the Authority will take into consideration the Contractor’s failure to carry out its M/WBE Participation Plan in its evaluation for award of future Authority contracts.”

5. Delete Appendices A1-A5 (DBE Forms)

QUESTIONS AND ANSWERS

The following information is made available in response to questions submitted by prospective Proposers to the Port Authority of New York and New Jersey’s (the “Port Authority” or the “Authority”) RFP for an Enterprise Risk Management (ERM)/Governance Risk Compliance (GRC) Software Solution. It addresses only those questions that the Port Authority has deemed to require additional information and/or clarification. The fact that information has not been supplied with respect to any questions asked by a Proposer does not mean or imply anything (nor should it be deemed to have any meaning, construction or implication) with respect to the terms and provisions of the Request for RFP, which will be construed without reference to such questions.

The Port Authority makes no representations, warranties or guarantees that the information contained herein is accurate, complete or timely or that such information accurately represents the conditions that would be encountered during the performance of the Contract. The furnishing of such information by the Port Authority shall not create or be deemed to create any obligation or liability upon it for any reason whatsoever and each Proposer, by submitting its proposal, expressly agrees that it has not relied upon the foregoing information, and that it shall not hold the Port Authority liable or responsible therefor in any manner whatsoever. Accordingly, nothing contained herein and no representation, statement or promise, of the Port Authority, its Commissioners, officers, agents, representatives, or employees, orally or in writing, shall impair or limit the effect of the warranties of the Proposer required by this RFP and any resulting contract and the Proposer agrees that it shall not hold the Port Authority liable or responsible therefor in any manner whatsoever.

	Question/Request	Answer
1	Page 63, Item V: “Review physical access authorizations and logs.” Please describe the concept of physical access. Do you want to track who uses badges at a particular gate, for example?	This requirement pertains to the technical infrastructure (e.g. network, operating system, database, etc.) to support the selected system, not the physical space where the applications reside.
2	Page 63, Item W: “Inventory physical security devices and change locks, codes, and combinations.” What kind of inventory are you referring to? Should locks, codes and combinations be stored in the software suite?	The inventory refers to any protected information that needs to be physically secured. The number of locks and frequency of code changes shall be inventoried in the software suite.
3	Page 64, Section 4.8: “Incident Response.” What type of incidents are you referring to? What level of details should we have to track them?	The requirement refers to any cyber security-related incidents. The incidents will need to be tracked according to the controls listed in the National Institute of Standards and Technology (NIST) 800 series, specifically NIST 800-61.

4	Page 64, Section 6.A: "Alloy Asset Management." Are the assets integrated with a third party system? If yes, which one?	The assets are not integrated with a third-party system.
5	Our firm currently has agreements with the Port Authority. Could either of those agreements be expanded to include the Scope of Work described in the RFP?	The Port Authority intends to issue a new contract resulting from this publicly advertised RFP 41681.
6	Pages 62, 63 of the RFP: Will the contractor be responsible for creating the items mentioned on these pages (e.g., Authority Policies and Procedures, Authority's Approach to Risk Management, and Authority's Business Strategy)? Or will those items be provided by the Authority for the contractor's review, etc.?	The Contractor shall not be required to produce the Authority's policies and procedures, approach to risk management, and business strategy. The Contractor shall provide only the selected system and any services related to implementing, configuring and maintaining it to satisfy the Authority's requirements.
7	Reference Attachment D, Scope of Work, Section 1 (General Requirements), subsection I: "Update and track status of plans, objectives, actions and milestones." Is the updating and tracking strictly focused on enterprise risk items or are you talking more broadly for all of the items for the Port Authority?	Updating and tracking items shall apply for all items mentioned in the RFP's Scope of Work (Attachment D), not just for items related to enterprise risk.
8	Reference Attachment D, Scope of Work, Section 1 (General Requirements), subsection L: "Track performance of certification and accreditation activities related to organizational assets." Will the certification and accreditation activities and their mapping to organizational assets be provided through other information systems designated elsewhere in this SOW?	No.
9	Reference Attachment D, Scope of Work, Section 1 (General Requirements), subsection O: "Track performance of specific cyber-security activities for compliance." Will the specific cyber security-related activities be provided by another information system designated elsewhere in this SOW?	Specific cyber security-related activities could result from various sources (e.g. plans, policies, specific incidents, etc.). Information related to these activities could reside in other systems used by the Port Authority.
10	Reference Attachment E, Cost Proposal. Are we to price this as firm-fixed price (plus reimbursables), provide a quote as time-and-materials, or a combination of the two?	Cost Proposals shall adhere to the format provided in Attachment E of the RFP. Each table in Attachment E shall be completed and provided in the Proposer's Cost Proposal.
11	The RFP states that we must print 10 copies of the RFP. Can this number be reduced and the Port Authority distribute the proposals electronically.	Proposers shall comply with the submission requirements described in Section E on page 8 of the RFP.
12	Will the Port Authority be interested in implementing particular software solutions for this engagement?	The Port Authority will consider all proposed solutions from proposers that demonstrate satisfaction of the "Proposer Prerequisites" (Section 3, Pages 10-11).

13	Describe the Port Authority's compliance requirements and current processes?	The Port Authority will provide such information to the selected proposer (i.e. Contractor).
14	Describe Port Authority's risk management process? How often does the Port Authority conduct risk assessments?	The Port Authority follows the Risk and Insurance Management Society (RIMS) Risk Maturity Model (RMM), which provides a framework for implementing the Port Authority's Enterprise Risk Management program. Department and facility risk registers are updated on a continual basis. Strategic risks are identified by executive management on an annual basis.
15	Does the Port Authority have a risk and control matrix? If so, please provide a sample.	The Port Authority does not have a risk and control matrix.
16	Describe the type and number of assets to be covered in the assessment?	ERM assessments are conducted at the department and facility levels. The Port Authority currently maintains approximately fifty risk registers that cover all business risks.
17	How is asset information stored today in the Port Authority? Do you have a Configuration Management Database (CMDB)?	Asset information is stored in various systems throughout the Port Authority. Regarding asset management, the selected software is expected to integrate with <i>Alloy Asset Management</i> . However, the scope of work for the contract that is expected to result from this RFP does not require the Contractor to perform such integration. The Port Authority does not have a Configuration Management Database.
18	Does the Port Authority have an overall roadmap defined for risk and compliance process?	The Port Authority follows the Risk and Insurance Management Society (RIMS) Risk Maturity Model (RMM), which provides a framework for implementing the Port Authority's Enterprise Risk Management program.
19	Governance, Risk and Compliance Management automation requires an assessment that should be performed in order to identify use cases, analyze current state opportunities and define a roadmap and projects. We can perform this assessment and create a roadmap for eGRC implementation. Is this activity required or are the use cases developed/are in the process of being developed?	Use Cases may be required during the implementation of the selected system.
20	Provide the number of stakeholders whom we need to work with for this implementation.	The Contractor shall work with personnel from several departments in the Port Authority. At this time, the Port Authority has not determined the complete roster of such personnel.
21	What is PANYNJ's preferred deployment model (on-premise or SaaS)?	"The Contractor shall furnish an on-premise Enterprise Risk Management. (ERM)/Governance Risk Compliance (GRC) software solution to support the tracking, measurement, management, and reporting of enterprise risks" (Attachment D, Scope

		of Work, Section 1, Page 61). (Emphasis added)
22	How many instances (e.g development, testing, staging and production) would the Port Authority require?	The Port Authority requires the following instances: Development, Quality Assurance and Production.
23	Please provide a description of the type, frequency and number of reports that the Port Authority would expect from this system.	Refer to the section entitled Reporting Requirements (Section 5, page 65) for the type of expected reports. The exact number of reports and their frequency shall be determined during the implementation of the selected system.
24	How will proposals be evaluated?	Refer to Section 5 (Evaluation Criteria and Ranking) on pages 12-13 of the RFP.
25	Do you have an electronic version of the RFP to make life easier?	The only version of the RFP available to proposers is on the Port Authority's website : http://www.panynj.gov/business-opportunities/bid-proposal-advertisements.html . Choose the tab entitled "Goods and Services" and scroll to #41681.
26	Provide a breakout of the 350 users (# of admin), vs light users.	The selected system shall be able to "Accommodate 350+ concurrent users, including 5-10 administrators, 100 frequent / 'power' users, and an additional 200 infrequent users, with capacity to accommodate user growth" (Section 2.E, Page 63).
27	Do interested proposers need to register in order to provide a proposal?	No.
28	Describe the integration requirements? Does the Port Authority require an automated API for the integration?	The Scope of Work does not require the Contractor to integrate the selected system with the applications listed in Section 6 of the Attachment D (pages 65-66). Proposers shall "demonstrate the proposed System's ability to integrate with the applications listed in Section 6 of the SOW (Attachment D)" (Section 6, Pg. 17).
29	Do you have a process for jointly responding to RFPs with a partner? If so, what is the process for responding jointly?	Refer to Section A (Letter of Transmittal) on page 15 of the RFP. Moreover, with respect to the prerequisites, refer to Section 3 (pages 10-11) of the RFP.
30	Please let us know the preferred deployment model - On-Premise or Cloud model?	See the answer to question 21, above.
31	Do you have a target date for having a system implemented and rollout strategy (1 site, 1 region, 1 BU, big bang, etc.)?	Proposers shall provide a plan for installing (implementing) their proposed systems (Section 3, Page 17). The Port Authority anticipates, but does not a guarantee, a phased implementation of the selected system, with the initial beginning in the third quarter of 2015.
32	When would you be taking decision on final vendor?	The Port Authority intends, but does not guarantee, to select a proposer in the late second quarter or early third quarter of 2015.

33	<p>Could you please help us the number of users based on below definitions:</p> <ul style="list-style-type: none"> • Regular Users: Use system Up to Once a week(Sample Role: Risk Managers, Risk Identifiers, Risk and Control Documentation managers) • Medium Users: Use System Up to once a quarter(Sample Role: Risk Policy Editors, Reviewer of Controls, Control Testers, Risk Mitigation Plan Users, Risk Auditors) • Light Users- Use system Less than once a quarter but more than once a year(Sample Role: Issue Tracking Users, Reporting Users) • Mass Users: Read only Risk Policy Users ,Annual Survey Users 	See the answer to question 26, above.
----	---	---------------------------------------

This communication should be initialed by you and annexed to your proposal upon submission. In case any Proposer fails to conform to these instructions, its proposal will nevertheless be construed as though this communication had been so physically annexed and initialed.

THE PORT AUTHORITY OF NEW YORK & NEW JERSEY

CARMEN REIN
GENERAL MANAGER

PROPOSER’S NAME: _____
INITIALED: _____
DATE: _____

QUESTIONS CONCERNING THIS ADDENDUM MAY BE ADDRESSED TO JAMES SUMMERVILLE:
JSUMMERVILLE@PANYNJ.GOV, 201-395-3454

ATTACHMENT H: CONTROL REQUIREMENTS CONTRACT CHECKLIST

General

- Documented procedures, flowcharts and process maps for the application.
- Conduct regular audits, vulnerability testing, and security scanners.
- SSAE 16 SOC 2 (previously known as SAS 70 Level 2)
- Federal Risk and Authorization Management Program (FedRAMP) Certification
- ISO27001 Certification
- Criminal Justice Information Services security policies and procedures (CJIS) compliant for law enforcement information and systems.
- Background check should be performed on all personnel.

System/Security Administration

- Administrative personnel should receive training.
- Administrative staff should receive general security awareness training before access is provided. All security training must be reinforced at least every three years and must be tracked as per the PA Information Security Handbook.
- System and security administration procedures should be documented and distributed.
- Administrator(s) roles and responsibilities should be documented.
- Developers and/or programmers should not have access to the production server.
- Operating system administrators should not have access to the production database and application.

Hardening of operating system/database that supports the application:

- Disable and/or remove unnecessary ports/services.
- Remove all manufacturer samples from the production system. Scripts must be removed from production systems, except those required for the operation and maintenance of the system.
- Default, public, and guest accounts should be secured/locked/removed.
- Change all default passwords; delete all default content and login scripts.
- Limit administrative and user account privilege and access.
- Document system accounts like administrator, root, oracle, and sys.
- Document user/group access rights
 - Users/groups should be setup with least access required to perform job responsibilities.
- Implement access control at the database level (i.e. user roles and permissions, passwords, secure links)
- Use secure encrypted remote access methods.
- If the application is a web application, log (and monitor) web traffic and trend the activity looking for abnormal activity.
- Ensure that appropriate security and vulnerability assessment tools are running.
- At login, last user login should not display.
- Inventory listing of hardware and software should be current and maintained.

License Management

- Ensure that application licensing requirements are documented, reviewed and maintained.
- Application licenses should be current/valid and individuals/groups with application access should have completed the necessary access request forms and adhere to licensing requirements.

Logical Access Controls

- All users are required to read the Agency Policy Computing Resource Administrative Instruction (AI 15-4.03) and sign an acknowledgement of the Agency IT Acceptable Use Code of Conduct policy prior to account activation.
- Procedures to grant/modify/delete access should be documented.
 - Access request forms for adding/modifying/deleting users should be used.
 - Account expiration for contractors and consultants.
 - Accounts adequately identify the user – no generic accounts
- Ensure that security administrator procedures exist to:
 - Create/remove application access in a timely manner
 - Review user roles/permissions
- Validate that all users have accessed the application within the past 90 days.
 - Review dormant accounts
 - Inactive accounts should be removed.
- Each user has a unique user ID as described in the Port Authority Standard and Guidelines.
 - All user accounts profile should include Employee ID# and full user name.
- Roles are setup with least access required to perform job responsibilities.
- Roles should have a segregation of duties/roles.
- All accounts must have an individual or business group assigned to be responsible for account management.
- Segregation of duties and areas of responsibility must be implemented where appropriate.
- Whenever segregation of duties is not technically feasible, other compensatory controls must be implemented, such as monitoring of activities, audit trails and management supervision. The PA must approve these compensating controls.
- Review of audit trails and system approvals must be performed independent and retained to document the implementation of these security controls
- Access Control List (ACL) should include:
 - Current list of ACL
 - Creation and updates to ACL
 - Testing and approvals of ACL
- The application should have the PA's warning banner on the login screen. The application has a warning banner, terms of use, and/or privacy statement that was approved by the Port Authority on the login screen.
- The system should have an access role that would allow real only access to all application, database and operating system screens, functions, logs and reports.
- Remote access should be approved, secured, and documented in accordance with PA policy. Remote access, at a minimum, must consist of multifactor authentication mechanisms, secured communications (SSL/ VPN encryption methodology), access control mechanisms and logging of user activity.

Password Controls

- Ensure that password controls for the system are consistent with this requirements or more stringent
 - Passwords must be at least 10 alphanumeric characters long
 - Passwords must be changed every 90 days (administrators every 30 days)
 - Passwords must not be shared
 - Password complexity enable (capital letter, number, special character)
 - contain at least two upper and lowercase alphabetic characters,
 - contain at least one number (0-9)
 - contain at least one special character (e.g.-+};>_?&\$%#).
 - Accounts should be locked after a three logon failures
 - Passwords should not be the same account name

- No concurrent login capabilities
- End user accounts will be disabled (not deleted) after 60 days of non-use.
- Password file should be securely stored with limited access and encrypted.
- Application forces initial passwords to be changed and the initial passwords should not be easily guessable.
- Maintain a password dictionary and password history should be set to 5.
- Set “automatic session timeout” to 15 minutes of inactivity and require user to log back in with valid ID and password.
- Smartphones and smart device, where capable, shall leverage biometric access to provide the most security for the least inconvenience.

Application Controls

Data Validation & Input Controls

- The application should have input controls to verify the validity of the data entered.

Data Retention and Management

- All data should be classified according to its sensitivity (confidential, etc) and protected accordingly.
- Data archive strategy should be documented and in place.
 - Should specify how long active data is kept.

Data Integrity and Security

- Sensitive data, such as credit card #s and social security #s, should be encrypted.
- Data should be restricted and audit trails should be available to identify all user activity include view access to sensitive data.
- Sensitive data should be stored in the database encrypted and blocked from user views in the application unless it is authorized.
- Encryptions level at a minimum should be AES 256bit when encryption is used.

Application Interfaces

- Interfaces should have secured transmission and be archived.
- Reconciliation of data should be done on a batch record and totals. Detail data reconciliations should be completed on periodic basis.

Processing Controls

- Application databases/interfaces should have the necessary controls to prevent processing of inaccurate, duplicate, or unauthorized transactions and producing inaccurate outputs.
- Controls to ensure that all data is processed and accounted for should be in place.
- Rejected items should be logged, tracked and resolved in a timely manner.

Change Management

- Processes and tools should be used to report, track, approve, fix, and monitor changes on the application.
- The application and all changes to the application should be tested before being put into production.
 - Documentation of approval for change and evidence of testing should be in place.
 - Specific timetable/schedule should be documented.
- Emergency procedures should be documented and distributed.
- Separate environments are required for development, test, quality assurance, production.
- Procedures should require that no changes be made directly in the production environment without going through the development/test/quality assurance environments.

- Formal change control procedures for all systems must be developed, implemented and enforced.
- Where technically feasible, development software and tools must not be maintained on production systems.
- Source code for application or software must not be stored on the production system running that application or software.
- Privileged access to production systems by development staff must be restricted.

Application Logging, Audit Trails and Record Retention

- Audit trails for operating, application, and database systems should exist and reviewed.
- Users and roles should be tracked and reviewed
 - Maintain documentation
- All failed logon attempts should be logged.
- All sensitive transactions and changes should be logged and an audit trail created.
- Audit trails should contain who made the change, when it was made, and what was changed.
- Only the security administrator should have access to change or delete these logs or audit trails.
- Audit trails should be reviewed by the business owner(s) and security administrator.
- Management reporting should be produced through the application.
- Access reports by user and privilege should be produced and reviewed periodically including access violation reports.

Contingency Planning, Disaster Recovery and Backup Management

- A business contingency plan and a disaster recovery plan for the application should be documented and stored off-site, including escalation plan and current call tree.
- Plans should be tested and the outcomes of the tests (success/failure) should be documented.
- Regular backups of the application and the application data should be stored off-site.
- Application executables should be stored off-site or in escrow.
- Application configurations should be documented and backed-up.
- Full system backup should be encrypted.
- Backup procedures should be documented.
- Tape maintenance should include:
 - Periodically testing integrity of tape
 - Procedures for tape destruction due to faulty or scratched hardware.

Performance Monitoring

- Incident monitoring procedures should be documented and incidents logs should be reviewed to ensure that appropriate action is taken.
- Performance statistics should be examined and reviewed periodically by system administrators/business owner(s).
 - If vendor(s) support the application, a service level agreement for uptime, performance monitoring, updates, etc should be confirmed.
- Baseline tools or security products should be used and checked on a quarterly basis.

Patch Management

- Patch management procedures and documentation
 - Procedures should include testing, approvals, and distribution.
 - Documentation should include emergency procedures.

- Apply all new patches and fixes to operating system and application software for security.
- All security patches must be reviewed, evaluated and appropriately applied in a timely manner. This process must be automated, where technically possible.

Physical Protection

- Physical access to the application hardware should be appropriately restricted.
 - Physical access secured by single authentication mechanism i.e. swipe card.
 - Physical security adequate for equipment (locked cabinets).
- Appropriate fire suppression systems should be in place.
- Environmental condition adequately controlled (no water, dirt, clutter) and monitored.
 - Temperature and humidity monitoring should be implemented.
- Security cameras installed in sensitive areas
- Power surge protection and emergency power backup are in place.
- All hardware and software assets must be inventoried.
- Visitors including maintenance personnel, to data center, server and network equipment storage facilities must be escorted at all times.

Anti-virus/Malware/ Integrity/Vulnerability Software Management

- Virus patch management procedures must be documented, including emergency update procedures.
- Anti-virus and software integrity checkers must be implemented to prevent and detect the introduction of malicious code or other threats.
- Virus software engines and definitions must be implemented and up-to-date.
- A remote distribution server should be implemented for virus software updates and documentation on remote distribution should be current and maintained.
- Intrusion detection system must be in place,
- All systems must have vulnerability scans performed before going into production and periodically thereafter. Appropriate action, such as patching or updating the system, must be taken to address discovered vulnerabilities.
- Host-based intrusion detection/ firewalls software must be installed and enabled on all systems to protect from threats and to restrict access. Incident response procedures must be in place to address any alerts identified and system owner should be notified of alerts and what action was taken to mitigate the issues.
- Monitoring systems must be deployed (e.g., intrusion detection/prevention systems) at strategic network locations to monitor inbound, outbound and internal network traffic.
- Monitoring systems must be configured to alert incident response personnel to indications of compromise or potential compromise.
- Procedures must be established to maintain information security during an adverse event.
- Firewalls should be implemented.
- Firewall rules documentation should be up-to-date.
- Network management connections must be performed from a secure, dedicated network.
- Network authentication is required for all devices connecting internal networks.

Wireless Device

- Devices should be using WPA/WPA2 and AES encryption or better.
- Devices should disallow broadcasting of the SSID.
- All default parameters should be changed.
- Devices should have MAC address filtering enable or some type of authentication mechanism in place.

Web Application Vulnerabilities and Controls

- The following best practice and standards from these three web sites shall be followed:
 - The Open Web Application Security Project (OWASP) - www.owasp.org
 - www.webappsec.org (a consortium of web application security professionals)
 - Center for Internet Security (CIS) – www.cisecurity.org
- Perform data validation & integrity checks for field values and ensure the HTML special characters are stripped for all HTML request.
- Do not allow site pages to be cached by user browsers.
- All sensitive, personal or confidential data (including SSN, passwords, session IDs for sensitive applications, confidential or sensitive business transactions, etc.) should be transmitted between browser and server within an SSL-encrypted session (or other encrypted transmission) and are encrypted in the database at rest.
- All sensitive and personal data should be masked and encrypted were possible.
- Legal Issues:
 - The site should have a privacy statement and term of usage.
 - American Disability Act – Section 508 should be consider during the development process due to the requirement that federal agencies’ electronic and information technology is accessible to people with disabilities.
- Web Authentication: To prevent passwords from being passed in the clear, have authentication occur within an SSL encrypted tunnel. Use SSL (certificate) to protect the password.
- Password Reset:
 - For internal applications, reset passwords via the helpdesk or security administrator of the site
 - For external applications, send temporary password to known e-mail address, that must be changed upon login and/or
 - Have customer service reset after the user has been validated.
 - If possible, use two factor authentications like Secure ID fobs.

Disaster Recovery

- The Disaster Recovery plan should include at a minimum the following areas.
 - Business Impact Analysis
 - Critical Time Frame
 - Application System Impact Statements
 - Recovery Strategy & Approach
 - Recovery Time Objectives (RTO)/Recovery Point Objectives (RPO) for all critical systems.
 - Disaster Definition
 - Detailed Recovery Steps for each Disaster Definition
 - Escalation Plans and Decision Points
 - System Components- An inventory of the criticality of systems (including but not limited to software and operating systems, firewalls, switches, routers and other communication equipment).
 - Disaster Recovery Emergency Procedures
 - Plan Procedure Checklist
 - Disaster Recovery Team Organization
 - Salvage Team & Team Responsibilities
 - Disaster Recovery Responsibilities
 - Essential Position – Require back-up personnel to be assigned.
 - Contacts information Disaster Recovery Team and critical vendors - this area should be reviewed semi-annually for updates and changes.
 - Post-Disaster – Detail what steps need to be taken to move from disaster mode back to normal operations.

- Contingency plans (e.g., business continuity plans, disaster recovery plans, continuity of operations plans) must be established and tested regularly.
- Backup copies of procedures, software, and system images should be taken regularly and moved offsite.
 - Backups and restoration must be tested regular