

High-Level Security Reviews

The scope of this work shall be to perform high-level reviews of the [COMAPNY NAME] security program and its implementation to determine what is lacking and what needs to be looked at in depth, such as:

- a. Management procedures and controls;
- b. Physical, data, operating system, application software, personnel, and network security; and
- c. Disaster/contingency recover and planning.

Program assessment is a high-level review of the computer security program and its implementation to determine what is lacking and what needs to be looked at in depth. Tasking under this requirement could include the following standard tasks:

1. Review Management Procedures and Controls: Offeror shall examine the management procedures that support security. This includes a study of the organization chart, the authorities and responsibilities, and the separation of functions. Offeror shall also provide a list of management controls to be reviewed in each area (general, physical, data, and system and application software). This list shall, at a minimum, include:
 - (a) Written policies and operating procedures of the data center;
 - (b) Malfunction and hardware error reporting procedures;
 - (c) User job accounting procedures;
 - (d) Efficiency control evaluations;
 - (e) Organization and reporting hierarchy including proper separation of duties; and
 - (f) Development and implementation of security awareness and training.
2. Review Physical Security: Offeror shall review the physical protection of personnel, facility, and computer assets. Offeror shall develop a list of physical security procedures and controls in place. This list shall include authorizations for access to each area and, at a minimum include:
 - (a) Physical access controls and their effectiveness;
 - (b) Locks and entry procedures;
 - (c) Air conditioning, uninterruptible power supply, and fire suppression and pumping equipment for adequacy and proper maintenance;
 - (d) Reports distribution;
 - (e) Protection against hardware and software theft and other human and machine-related threats;
 - (f) Procedures for off-site storage of data and software;

- (g) Procedures for reacting to natural disasters and other nature-based threats to the facility, such as flood, fire, earthquake, hurricane, or twister; and
 - (h) Personal computer use and software copyright license policy.
3. Review Data Security: Offeror shall examine sensitive and critical databases and files. Offeror shall develop a list for review of data security techniques and methods, which, at a minimum, shall include:
- (a) Access control, integrity controls, and backup procedures;
 - (b) Data element documentation;
 - (c) Sensitive data procedures and implementation;
 - (d) Existing privacy policies and protection;
 - (e) Data access (both the authorization and implementation);
 - (f) Application software and how applications are moved into production;
 - (g) Written user responsibilities for management of data and applications; and
 - (h) Direct access storage device (DASD) management techniques and the impact on user file integrity.
4. Review Operating System Security: Offeror shall examine the specific operating system. This examination shall, at a minimum, include:
- (a) Review of the operating system and its installation;
 - (b) Backup and restore procedures;
 - (c) Review of system exits;
 - (d) Verification of audit trails;
 - (e) Review of handling and availability of system logs;
 - (f) Identification of change control procedures (installation of new software releases);
 - (g) Check for procedures which ensure that software patches are kept current;
 - (h) Review of installation for integrity;
 - (i) Review interfaces to access control package (if installed);
 - (j) Identification of primary access control software and files and procedures for ensuring that all software runs under its control;
 - (k) Review of access authorizations for appropriateness and completeness; and
 - (l) Review of interfaces with the access control package for integrity.
5. Review Application Software Security: Offeror shall review the system development life cycle (SDLC) used to manage application development and maintenance. This review shall minimally include:
- (a) Methods for developing and documenting application controls;
 - (b) Adherence to SDLC;

- (c) A review of quality assurance and testing procedures;
 - (d) Change control procedures for corrections and enhancements;
 - (e) Check for procedures which ensure that software patches are kept current;
 - (f) System documentation and security standards and adherence to both; and
 - (g) Application operation and access to applications.
6. Review Personnel Security: Offeror shall develop a report which evaluates compliance with federal and [COMAPNY NAME] personnel security policies and procedures covering such elements as position sensitivity classification, personnel security screening, information confidentiality, and security training and awareness. The report shall address whether the policies and procedures cover personnel in all positions with access to sensitive data.
 7. Review Network Security: Offeror shall review network security, evaluating its confidentiality, integrity, and availability. This review shall include, as applicable, access control, authentication, security administration, type and security of network media, security of file and print servers, encryption, interfaces between network and operating system/application software security modules, and conformance to networking standards.
 8. Review Disaster Recovery Plans: Offeror shall review the disaster recovery plan for user involvement, practical application, thoroughness, and correctness. Offeror shall review the most recent test plans and test results, noting identified deficiencies and corrective actions incorporated into the plan.
 9. Program Assessment Report: Offeror shall develop a program assessment report, which summarizes overall security compliance. The report shall detail major security weaknesses requiring correction and potential savings. It shall provide a summary of each area by: area reviewed, findings, impact of weaknesses in security (if any), and recommendations of actions that could be taken by management (if any). The report shall also identify those areas requiring more detailed study.
 10. Proposed Purchase Order Deliverables:

DELIVERABLES	DUE DATE
(a) Work Plan Development	<X> *
(b) Management Procedures and Controls Report	<X> *

- (c) Physical Security Procedures and Controls Report <X> *
- (d) Data Security Techniques and Methods Report <X> *
- (e) Operating System Report <X> *
- (f) Application Software Security Report <X> *
- (g) Personnel Security Report <X> *
- (h) Network Security Review Report <X> *
- (i) Disaster Recovery Review Report <X> *
- (j) Program Assessment Report <X> *

* (Working days from the beginning of the contract or from the previous milestone, as determined by the organization)