AppliedCS
Helping institutions manage compliance & risk

Job Description for an Information Security Officer

The Information Security Officer's role is to provide oversight and direction for developing and supporting Information Security initiatives. The Information Security Officer (ISO) assists in the planning and implementation of the company IT system, business operation, and facility defenses against security breaches and vulnerability issues. This individual is also responsible for directing the administration of security policies, activities, and standards.

The ISO should be responsible and accountable for administration of the Information Security Program. At a minimum, the ISO should directly manage or oversee the risk assessment process, development of policies, standards, procedures, testing, and security reporting processes. To ensure appropriate segregation of duties, the ISO should report directly to the Board or to senior management and have sufficient independence to perform their assigned tasks. The ISO should be a risk manager and not a production resource assigned to the Information Technology Department. The ISO should have the authority to respond to a cybersecurity incident by ordering emergency actions to protect the financial institution and its customers from an imminent loss of information or value. A cybersecurity incident occurs when the confidentiality, integrity, availability, or accountability of an information system is compromised. The ISO should have sufficient knowledge, background, and training, as well as an organizational position, to enable him/her to perform assigned tasks.

Information Security Officer Responsibilities

1. Overseeing the performance of each risk assessment and the integration of the risk assessments into a cohesive whole.
2. Prepare and present Risk Analysis to the Board of Directors for approval/disapproval on any risk considered to be too costly or disruptive to be remediated.
3. Research, develop, implement, test and review an institution's information security to protect information and prevent unauthorized access.
4. Identify requirements, resources, applicable protection technology, industry "best practices" and administrative procedures pertaining to information protection and make sure management has working knowledge of this information.
5. Ensure that facilities, premises, and equipment are secure and adhere to all applicable laws and regulations regarding information security.
6. Act as advocate and primary liaison for the company's information security vision via regular written and in-person communications with the company's executives, department heads, and end users.
7. Assist with the design, implementation, maintenance and training of disaster recovery and business continuity plans, procedures, audits, and enhancements.
8. Evaluate new technology prior to purchase or implementation by performing a risk assessment on the technology.
9. Ensure the development, maintenance and training of Information Security Policies with compliance to Federal and State laws and guidance.

10. Ensure the development and maintenance of operational procedures and standards as they relate to Information Security.
11. Ensure inventory of all IT Assets is maintained and kept current, including proper record retention and oversight for IT Asset disposition.
12. Establish a process to identify, track, and report on security patch management.
13. Establish a Chain of Custody that documents (in writing) the name, title, office, and phone number of each individual having sequential possession of a system's hard drive when it is removed due to compromise and the need for possible forensic examination of evidence for potential prosecution.
14. Development and management of the Incident Response and Reporting Program. This program should include the following elements: Policy, Procedures, Contact Lists; Reporting Forms, Customer Notification Templates; Testing Criteria, and Common Scenario Playbooks. At a minimum an annual table top test should be performed by the Incident Response Team. (The Role the ISO plays during an Incident should be outlined within the Incident Response and Reporting Program.)
15. Ensuring examiners, auditors, and assessors have documentation, materials, network and facility access as needed.
16. Maintaining awareness of the latest threats including: Malware; new attack vectors; attack methodology; threat patterns; trends; and general threat intelligence.
17. Establishing contacts with Local, State and Federal Law enforcement and regulatory examiners. The ISO is encouraged to share non-attributable Incident or Breach information with appropriate individuals to assist in helping others defend themselves.
18. Creation of an annual Information Security Report and the delivery of this report to the Board of Directors. This report should include elements outlined in Appendix B of Part 364 Interagency Guidelines Establishing Information Security Standards.
19. Participate in compliance committee meetings, Audit Committee meetings and IT Steering Committee meetings when possible and appropriate. This participation is to ensure: Information Security is considered in all aspects of the business; and an Information Security Dialog can be maintained on an ongoing basis.
20. Continue his/her education where possible to keep current on: Information Technology; The Banking Business and products; Current Regulatory requirements and guidelines; and Information Security.
21. Responsible for ensuring all staff receives security awareness training with current and job appropriate content. The ISO is also responsible for ensuring documentation of who has had what training and when.
22. Evaluate, perform and monitor Information Security Risk Analysis for key technology vendors.

<u>Management Responsibilities</u>

- Senior management is accountable for abiding by the Board of Directors' guidance for risk acceptance and mitigation decisions.