Sources Concerning Management

FFIEC Information Security Booklet – July 2006

Page 1: Individual financial institutions and their service providers must maintain effective security programs adequate for their operational complexity. These **security programs must have strong** board and **senior management level support, integration of security activities and controls** throughout the organization's business processes, and clear accountability for carrying out security responsibilities.

Page 4: Financial institutions should implement an ongoing security process and institute appropriate governance for the security function, **assigning clear and appropriate roles and responsibilities to** the board of directors, **management**, and employees.

Page 4: The security process is the method an organization uses to implement and achieve its security objectives. The process is designed to identify, measure, manage, and control the risks to system and data availability, integrity, and confidentiality, and to ensure accountability for system actions. The process includes five areas that serve as the framework for this booklet:

- Security Controls Implementation—The acquisition and operation of technology, the specific assignment of duties and responsibilities to managers and staff, the deployment of risk-appropriate controls, and **the assurance that management** and staff **understand their responsibilities and have the knowledge, skills, and motivation necessary to fulfill their duties**.

Page 5: **Information security** is a significant business risk that **demand engagement of** the Board of Directors and **senior business management**. It is the responsibility of everyone who has the opportunity to control or report the institution's data. **Information security should be supported throughout the institution, including** the board of directors, **senior management**, information security officers, employees, auditors, service providers, and contractors.

Page 5: The board of directors, or an appropriate committee of the board, is responsible for overseeing the development, implementation, and maintenance of the institution's information security program, and **making senior management accountable for its actions.** Oversight requires the board to provide management with guidance; approve information security plans, policies and programs; and review reports on the effectiveness of the information security program. The board should provide management with its expectations and requirements and hold **management accountable for**

- **Central oversight and coordination,**
- **Assignment of responsibility,**
- **Risk assessment and measurement,**
- **Monitoring and testing,**
- **Reporting, and**
- **Acceptable residual risk.**

Page 6: The board should approve written information security policies and the written report on the effectiveness of the information security program at least annually. A written report to the board should describe the overall status of the information security program. At a minimum, **the report should address** the results of the risk assessment process; risk management and control decisions; service provider arrangements; results of security monitoring and testing; security breaches or violations and **management's responses**; and recommendations for changes to the information security program. **The annual approval should consider the results of management assessments and reviews**, internal and external audit activity related to information security, third-party reviews of the information security program and information security measures, and other

internal or external reviews designed to assess the adequacy of information security controls.

Senior management's attitude towards security affects the entire organization's commitment to security. For example, the failure of a financial institution president to comply with security policies could undermine the entire organization's commitment to security. **Senior management should**

- Clearly support all aspects of the information security program;
- Implement the information security program as approved by the board of directors;
- Establish appropriate policies, procedures, and controls;
- Participate in assessing the effect of security issues on the financial institution and its business lines and processes;
- Delineate clear lines of responsibility and accountability for information security risk management decisions;
- Define risk measurement definitions and criteria;
- Establish acceptable levels of information security risks; and
- Oversee risk mitigation activities.

Senior management should designate one or more individuals as information security officers. Security officers should be responsible and accountable for administration of the security program. At a minimum, they should directly manage or oversee the risk assessment process, development of policies, standards, and procedures, testing, and security reporting processes. To ensure appropriate segregation of duties, the information security officers should report directly to the board or to senior management and have sufficient independence to perform their assigned tasks. Typically, **the security officers should be risk managers** and not a production resource assigned to the information technology department.

Page 7: **Senior management should enforce its security program by clearly communicating responsibilities and holding appropriate individuals accountable for complying with these requirements.** A central authority should be responsible for establishing and monitoring the security program. **Security management responsibilities**, however, **may be distributed to various lines of business** depending on the institution's size, complexity, culture, nature of operations, and other factors. The distribution of duties should ensure an appropriate segregation of duties between individuals or organizational groups.

Senior management also has the responsibility to ensure integration of security controls throughout the organization. To support integration, **senior management should**

- **Ensure the security process is governed by organizational policies and practices that are consistently applied,**
- **Require that data with similar criticality and sensitivity characteristics be protected consistently regardless of where in the organization it resides,**
- **Enforce compliance with the security program in a balanced and consistent manner across the organization,**
- **Coordinate information security with physical security, and**
- **Ensure an effective information security awareness program has been implemented throughout the organization.**

Senior management should make decisions regarding the acceptance of security risks and the performance of risk mitigation activities using guidance approved by the board of directors. Those decisions should be incorporated into the institution's policies, standards, and procedures.

Page 7: **Management also should consider and monitor the roles and responsibilities of external parties.** The security responsibilities of technology service providers (TSPs), contractors, customers, and others who have access to the institution's systems and data should be clearly delineated and documented in contracts. **Appropriate reporting mechanisms should be in place to allow management to make judgments as to the fulfillment of those responsibilities.** Finally, sufficient controls should be included in the contract to **enable management to enforce contractual requirements**.

Page 15: A risk assessment is the key driver of the information security process. Its effectiveness is directly related to the following key practices: [Excerpt]

- Multidisciplinary and Knowledge Based Approach—A consensus evaluation of the risks and risk mitigation practices requires the involvement of users with a broad range of expertise and business knowledge. Not all users may have the same opinion of the severity of various attacks, the importance of various controls, and the importance of various data elements and information system components. **Management should apply a sufficient level of expertise to the assessment.**
- Accountable Activities—**The responsibility for performing risk assessments should reside primarily with members of management** in the best position to determine the scope of the assessment and the effectiveness of risk reduction techniques. For a mid-sized or large institution, those managers will likely be in the business unit. The information security officer(s) is (are) responsible for overseeing the performance of each risk assessment and the integration of the risk assessments into a cohesive whole. **Senior management is accountable for abiding by the board of directors' guidance for risk acceptance and mitigation decisions.**
- Enhanced Knowledge—Risk assessment increases management's knowledge of the institution's mechanisms for storing, processing, and communicating information, as well as the importance of those mechanisms to the achievement of the institution's objectives. **Increased knowledge allows management to respond more rapidly to changes in the environment.** Those changes can range from new technologies and threats to regulatory requirements.
- Regular Updates—Risk assessments should be updated as new information affecting information security risks is identified (e.g., a new threat, vulnerability, adverse test result, hardware change, software change, or configuration change). At least once a year, **senior management should review the entire risk assessment to ensure relevant information is appropriately considered**.

Page 23: **Management** and information system administrators **should critically evaluate information system access privileges and establish access controls to prevent unwarranted access**. Access rights should be based upon the needs of the applicable user to carry out legitimate and approved activities on the financial institution's information systems. Policies, procedures, and criteria need to be established for both the granting of appropriate access rights and for the purpose of establishing those legitimate activities.

Page 25: Depending on the risk associated with the access, authorized internal users should generally receive a copy of the policy and appropriate training, and signify their understanding and agreement with the policy **before management grants access to the system**.

Page 42: A firewall policy states management's expectations for how the firewall should function and is a component of the overall security policy. It should establish rules for traffic coming into and going out of the security domain and how the firewall will be managed and updated. Therefore, it is a type of security policy for the firewall and forms the basis for the firewall rules. The firewall selection and the firewall policy should stem from the ongoing security risk assessment process. Accordingly, **management needs to update the firewall policy as the institution's security needs and the risks change**.

Page 49: Institution **management should consider a number of issues regarding application access control**.

Page 50: Financial institutions should **secure remote access** to and from their systems by

- Disabling remote communications if no business need exists,
- **Tightly controlling access through management approvals and subsequent audits**,
- Implementing robust controls over configurations at both ends of the remote connection to prevent potential malicious use,
- Logging and monitoring all remote access communications,
- Securing remote access devices, and
- Using strong authentication and encryption to secure communications.

Page 50: Remote access to a financial institution's systems provides an attacker with the opportunity to subvert the institution's systems from outside the physical security perimeter. Accordingly, **management should establish policies restricting remote access and be aware of all remote-access devices attached to their systems**. These devices should be strictly controlled. Good controls for remote access include the following actions: [Excerpt]

- Disallow remote access by policy and practice unless a compelling business justification exists.
- **Require management approval for remote access.**
- Regularly review remote access approvals and rescind those that no longer have a compelling business justification.
- Appropriately configure remote access devices.

Page 65: Financial institutions should develop security control requirements for new systems, system revisions, or new system acquisitions. **Management will define the security control requirements based on their risk assessment process** evaluating the value of the information at risk and the potential impact of unauthorized access or damage. Based on the risks posed by the system, **management may use a defined methodology for determining security requirements**, such as ISO 15408, the Common Criteria. **Management may also refer to published, widely recognized industry standards as a baseline** for establishing their security requirements. For example, for externally facing Web applications the Open Web Application Security Project (www.owasp.org) produces one commonly accepted guideline. **A member of senior management should document acceptance of the security requirements for each new system or system acquisition, acceptance of tests against the requirements, and approval for implementing in a production environment.**

Page 67: When deploying off-the-shelf software, **management should harden the resulting system**.

Page 70: Changes to operating systems may degrade the efficiency and effectiveness of applications that rely on the operating system for interfaces to the network, other applications, or data. Generally, **management should implement an operating system change control process** similar to the change control process used for application changes. In addition, **management should review application systems following operating system changes** to protect against a potential compromise of security or operational integrity. Isolated software libraries should be used for the creation and maintenance of software. Typically, separate libraries exist for development, test, and production.

Page 71: Financial institutions should protect the confidentiality of information about their customers and organization. A breach in confidentiality could disclose competitive information, increase fraud risk, damage the institution's reputation, violate customer privacy and associated rights, and violate regulatory requirements. Confidentiality agreements put all parties on notice that the financial institution owns its information, expects strict confidentiality, and prohibits information sharing outside of that required for legitimate business needs.

Management should obtain signed confidentiality agreements before granting new employees and contractors access to information technology systems.

Page 72: Job descriptions, employment agreements, and policy awareness acknowledgements increase accountability for security. **Management can communicate general and specific security roles and responsibilities** for all employees within their job descriptions. **Management should expect all employees, officers, and contractors to comply with security and acceptable-use policies and protect the institution's assets, including information.** The job descriptions for security personnel should describe the systems and processes they will protect and the control processes for which they are responsible. **Management can take similar steps to ensure contractors and consultants understand their security responsibilities** as well.

Page 72: Financial institutions need to educate users regarding their security roles and responsibilities. Training should support security awareness and strengthen compliance with security policies, standards, and procedures. Ultimately, **the behavior and priorities of senior management heavily influence the level of employee awareness and policy compliance, so training and the commitment to security should start with senior management**. Training materials for desktop and workstation users would typically review the acceptable-use policy and include issues like desktop security, logon requirements, password administration guidelines, etc. Training should also address social engineering and the policies and procedures that protect against social engineering attacks. Many institutions integrate a signed security awareness agreement along with periodic training and refresher courses.

Page 74: **IT management should ensure secure storage of media.** Controls could include physical and environmental controls such as fire and flood protection, limited access (e.g., physical locks, keypad, passwords, and biometrics), labeling, and logged access. **Management should establish access controls to limit access to media**, while ensuring that all employees have authorization to access the minimum data required to perform their responsibilities. More sensitive information such as system documentation, application source code, and production transaction data should have more extensive controls to guard against alteration (e.g., integrity checkers, cryptographic hashes).Furthermore, policies should minimize the distribution of sensitive information, including printouts that contain the information. Periodically, the security staff, audit staff, and data owners should review authorization levels and distribution lists to ensure they remain appropriate and current.

Page 74: Computer-based media presents unique disposal problems, and policies and procedures should comprehensively address all of the various types of electronic media in use. Residual data frequently remains on media after erasure. Since that data can be recovered, additional disposal techniques should be applied to sensitive data. Physical destruction of the media, for instance by subjecting a compact disk to microwaves, can make the data unrecoverable. Additionally, data can sometimes be destroyed after overwriting. Overwriting may be preferred when the media will be reused. Institutions should base their disposal policies on the sensitivity of the information contained on the media and, through policies, procedures, and training, ensure that the actions taken to securely dispose of computer-based media adequately protect the data from the risks of reconstruction. Where practical, **management should log the disposal of sensitive media, especially computer-based media**. Logs should record the party responsible for and performing disposal, as well as the date, medial type, hardware serial number, and method of disposal.

Page 89: **Management is responsible for considering the following key factors in developing and implementing independent tests:**

- Personnel. Technical testing is frequently only as good as the personnel performing and supervising the test. **Management is responsible for reviewing the qualifications of the testing personnel** to satisfy itself that the capabilities of the testing personnel are adequate to support the test objectives.

- Scope. The tests and methods utilized should be sufficient to validate the effectiveness of the security process in identifying and appropriately controlling security risks.
- Notifications. **Management is responsible for considering whom to inform within the institution about the timing and nature of the tests.** The need for protection of institution systems and the potential for disruptive false alarms must be balanced against the need to test personnel reactions to unexpected activities.
- Data Integrity, Confidentiality, and Availability. **Management is responsible for carefully controlling information security tests to limit the risks to data integrity, confidentiality, and system availability.** Because testing may uncover nonpublic customer information, appropriate safeguards to protect the information must be in place. Contracts with third parties to provide testing services should require that the third parties implement appropriate measures to meet the objectives of the 501(b) guidelines. **Management is responsible for ensuring that employee and contract personnel who perform the tests or have access to the test results have passed appropriate background checks, and that contract personnel are appropriately bonded.** Because certain tests may pose more risk to system availability than other tests, **management is responsible for considering whether to require the personnel performing those tests to maintain logs of their testing actions.** Those logs can be helpful should the systems react in an unexpected manner.
- Confidentiality of Test Plans and Data. Since knowledge of test planning and results may facilitate a security breach, institutions should carefully limit the distribution of their testing information. **Management is responsible for clearly identifying the individuals responsible for protecting the data and providing guidance for that protection, while making the results available in a useable form to those who are responsible for following up on the tests. Management also should consider requiring contractors to sign nondisclosure agreements and to return to the institution information they obtained in their testing.**
- Frequency. The frequency of testing should be determined by the institution's risk assessment. High-risk systems should be subject to an independent test at least once a year. Additionally, firewall policies and other policies addressing access control between the financial institution's network and other networks should be audited and verified at least quarterly. Factors that may increase the frequency of testing include the extent of changes to network configuration, significant changes in potential attacker profiles and techniques, and the results of other testing.
- Proxy Testing. Independent testing of a proxy system is generally not effective in validating the effectiveness of a security process. Proxy testing, by its nature, does not test the operational system's policies and procedures, or its integration with other systems. It also does not test the reaction of personnel to unusual events. Proxy testing may be the best choice, however, when management is unable to test the operational system without creating excessive risk.

Page 91: The security response center should be governed by policies and procedures that address security incidents: [Excerpt]

- Monitoring policies should enable adequate continual and ad-hoc monitoring of communications and the use of the results of monitoring in subsequent legal procedures. The responsibility and authority of security personnel and system administrators for monitoring should be established, and **the tools used should be reviewed and approved by appropriate management** with appropriate conditions for use.

Page 93: **Management is responsible for ensuring the protection of institution and customer data**, even when that data is transmitted, processed, stored, or disposed of by a service provider. Service providers should have appropriate security monitoring based on the risk to their organization, their customer institutions, and the institution's customers. Accordingly, **management** and auditors evaluating TSPs **should use the guidance in this booklet in performing initial due diligence, constructing contracts, and exercising ongoing oversight**

or audit responsibilities. Where indicated by the institution's risk assessment, **management is responsible for monitoring the service provider's activities** through review of timely audits and test results or other equivalent evaluations.

Page 95: Effective monitoring of threats includes both non-technical and technical sources. Non-technical sources include organizational changes, business process changes, new business locations, increased sensitivity of information, or new products and services. Technical sources include new systems, new service providers, and increased access. Security personnel and financial institution **management must remain alert to emerging threats and vulnerabilities**. This effort could include the following security activities: [Excerpt]

- **Senior management support for strong security policy awareness and compliance. Management** and employees **must remain alert to operational changes** that could affect security and actively communicate issues with security personnel. Business line **managers must have responsibility and accountability for maintaining the security of their personnel, systems, facilities, and information.**
- **Senior management should require periodic self-assessments** to provide an ongoing assessment of policy adequacy and compliance and ensure prompt corrective action of significant deficiencies.