Federal Financial Institutions Examination Council

FFIEC

Information Security IS

JULY 2006

IT Examination Handbook

TABLE OF CONTENTS

Introduction

Overview

Information is one of a financial institution's most important assets. Protection of information assets is necessary to establish and maintain trust between the financial institution and its customers, maintain compliance with the law, and protect the reputation of the institution. Timely and reliable information is necessary to process transactions and support financial institution and customer decisions. A financial institution's earnings and capital can be adversely affected if information becomes known to unauthorized parties, is altered, or is not available when it is needed.

Information security is the process by which an organization protects and secures its systems, media, and facilities that process and maintain information vital to its operations. On a broad scale, the financial institution industry has a primary role in protecting the nation's financial services infrastructure. The security of the industry's systems and information is essential to its safety and soundness and to the privacy of customer financial information. 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. This booklet provides guidance to examiners and organizations on assessing the level of security risks to the organization and evaluating the adequacy of the organization's risk management.

Organizations often inaccurately perceive information security as the state or condition of controls at a point in time. Security is an ongoing process, whereby the condition of a financial institution's controls is just one indicator of its overall security posture. Other indicators include the ability of the institution to continually assess its posture and react appropriately in the face of rapidly changing threats, technologies, and business conditions. A financial institution establishes and maintains truly effective information security when it continuously integrates processes, people, and technology to mitigate risk in accordance with risk assessment and acceptable risk tolerance levels. Financial institutions protect their information by instituting a security process that identifies risks, forms a strategy to manage the risks, implements the strategy, tests the implementation, and monitors the environment to control the risks.

Financial institutions may outsource some or all of their information processing. Examiners may use this booklet when evaluating the financial institution's risk management process, including the duties, obligations, and responsibilities of the service provider for information security and the oversight exercised by the financial institution.

Coordination with GLBA Section 501(b)

Member agencies of the Federal Financial Institutions Examination Council (FFIEC) implemented section 501(b) of the Gramm-Leach-Bliley Act of 1999 (GLBA)See Appendix C for a listing of laws, regulations, and agency guidance. by defining a process-based approach to security in the "Interagency Guidelines Establishing Information Security Standards" (501(b)

guidelines) . The 501(b) guidelines afford the FFIEC agenciesBoard of Governors of the Federal Reserve System (Federal Reserve Board), Federal Deposit Insurance Corporation (FDIC), National Credit Union Administration (NCUA), Office of the Comptroller of the Currency (OCC), and Office of Thrift Supervision (OTS). (agencies) enforcement options if financial institutions do not establish and maintain adequate information security programs. This booklet follows the same process-based approach, applies it to various aspects of the financial institution's operations and all related data, and serves as a supplement to the agencies' GLBA 501(b) expectations.

Security Objectives

Information security enables a financial institution to meet its business objectives by implementing business systems with due consideration of information technology (IT)-related risks to the organization, business and trading partners, technology service providers, and customers. Organizations meet this goal by striving to accomplish the following objectives.Underlying Models for IT Security, NIST, SP800-33, p. 2.

- Availability-The ongoing availability of systems addresses the processes, policies, and controls used to ensure authorized users have prompt access to information. This objective protects against intentional or accidental attempts to deny legitimate users access to information or systems.
- Integrity of Data or Systems-System and data integrity relate to the processes, policies, and controls used to ensure information has not been altered in an unauthorized manner and that systems are free from unauthorized manipulation that will compromise accuracy, completeness, and reliability.
- Confidentiality of Data or Systems-Confidentiality covers the processes, policies, and controls employed to protect information of customers and the institution against unauthorized access or use.
- Accountability-Clear accountability involves the processes, policies, and controls necessary to trace actions to their source. Accountability directly supports non-repudiation, deterrence, intrusion prevention, security monitoring, recovery, and legal admissibility of records.
- Assurance-Assurance addresses the processes, policies, and controls used to develop confidence that technical and operational security measures work as intended. Assurance levels are part of the system design and include availability, integrity, confidentiality, and accountability. Assurance highlights the notion that secure systems provide the intended functionality while preventing undesired actions.

Integrity and accountability combine to produce what is known as non-repudiation. Non-repudiation occurs when the financial institution demonstrates that the originators who initiated the transaction are who they say they are, the recipient is the intended counter party, and no changes occurred in transit or storage. Non-repudiation can reduce fraud and promote the legal enforceability of electronic agreements and transactions. While non-repudiation is a goal and is conceptually clear, the manner in which non-repudiation can be achieved for electronic systems in a practical, legal sense may have to wait for further judicial clarification.The federal E-Sign Act, 15 USC 7001, et seq., does not resolve this issue.

Regulatory Guidance, Resources, and Standards

Financial institutions developing or reviewing their information security controls, policies,

procedures, or processes have a variety of sources upon which to draw. First, federal laws and regulations address security, and regulators have issued numerous security related guidance documents.See Appendix B for a listing of laws, regulations, and agency guidance. See also the FFIEC IT Examination Handbook series of booklets, of which this booklet is a part. Institutions also have a number of third-party or security industry resources to draw upon for guidance, including outside auditors, consulting firms, insurance companies, and information security professional organizations. In addition, many national and international standard-setting organizations are working to define information security standards and best practices for electronic commerce. While no formal industry accepted security standards exist, these various standards provide benchmarks that both financial institutions and their regulators can draw upon for the development of industry expectations and security practices. Some standard-setting groups include the following organizations:

- The National Institute of Standards and Technology (NIST) at www.nist.gov;
- The International Organization for Standardization (ISO) Information technology atwww.iso.ch with specific standards such as
  The code of practice for information security management (ISO/IEC 17799) and
  Information technology-Security techniques-Evaluation criteria for IT security (ISO/IEC 15408); and
- The Information Systems Audit and Control Association (ISACA)-Control Objectives for Information Technology (CobiT), at www.isaca.org/cobit.htm.

Security Process

Action Summary

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.

Overview

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:

- Information Security Risk Assessment-A process to identify and assess threats, vulnerabilities, attacks, probabilities of occurrence, and outcomes.
- Information Security Strategy-A plan to mitigate risk that integrates technology, policies, procedures, and training. The plan should be reviewed and approved by the board of directors.
- 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.

- Security Monitoring-The use of various methodologies to gain assurance that risks are appropriately assessed and mitigated. These methodologies should verify that significant controls are effective and performing as intended.
- Security Process Monitoring and Updating-The process of continuously gathering and analyzing information regarding new threats and vulnerabilities, actual attacks on the institution or others combined with the effectiveness of the existing security controls. This information is used to update the risk assessment, strategy, and controls. Monitoring and updating makes the process continuous instead of a one-time event.
  Security risk variables include threats, vulnerabilities, attack techniques, the expected frequency of attacks, financial institution operations and technology, and the financial institution's defensive posture. All of these variables change constantly. Therefore, an institution's management of the risks requires an ongoing process.

Governance

Governance is achieved through the management structure, assignment of responsibilities and authority, establishment of policies, standards and procedures, allocation of resources, monitoring, and accountability. Governance is required to ensure that tasks are completed appropriately, that accountability is maintained, and that risk is managed for the entire enterprise. Although all aspects of institutional governance are important to the maintenance of a secure environment, this booklet will speak to those aspects that are unique to information security. This section will address the management structure, responsibilities, and accountability.

Management Structure

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. Each role has different responsibilities for information security and each individual should be accountable for his or her actions. Accountability requires clear lines of reporting, clear communication of expectations, and the delegation and judicious use of appropriate authority to bring about appropriate compliance with the institution's policies, standards, and procedures.

Responsibility and Accountability

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.

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.

Security officers should have the authority to respond to a security eventA security event occurs when the confidentiality, integrity, availability, or accountability of an information system is compromised. by ordering emergency actions to protect the financial institution and its customers from an imminent loss of information or value. They should have sufficient knowledge, background, and training, as well as an organizational position, to enable them to perform their assigned tasks.

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.

Employees should know, understand, and be held accountable for fulfilling their security responsibilities. Institutions should define these responsibilities in their security policy. Job descriptions or contracts should specify any additional security responsibilities beyond the general policies. Financial institutions can achieve effective employee awareness and understanding through security training and ongoing security-related communications, employee certifications of compliance, self-assessments, audits, and monitoring.

Internal auditors should pursue their risk-based audit program to ensure appropriate policies and procedures and the adequacy of implementation, and issue appropriate reports to the Board of Directors. For more information, refer to the "Audit" booklet in the FFIEC IT Examination Handbook.

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. For more information, refer to the "Outsourcing Technology Services" booklet in the FFIEC IT Examination Handbook.

Information Security Risk Assessment

Action Summary

Financial institutions must maintain an ongoing information security risk assessment program that effectively

- Gathers data regarding the information and technology assets of the organization, threats to those assets, vulnerabilities, existing security controls and processes, and the current security standards and requirements;
- Analyzes the probability and impact associated with the known threats and vulnerabilities to their assets; and
- Prioritizes the risks present due to threats and vulnerabilities to determine the appropriate level of training, controls, and assurance necessary for effective mitigation.

Overview

The quality of security controls can significantly influence all categories of risk.The various FFIEC agencies have different names for the various categories of risk. The Federal Reserve includes six types of risk, which are credit, market, liquidity, operational, legal, and reputational. The OCC includes nine types of risk which are credit, interest rate, liquidity, price, foreign exchange, transaction, compliance, reputation, and strategic. This booklet uses the Federal Reserve categories with the addition of strategic risk and the assumption that market risk includes interest rate risk, price risk, and foreign exchange risk.Traditionally, examiners and institutions recognized the direct impact on operational/transaction risk from incidents related to fraud, theft, or accidental damage. Many security weaknesses, however, can directly increase exposure in other risk areas. For example, the GLBA introduced additional legal/compliance risk due to the potential for regulatory noncompliance in safeguarding customer information. The potential for legal liability related to customer privacy breaches may present additional risk. Effective application access controls can strengthen credit and market risk management by enforcing risk limits on loan officers or traders. For example, if a trader were to exceed the intended trade authority, the institution may unknowingly assume additional market risk exposure.

A strong security program reduces levels of reputation, operational, legal, and strategic risk by limiting the institution's vulnerability to intrusion attempts and maintaining customer confidence and trust in the institution. Security concerns can quickly erode customer confidence and potentially decrease the adoption rate and rate of return on investment for strategically important products or services. Examiners and risk managers should incorporate security issues into their risk assessment process for each risk category. Financial institutions should ensure that security risk assessments adequately consider potential risk in all business lines and risk categories.

Information security risk assessment is the process used to identify and understand risks to the confidentiality, integrity, and availability of information and information systems. In its simplest form, a risk assessment consists of the identification and valuation of assets and an analysis of those assets in relation to potential threats and vulnerabilities, resulting in a ranking of risks to mitigate. The resulting information should be used to develop strategies to mitigate those risks.

An adequate assessment identifies the value and sensitivity of information and system components and then balances that knowledge with the exposure from threats and vulnerabilities. A risk assessment is a pre-requisite to the formation of strategies that guide the institution as it develops, implements, tests, and maintains its information systems security posture. An initial risk assessment may involve a significant one-time effort, but the risk assessment process should be an ongoing part of the information security program.

Risk assessments for most industries focus only on the risk to the business entity. Financial institutions must also consider the risk to their customers' information. For example, the 501(b) guidelines require financial institutions to "protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to any customer."

Key Steps

Common elements of risk assessment approaches involve three phases: information gathering, analysis, and prioritizing responses. Vendor concerns add additional elements to the process.

Gather Necessary Information

An effective risk assessment should be based on a current and detailed knowledge of the institution's operating and business environments. Sufficient information should be referenced in the risk assessment to document a thorough understanding of these environments. Both technical and non-technical information should be gathered. Examples of relevant technical information include network maps detailing internal and external connectivity; hardware and software inventories; databases and files that contain critical and/or confidential information; processing arrangements and interfaces with external entities; hardware and software configurations; and policies, standards, and procedures for the operation, maintenance, upgrading, and monitoring of technical systems.

Non-technical information that may be necessary includes the policies, standards, and procedures addressing physical security (including facilities as well as information assets that include loan documentation, deposit records and signature cards, and key and access code lists), personnel security (including hiring background checks and behavior monitoring), vendor contracts, personnel security training and expertise, and insurance coverage. Additionally, information regarding control effectiveness should be gathered. Typically, that information comes from security monitoring, including self-assessments, metrics, and independent tests.

Identification of Information and Information Systems

A risk assessment should include an identification of information and the information systems to be protected, including electronic systems and physical components used to access, store, transmit, protect, and eventually dispose of information. Information and information systems can be both paper-based and electronic-based.

The institution's analysis should include a system characterization and data flow analysis of networks (where feasible), computer systems, connections to business partners and the Internet, and the interconnections between internal and external systems. Some systems and data stores may not be readily apparent. For example, backup tapes, portable computers, personal digital assistants, media such as compact disks, micro drives, and diskettes, and media used in software development and testing should be considered.

In identifying information and the information systems, it is important to understand how the institution uses information in its day-to-day operations. For example, the risk assessment should address employee access, use, and dissemination of information in response to requests. Institutions should also consider how they store, transmit, transfer, and dispose of media (paper or

electronic) containing information, authorize and authenticate those who receive information both physically and electronically, and how they make information available for viewing.

A financial institution's outsourcing strategy also should be considered in identifying relevant data flows and information processing activities. The institution's system architecture diagram and related documentation should identify service provider relationships, where and how data is passed between systems, and the relevant controls that are in place.

Analyze the Information

Classify and Rank Sensitive Data, Systems, and Applications
Financial institutions should assess the relative importance of the various information systems based on the nature of their function, the criticality of data they support, and the sensitivity of data they store, transmit, or protect. When assessing the sensitivity of data, institutions should consider the increased risk posed to the institution from the aggregation of data elements.

Institutions may establish an information data classification program to identify and rank data, systems, and applications in order of importance. Classifying data allows the institution to ensure consistent protection of information and other critical data throughout the system. Classifying systems allows the institution to focus its controls and efforts in an efficient and structured manner. Systems that store or transmit data of different sensitivities should be classified as if all data were at the highest sensitivity. Classification should be based on a weighted composite of all relevant attributes.

Assess Threats and Vulnerabilities
Financial institutions should assess potential threats and vulnerabilities of their information systems. Generally, this assessment is to determine which threats or vulnerabilities deserve priority attention relative to the value of the information or information systems being protected. Although threats and vulnerabilities need to be considered simultaneously, it is important to distinguish threats from vulnerabilities.

Threats are events that could cause harm to the confidentiality, integrity, or availability of information or information systems. They can be characterized as the potential for agents exploiting a vulnerability to cause harm through the unauthorized disclosure, misuse, alteration, or destruction of information or information systems. Threats can arise from a wide variety of sources. Traditionally, the agents have been categorized as internal (malicious or incompetent employees, contractors, service providers, and former insiders) and external (criminals, recreational hackers, competitors, and terrorists). Each of the agents identified may have different capabilities and motivations, which may require the use of different risk mitigation and control techniques and the focus on different information elements or systems. Natural and man-made disasters should also be considered as agents.

Vulnerabilities can be characterized as weaknesses in a system, or control gaps that, if exploited, could result in the unauthorized disclosure, misuse, alteration, or destruction of information or information systems. Vulnerabilities are generally grouped into two types: known and expected. Known vulnerabilities are discovered by testing or other reviews of the environment, knowledge of policy weaknesses, knowledge of inadequate implementations, and knowledge of personnel issues. Adequate and timely testing is essential to identify many of these vulnerabilities. Inadequate or untimely testing may critically weaken the risk assessment.

Expected vulnerabilities to consider are those that can reasonably be anticipated to arise in the future. Examples may include unpatched software, new and unique attack methodologies that

bypass current controls, employee and contractor failures to perform security duties satisfactorily, personnel turnover resulting in less experienced and knowledgeable staff, new technology introduced with security flaws, and failure to comply with policies and procedures. Although some vulnerabilities may exist only for a short time until they are corrected, the risk assessment should consider the risk posed for the time period the vulnerability might exist.

Financial institutions should analyze through scenarios the probability of different threat agents causing damage. These scenarios should consider the financial institution's business strategy, quality of its control environment, and its own experience, or the experience of other institutions and entities, with respect to information security failures. The assignment of probabilities by the financial institution should be appropriate for the size and complexity of the institution. Simple approaches (e.g., probable, highly possible, possible, and unlikely) are generally sufficient for smaller, non-complex, financial institutions.

Business lines should also analyze the potential damage, or impact, of a threat agent's action. Impact can be measured in terms of data integrity, confidentiality, and availability of information; costs associated with finding, fixing, repairing, and restoring a system; lost productivity; financial losses; and other issues affecting the institution's operations, and reputation.

Many analytical methods may be used to arrive at the likelihood and impact of a threat agent's action. Methods fall into two general categories: quantitative and qualitative. Quantitative methods involve assigning numerical measurements that can be entered into the analysis to determine total and residual risks. Measurements may include costs to safeguard the information and information systems, value of that information and those systems, threat frequency and probability, and the effectiveness of controls. Techniques may include manual or automated data analysis to provide measurement of the potential damage in relation to the controls. A shortcoming of quantitative methods is a lack of reliable and predictive data on threat frequency and probability, and the future reliability and performance of the control structure. That shortcoming is typically addressed by assigning numeric values based on qualitative judgments.

Qualitative analysis involves the use of scenarios and attempts to determine the seriousness of threats and the effectiveness of controls. Qualitative analysis is by definition subjective, relying upon judgment, knowledge, prior experience, and industry information. Qualitative techniques may include walk-throughs, storyboarding, surveys, questionnaires, interviews, and workgroups to obtain information about the various scenarios. Each identified threat should be analyzed to determine potential severity and loss against the effectiveness of the existing control structure.

Evaluate Control Effectiveness

The institution should identify controls that will mitigate the impact or likelihood of each identified threat agent exploiting a specific vulnerability. Controls are generally categorized by timing (preventive, detective, or corrective) or nature (administrative, technical, or physical). The evaluation should recognize the unique control environment of the institution, and evaluate the effectiveness of that environment in responding to the threats arrayed against it. The evaluation should address the controls that prevent harm as well as those that detect harm and correct damage that occurs. Preventive controls act to limit the likelihood of a threat agent succeeding. Detective and corrective controls are essential to identify harmful actions as they occur, to facilitate their termination, and to reduce damage.

Controls should not be assumed to be completely effective. Measures of control effectiveness can be obtained from a well-planned and executed security monitoring program. Self-assessments, metrics, and independent tests may address compliance with existing controls and the adequacy of those controls. A well-planned and executed security monitoring program is sound industry practice and should be based on an assessment of the risk of non-compliance or circumvention of the institution's controls.

The evaluation of controls should also encompass the risks to information held and processed by service providers. An institution's contract with the service provider should contain language that establishes standards the service provider should meet and provide for periodic reporting against those standards. The contract should include a provision for the independent review of internal controls at service providers and vendors, require that timely action be taken to address identified vulnerabilities, and require a reporting to the institution of the review, its findings, and the actions taken in response to the findings. The report should be sufficient to enable the institution to evaluate contract compliance and to assess risk.

The evaluation of controls should include a review of the relevant physical access controls - including access to records, equipment, and financial institution and data center facilities - and provide an assessment of potential vulnerabilities to a physical attack or other disaster. Reviews should be comprehensive and address all data and facilities, including remote facilities. Because the risk from many threat scenarios may be mitigated by physical as well as other controls, the physical control evaluation is an integral part of the overall scenario evaluation.

Assign Risk Ratings

After completing the inventory of information and systems, assessing the likelihood and exposure of identified threats and vulnerabilities, and evaluating control effectiveness, the institution should assign risk ratings to the information and information systems. The key to assigning risk ratings is to organize the information and information systems within a logical framework.

The framework should recognize that not all threats and risks are equal and acknowledge that financial institutions have finite managerial and financial resources. As with credit or interest rate risk, reasonably foreseeable risks should be prioritized and rated according to the sensitivity and importance of the information.

The probability or likelihood of an event occurring, and the impact the event would have on a financial institution should be considered in determining the appropriate risk rating for information. The probability of an event occurring, and its impact on the institution, is directly influenced by a financial institution's business profile and the effectiveness of its controls. Typically, the result is expressed in differing levels of risk, for example, "High," "Medium," or "Low" ratings. The specific risk rating is judgmentally determined and assigned in relation to the level of exposure and the threat likelihood, taking into consideration the adequacy of related internal controls. Where controls are inadequate or found not to exist, the risk assessment should include an action plan to improve the controls.

Once the risks associated with threats and vulnerabilities have been assessed, probabilities assigned, and risks rated, risks should be segregated into those the financial institution is willing to accept and those that should be mitigated. Guidance from the board of directors should be used for that segregation. Once the institution identifies the risks to mitigate, it can begin to develop its risk mitigation strategy.

Key Risk Assessment Practices

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

- 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.

- Systematic and Central Control-Defined procedures and central control and coordination help to ensure standardization, consistency, and completeness of risk assessment policies and procedures, as well as coordination in planning and performance. Central control and coordination will also facilitate an organizational view of risks and lessons learned from the risk assessment process.
- Integrated Process-A risk assessment provides a foundation for the remainder of the security process by guiding the selection and implementation of security controls and the timing and nature of testing those controls. Testing results, in turn, provide evidence to the risk assessment process that the controls selected and implemented are achieving their intended purpose. Testing can also validate the basis for accepting risks.
- 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.
- Documentation-Documentation of the risk assessment process and procedures assists in ensuring consistency and completeness as well as accountability. This documentation provides a useful starting point for subsequent assessments, potentially reducing the effort required in those assessments. Decisions to mitigate or accept risk should be documented in order to achieve accountability for risk 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.

Information Security Strategy

Action Summary

Financial institutions should develop a strategy that defines control objectives and establishes an implementation plan. The security strategy should include

- Appropriate consideration of prevention, detection, and response mechanisms,
- Implementation of the least permissions and least privileges concepts,
- Layered controls that establish multiple control points between threats and organization

assets, and
- Policies that guide officers and employees in implementing the security program.

Information Security Strategy

An information security strategy is a plan to mitigate risks while complying with legal, statutory, contractual, and internally developed requirements. Typical steps to building a strategy include the definition of control objectives, the identification and assessment of approaches to meet the objectives, the selection of controls, the establishment of benchmarks and metrics, and the preparation of implementation and testing plans.

The selection of controls is typically grounded in a cost comparison of different strategic approaches to risk mitigation. The cost comparison typically contrasts the costs of various approaches with the potential gains a financial institution could realize in terms of increased confidentiality, availability, or integrity of systems and data. Those gains could include reduced financial losses, increased customer confidence, positive audit findings, and regulatory compliance. Any particular approach should consider: (1) policies, standards, and procedures; (2) technology design; (3) resource dedication; (4) training; and (5) testing.

For example, an institution's management may be assessing the proper strategic approach to the security monitoring of activities for an Internet environment. Two potential approaches are identified for evaluation. The first approach uses a combination of network and host sensors with a staffed monitoring center. The second approach consists of daily access log review. The former alternative is judged much more capable of detecting an attack in time to minimize any damage to the institution and its data, albeit at a much greater cost. The added cost is entirely appropriate when customer data and institution processing capabilities are exposed to an attack, such as in an Internet banking environment. The latter approach may be appropriate when the primary risk is reputational damage, such as when the only information being protected is an information-only Web site, and the Web site is not connected to other financial institution systems.

Key Concepts

Security requires the integration of people, process, and technology. Each of the three components should be managed considering the capabilities and limitations of the other components. When the components are considered in total, they should provide for adequate overall risk mitigation.

Security strategies include prevention, detection, and response, and all three are needed for a comprehensive and robust security framework. Typically, security strategies focus most resources on prevention. Prevention addresses the likelihood of harm. Detection and response are generally used to limit damage once a security breech has occurred. Weaknesses in prevention may be offset by strengths in detection and response.

Security strategies should establish limitations on access and limitations on the ability to perform unauthorized actions. Those limitations derive from concepts known as security domains, least permissions, and least privileges.

The creation of security domains involves designing a network so that users and network resources are grouped in a logical or physical manner, and control sets are established to mitigate the risks relevant to each individual domain. At the network level, connectivity between network areas may be disabled, or tightly controlled through perimeters. Tools could include firewalls, virtual local area networks (VLANs), router access control lists (ACLs), and directories. The tools allow for restrictions on access and authorizations at the network and application layers.

The concepts of least permissions and least privileges are used to provide functionality while limiting potentially harmful actions. They generally involve restricting authorizations at the network, server, and client level. For example, a user could be allowed access to only certain network resources and denied access to others. A user could be allowed access to some program functions or file areas and not allowed access to others. A program could be allowed access to some of a computer's or network's resources and disallowed access to others. Authorization for users most often is managed by assigning a user to a group, and granting permissions to the group.

Financial institutions should design multiple layers of security controls to establish several lines of defense between the attacker and the asset being attacked.An Internet security example of this concept may involve the following configuration: a packet filtering router with strict access control rules, in front of an application level firewall, in front of Web servers, in front of a transactional server, in front of a database server, with intrusion detection systems located at various points between the servers and on certain hosts. The layers should be at multiple control points throughout the communication and transactional flow and should include both systems and manual processes. To successfully attack an asset, each layer must be penetrated. With each penetration, the probability of detecting the attacker increases.

Architecture Considerations

Financial institutions can gain valuable insights into the development of a security architecture and the integration of that architecture into their other technology processes by referencing one or more widely recognized technology standards. Examples of the standards include

- Control Objectives for Information and Related Technology (CobiT) - provides a broad and deep framework for controls.
- IT Infrastructure Library (ITIL) - provides a list of recognized practices for IT service management.
- ISO 17799 - provides a library of possible controls that can be included in an architecture and guidance in control selection.
- BITS (Bank Information Technology Secretariat) and other industry publications for discrete controls, such as vendor management.

Primary considerations in a network security architecture are the policies, standards, and procedures employed as a part of the governance structure and the technology design. Other considerations are the necessary resources, personnel training, and testing. Each should be appropriate for the size and complexity of the institution and sufficiently flexible to allow for timely and necessary updates to keep pace with changes in technology and the overall environment.

Policies and Procedures

Technology Design

A financial institution can significantly mitigate the risk of security events by an appropriate technology design that provides for effective network-level monitoring, limits an intruder's ability to traverse the network, offers the minimum level of services required for business needs, and is updated in a timely manner to mitigate newly discovered vulnerabilities.

An effective means of accomplishing those goals is through the use of security domains. A security domain is a part of the system with its own policies and control mechanisms. Security domains for a network are typically constructed from routing controls and directories.

Domains constructed from routing controls may be bounded by network perimeters with perimeter controls. The perimeters separate what is not trusted from what may be trustworthy. The perimeters serve as well-defined transition points between trust areas where policy enforcement and monitoring takes place. An example of such a domain is a demilitarized zone (DMZ), bounded by a perimeter that controls access from outside and inside the institution.

Domains constructed from directories may limit access to network resources and applications based on role or function. Directory-driven domains may allow access to different network-driven domains. For example, a network management domain may use the same cabling and network interface cards as other domains, allow access to all computing devices in all domains, but limit the allowed access based on the user's role or function.

The selection of where to put which control is a function of the risk assessment. Institutions generally should establish defenses that address the network and application layers at external connections, whether from the Internet or service providers. Internally, perimeters can be established at higher-risk security domains, such as wire transfer, and to segregate at a network level those areas of the institution that work with customer information from other areas. Internal perimeters also may be used to create security domains based on geography or other logical or physical separations.

Hosts may also include security perimeters. Those perimeters are enforced through authorizations for users and programs. The authorizations can be a part of applications, the file system, and the operating system.

Outsourced Security Services

Security services may be outsourced to obtain greater expertise, a greater range of services, or to decrease cost. Should security services be outsourced, the institution retains the same responsibilities for security as if those services were performed in-house. The "Outsourcing Technology Servicing" booklet in the FFIEC IT Examination Handbook, provides additional information relevant to outsourcing.

Institutions should ensure they have sufficient expertise to oversee and manage an outsourced security service relationship. The expertise applied to monitor the outsourced security service relationship should be both contract-related, and security-related. The contract-related oversight addresses contract compliance. The security-related oversight entails understanding the scope and nature of the service sufficiently to identify and appropriately react when the services provided are not at the level indicated in the service level agreement, no longer appropriately coordinate with the security controls at the institution, or no longer provide the risk mitigation desired.

Institutions should monitor outsourced security service providers appropriate to the level of risk to ensure the service provider fulfills its responsibilities. Monitoring tools include reports from the service provider, independent reviews of the service provider's performance, and independent tests of the service provided.

Security Controls Implementation

Access Control

The goal of access control is to allow access by authorized individuals and devices and to disallow access to all others.

Authorized individuals may be employees, technology service provider (TSP) employees, vendors, contractors, customers, or visitors. Access should be authorized and provided only to individuals whose identity is established, and their activities should be limited to the minimum required for business purposes.

Authorized devices are those whose placement on the network is approved in accordance with institution policy. Change controls are typically used for devices inside the external perimeter, and to configure institution devices to accept authorized connections from outside the perimeter.

An effective control mechanism includes numerous controls to safeguard and limits access to key information system assets at all layers in the network stack. This section addresses logical and administrative controls, including access rights administration for individuals and network access issues. A subsequent section addresses physical security controls.

Access Rights Administration

Action Summary

Financial institutions should have an effective process to administer access rights. The process should include:

- Assigning users and devices only the access required to perform their required functions,
- Updating access rights based on personnel or system changes,
- Reviewing periodically users' access rights at an appropriate frequency based on the risk to the application or system, and
- Designing appropriate acceptable-use policies and require users to agree to them in writing.

System devices, programs, and data are system resources. Each system resource may need to be accessed by individuals (users) in order for work to be performed. Access beyond the minimum

required for work to be performed exposes the institution's systems and information to a loss of confidentiality, integrity, and availability. Accordingly, the goal of access rights administration is to identify and restrict access to any particular system resource to the minimum required for work to be performed. The financial institution's security policy should address access rights to system resources and how those rights are to be administered.

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.

Formal access rights administration for users consists of four processes:

- An enrollment process to add new users to the system;
- An authorization process to add, delete, or modify authorized user access to operating systems, applications, directories, files, and specific types of information;
- An authentication process to identify the user during subsequent activities; and
- A monitoring process to oversee and manage the access rights granted to each user on the system.

The enrollment process establishes the user's identity and anticipated business needs for information and systems. New employees, IT outsourcing relationships, and contractors may also be identified, and the business need for access determined during the hiring or contracting process.

During enrollment and thereafter, an authorization process determines user access rights. In certain circumstances the assignment of access rights may be performed only after the manager responsible for each accessed resource approves the assignment and documents the approval. In other circumstances, the assignment of rights may be established by the employee's role or group membership, and managed by pre-established authorizations for that group. Customers, on the other hand, may be granted access based on their relationship with the institution.

Authorization for privileged access should be tightly controlled. Privileged access refers to the ability to override system or application controls. Good practices for controlling privileged access include

- Identifying each privilege associated with each system component,
- Implementing a process to allocate privileges and allocating those privileges either on a need-to-use or an event-by-event basis,
- Documenting the granting and administrative limits on privileges,
- Finding alternate ways of achieving the business objectives,
- Assigning privileges to a unique user ID apart from the one used for normal business use,
- Logging and auditing the use of privileged access,
- Reviewing privileged access rights at appropriate intervals and regularly reviewing privilege access allocations,See ISO17799, 9.2.4 and
- Prohibiting shared privileged access by multiple users.

The access rights process programs the system to allow the users only the access rights they were granted. Since access rights do not automatically expire or update, periodic updating and review of access rights on the system is necessary. Updating should occur when an individual's business needs for system use changes. Many job changes can result in an expansion or reduction of access rights. Job events that would trigger a removal of access rights include transfers,

resignations, and terminations. When these job events occur, institutions should take particular care to promptly remove the access rights for users who have remote access privileges, access to customer information, and perform administration functions for the institution's systems.

Because updating may not always be accurate, periodic review of user accounts is a good control to test whether the access right removal processes are functioning and whether users exist who should have their rights rescinded or reduced. Financial institutions should review access rights on a schedule commensurate with risk.ISO17799, 9.2.4 requires reviews at six month intervals.

Access rights to new software and hardware present a unique problem. Typically, hardware and software are shipped with default users, with at least one default user having full access rights. Easily obtainable lists of popular software exist that identify the default users and passwords, enabling anyone with access to the system to obtain the default user's access. Default user accounts should either be disabled, or the authentication to the account should be changed. Additionally, access to these default accounts should be monitored more closely than other accounts.

Sometimes software installs with a default account that allows anonymous access. Anonymous access is appropriate, for instance, where the general public accesses an informational Web server. Systems that allow access to or store sensitive information, including customer information, should be protected against anonymous access.

The access rights process also constrains user activities through an acceptable-use policy (AUP). Users who can access internal systems typically are required to agree to an AUP before using a system. An AUP details the permitted system uses and user activities and the consequences of noncompliance. AUPs can be created for all categories of system users, from internal programmers to customers. An AUP is a key control for user awareness and administrative policing of system activities. Examples of AUP elements for internal network and stand-alone users include

- The specific access devices that can be used to access the network;
- Hardware and software changes the user can make to their access device;
- The purpose and scope of network activity;
- Network services that can be used and those that cannot be used;
- Information that is allowable and not allowable for transmission using each allowable service;
- Bans on attempting to break into accounts, crack passwords, or disrupt service;
- Responsibilities for secure operation; and
- Consequences of noncompliance.

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.

Customers may be provided with a Web site disclosure as their AUP. Based on the nature of the Web site, the financial institution may require customers to demonstrate knowledge of and agreement to abide by the terms of the AUP. That evidence can be paper based or electronic.

Authorized users may seek to extend their activities beyond what is allowed in the AUP, and unauthorized users may seek to gain access to the system and move within the system. Network security controls provide many of the protections necessary to guard against those threats.

Authentication

Action Summary

Financial institutions should use effective authentication methods appropriate to the level of risk. Steps include

- Selecting authentication mechanisms based on the risk associated with the particular application or services;
- Considering whether multi-factor authentication is appropriate for each application, taking into account that multi-factor authentication is increasingly necessary for many forms of electronic banking and electronic payment activities; and
- Encrypting the transmission and storage of authenticators (e.g., passwords, personal identification numbers (PINs), digital certificates, and biometric templates).

Authentication is the verification of identity by a system based on the presentation of unique credentials to that system. The unique credentials are in the form of something the user knows, something the user has, or something the user is. Those forms exist as shared secrets, tokens, or biometrics. More than one form can be used in any authentication process. Authentication that relies on more than one form is called multi-factor authentication and is generally stronger than any single-factor authentication method. Authentication contributes to the confidentiality of data and the accountability of actions performed on the system by verifying the unique identity of the system user.

Authentication over the Internet banking delivery channel presents unique challenges. That channel does not benefit from physical security and controlled computing and communications devices like internal local area networks (LANs), and is used by people whose actions cannot be controlled by the institution. The agencies consider the use of single-factor authentication in that environment, as the only control mechanism, to be inadequate for high-risk transactions involving access to customer information or the movement of funds to other parties. Financial institutions should perform risk assessments of their environment and, where the risk assessments indicate the use of single-factor authentication is inadequate, the institutions should implement multi-factor authentication, layered security, or other controls reasonably calculated to mitigate risk.

Authentication is not identification as that term is used in the USA PATRIOT Act (31 USC 5318 (l)). Authentication does not provide assurance that the initial identification of a system user is proper. Procedures for the initial identification of a system user are beyond the scope of this booklet.

Shared Secret Systems

Shared secret systems uniquely identify the user by matching knowledge on the system to knowledge that only the system and user are expected to share. Examples are passwords, pass phrases, or current transaction knowledge. A password is one string of characters (e.g., "t0Ol@Tyme"). A pass phrase is typically a string of words or characters (e.g., "My car is a shepherd") that the system may shorten to a smaller password by means of an algorithm. Current transaction knowledge could be the account balance on the last statement mailed to the user/ customer. The strength of shared secret systems is related to the lack of disclosure of and about the secret, the difficulty in guessing or discovering the secret, and the length of time that the secret exists before it is changed.

A strong shared secret system only involves the user and the system in the generation of the shared secret. In the case of passwords and pass phrases, the user should select them without any assistance from any other user, such as the help desk. One exception is in the creation of new accounts, where a temporary shared secret could be given to the user for the first log-in, after which the system requires the user to create a different password. Controls should prevent any user from re-using shared secrets that may have been compromised or were recently used by them.

Passwords are the most common authentication mechanism. Passwords are generally made difficult to guess when they are composed from a large character set, contain a large number of characters, and are frequently changed. However, since hard-to-guess passwords may be difficult to remember, users may take actions that weaken security, such as writing the passwords down. Any password system must balance the password strength with the user's ability to maintain the password as a shared secret. When the balancing produces a password that is not sufficiently strong for the application, a different authentication mechanism should be considered. Pass phrases are one alternative to consider. Due to their length, pass phrases are generally more resistant to attack than passwords. The length, character set, and time before enforced change are important controls for pass phrases as well as passwords.

Shared secret strength is typically assured through the use of automated tools that enforce the password selection policy. Authentication systems should force changes to shared secrets on a schedule commensurate with risk.

Passwords that are either not changed or changed infrequently are known as static passwords. While all passwords are subject to disclosure, static passwords are significantly more vulnerable. An attacker can obtain a password through technical means and through social engineering. Internet banking customers are targeted for such social engineering through phishing attacks. Institution employees and contractors may be similarly targeted. Static passwords are appropriate in systems whose data and connectivity is considered low risk, and in systems that employ effective compensating controls such as physical protections, device authentication, mutual authentication, host security, user awareness, and effective monitoring and rapid response.

Weaknesses in static password mechanisms generally relate to the ease with which an attacker can discover the secret. Attack methods vary.

- A keylogger or other monitoring device on the user's computer may record shared secrets and transmit them to the attacker. Keyloggers and other similar devices are an emerging problem for e-banking applications because financial institutions do not control the customer's computer.
  - Controls to protect against keyloggers include using different authentication methods such as dynamic passwords.
- A dictionary attack is one common and successful way to discover passwords. In a dictionary attack, the attacker obtains the system password file and compares the password hashes against hashes of commonly used passwords.
  - Controls against dictionary attacks include securing the password file from compromise, detection mechanisms to identify a compromise, heuristicBehavior-based intrusion detection to detect differences in user behavior, and rapid reissuance of passwords should the password file ever be compromised. While extensive character sets and storing passwords as one-way hashes can slow down a dictionary attack, those defensive mechanisms primarily buy the financial institution time to identify and react to the password file compromises.
- An additional attack method targets a specific account and submits passwords until the correct password is discovered.
  - Controls against these attacks are account lockout mechanisms, which commonly lock

out access to the account after a risk-based number of failed login attempts.Existing industry practice is no more than five access attempts for customer retail account access.

- A variation of the previous attack uses a popular password, and tries it against a wide range of usernames.
  - Controls against this attack on the server are a high ratio of possible passwords to usernames, randomly generated passwords, and scanning the Internet protocol (IP) addresses of authentication requests and client cookies for submission patterns.
- Password guessing attacks also exist. These attacks generally consist of an attacker gaining knowledge about the account holder and password policies and using that knowledge to guess the password.
  - Controls include training in and enforcement of password policies that make passwords difficult to guess. Such policies address the secrecy, length of the password, character set, prohibition against using well-known user identifiers, and length of time before the password must be changed. Users with greater authorization or privileges, such as root users or administrators, should have longer, more complex passwords than other users.
- Some attacks depend on patience, waiting until the logged-in workstation is unattended.
  - Controls include automatically logging the workstation out after a period of inactivityExisting industry practice is no more than 20-30 minutes but may be substantially less depending on the application. and heuristic intrusion detection.
- Attacks can take advantage of automatic log-in features, allowing the attacker to assume an authorized user's identity merely by using a workstation.
  - Controls include prohibiting and disabling automatic log-in features, screensaver activation that requires user re-authentication, and heuristic intrusion detection.
- Users' inadvertent or unthinking actions can compromise passwords. For instance, when a password is too complex to readily memorize, the user could write the password down but not secure the paper. Frequently, written-down passwords are readily accessible to an attacker under mouse pads or in other places close to the user's machines. Additionally, attackers frequently are successful in obtaining passwords by using social engineering and tricking the user into giving up their password.
  - Controls include user training, heuristic intrusion detection, and simpler passwords combined with another authentication mechanism.
- Attacks can also become much more effective or damaging if different network devices share the same or a similar password.
  Controls include a policy that forbids the same or similar password on particular network devices.

Passwords can also be dynamic. Dynamic passwords typically use seeds,A "seed" is a starting point for the dynamic password system. Shared starting points, timing, and logic between the token and the server allow password changes to synchronize between the two devices. or starting points, and algorithms to calculate a new shared secret for each access. Because each password is used for only one access, dynamic passwords can provide significantly more authentication strength than static passwords. In most cases, dynamic passwords are implemented through tokens. A token is a physical device, such as an ATM card, smart card, or other device that contains information used in the authentication process.

Token Systems

Token systems typically authenticate the token and assume that the user who was issued the token is the one requesting access. One example is a token that generates dynamic passwords after a set number of seconds. When prompted for a password, the user enters the password generated by the token. The token's password-generating system is identical and synchronized to that in the system, allowing the system to recognize the password as valid. The strength of this system of authentication rests in the frequent changing of the password and the inability of an attacker to guess the seed and password at any point in time.

Another example of a token system uses a challenge/response mechanism. In this case, the user identifies him/herself to the system, and the system returns a code to enter into the password-generating token. The token and the system use identical logic and initial starting points to separately calculate a new password. The user enters that password into the system. If the system's calculated password matches that entered by the user, the user is authenticated. The strengths of this system are the frequency of password change and the difficulty in guessing the challenge, seed, and password.

Other token methods involve multi-factor authentication, or the use of more than one authentication method. For instance, an ATM card is a token. The magnetic strip on the back of the card contains a code that is recognized in the authentication process. However, the user is not authenticated until he or she also provides a PIN, or shared secret. This method is two-factor, using both something the user has and something the user knows. Two-factor authentication is generally stronger than single-factor authentication. This method can allow the institution to authenticate the user as well as the token.

Weaknesses in token systems relate to theft or loss of the token either during delivery to the user or while in the possession of the user; ease in guessing any password-generating algorithm within the token; ease of successfully forging any authentication credential that unlocks the token; the reverse engineering, or cloning, of the token; and "man-in-the-middle" attacks. Each of these weaknesses can be addressed through additional control mechanisms. Token theft or loss generally is protected against by policies that require prompt reporting and cancellation of the token's ability to allow access to the system, and monitoring of token delivery and use. Additionally, the impact of token theft is reduced when the token is used in multi-factor authentication; for instance, the password from the token is paired with a password known only by the user and the system. This pairing reduces the risk posed by token loss, while increasing the strength of the authentication mechanism. Forged credentials are protected against by the same methods that protect credentials in non-token systems. Protection against reverse engineering requires physical and logical security in token design. For instance, token designers can increase the difficulty of opening a token without causing irreparable damage, or obtaining information from the token either by passive scanning or active input/output. Man-in-the-middle attacks can be protected against through the use of public key infrastructure (PKI).

Token systems can also incorporate public key infrastructure and biometrics.

Public Key Infrastructure

Public key infrastructure, if properly implemented and maintained, can provide a strong means of authentication. By combining a variety of hardware components, system software, policies, practices, and standards, PKI can provide for authentication, data integrity, defenses against customer repudiation, and confidentiality. The system is based on public key cryptography in which each user has a key pair-a unique electronic value called a public key and a mathematically related private key. The public key is made available to those who need to verify the user's identity.

The private key is stored on the user's computer or a separate device such as a smart card. When the key pair is created with strong encryption algorithms and input variables, the probability of deriving the private key from the public key is extremely remote. The private key must be stored in encrypted text and protected with a password or PIN to avoid compromise or disclosure. The private key is used to create an electronic identifier called adigital signature that uniquely identifies the holder of the private key and can only be authenticated with the corresponding public key.

The certificate authority (CA), which may be the financial institution or its service provider, plays

a key role by attesting with a digital certificate that a particular public key and the corresponding private key belongs to a specific user or system. It is important when issuing a digital certificate that the registration process for initially verifying the identity of users is adequately controlled. The CA attests to the individual user's identity by signing the digital certificate with its own private key, known as the root key. Each time the user establishes a communication link with the financial institution's systems, a digital signature is transmitted with a digital certificate. These electronic credentials enable the institution to determine that the digital certificate is valid, identify the individual as a user, and confirm that transactions entered into the institution's computer system were performed by that user.

The user's private key exists electronically and is susceptible to being copied over a network as easily as any other electronic file. If it is lost or compromised, the user can no longer be assured that messages will remain private or that fraudulent or erroneous transactions would not be performed. User AUPs and training should emphasize the importance of safeguarding a private key and promptly reporting its compromise.

PKI minimizes many of the vulnerabilities associated with passwords because it does not rely on shared secrets to authenticate customers, its electronic credentials are difficult to compromise, and user credentials cannot be stolen from a central server.Private keys are necessary to defeat the system, and those keys are stored in a distributed fashion on each user's access device. The primary drawback of a PKI authentication system is that it is more complicated and costly to implement than user names and passwords. Whether the financial institution acts as its own CA or relies on a third party, the institution should ensure its certificate issuance and revocation policies and other controls discussed below are followed.

When utilizing PKI policies and controls, financial institutions need to consider the following:

- Defining within the certificate issuance policy the methods of initial verification that are appropriate for different types of certificate applicants and the controls for issuing digital certificates and key pairs;
- Selecting an appropriate certificate validity period to minimize transactional and reputation risk exposure-expiration provides an opportunity to evaluate the continuing adequacy of key lengths and encryption algorithms, which can be changed as needed before issuing a new certificate;
- Ensuring that the digital certificate is valid by such means as checking a certificate revocation list before accepting transactions accompanied by a certificate;
- Defining the circumstances for authorizing a certificate's revocation, such as the compromise of a user's private key or the closing of user accounts;
- Updating the database of revoked certificates frequently, ideally in real-time mode;
- Employing stringent measures to protect the root key including limited physical access to CA facilities, tamper-resistant security modules, dual control over private keys and the process of signing certificates, as well as the storage of original and back-up keys on computers that do not connect with outside networks;
- Requiring regular independent audits to ensure controls are in place, public and private key lengths remain appropriate, cryptographic modules conform to industry standards, and procedures are followed to safeguard the CA system;
- Recording in a secure audit log all significant events performed by the CA system, including the use of the root key, where each entry is time/date stamped and signed;
- Regularly reviewing exception reports and system activity by the CA's employees to detect malfunctions and unauthorized activities; and
- Ensuring the institution's certificates and authentication systems comply with widely accepted PKI standards to retain the flexibility to participate in ventures that require the acceptance of the financial institution's certificates by other CAs.

The encryption components of PKI are addressed more fully under "Encryption."

Biometrics

Biometrics can be implemented in many forms, including tokens. Biometrics verifies the identity of the user by reference to unique physical or behavioral characteristics. A physical characteristic can be a thumbprint or iris pattern. A behavioral characteristic is the unique pattern of key depression strength and pauses made on a keyboard when a user types a phrase. The strength of biometrics is related to the uniqueness of the physical characteristic selected for verification. Biometric technologies assign data values to the particular characteristics associated with a certain feature. For example, the iris typically provides many more characteristics to store and compare, making it more unique than facial characteristics. Unlike other authentication mechanisms, a biometric authenticator does not rely on a user's memory or possession of a token to be effective. Additional strengths are that biometrics do not rely on people to keep their biometric secret or physically secure their biometric. Biometrics is the only authentication methodology with these advantages.

Enrollment is a critical process for the use of biometric authentication. The user's physical characteristics must be reliably recorded. Reliability may require several samples of the characteristic and a recording device free of lint, dirt, or other interference. The enrollment device must be physically secure from tampering and unauthorized use.

When enrolled, the user's biometric is stored as a template. Subsequent authentication is accomplished by comparing a submitted biometric against the template, with results based on probability and statistical confidence levels. Practical usage of biometric solutions requires consideration of how precise systems must be for positive identification and authentication. More precise solutions increase the chances a person is falsely rejected. Conversely, less precise solutions can result in the wrong person being identified or authenticated as a valid user (i.e., false acceptance rate). The equal error rate (EER) is a composite rating that considers the false rejection and false acceptance rates. Lower EERs mean more consistent operations. However, EER is typically based upon laboratory testing and may not be indicative of actual results due to factors that can include the consistency of biometric readers to capture data over time, variations in how users presents their biometric sample (e.g., occasionally pressing harder on a finger scanner), and environmental factors.

Weaknesses in biometric systems relate to the ability of an attacker to submit false physical characteristics or to take advantage of system flaws to make the system erroneously report a match between the characteristic submitted and the one stored in the system. In the first situation, an attacker might submit to a thumbprint recognition system a copy of a valid user's thumbprint. The control against this attack involves ensuring a live thumb was used for the submission. That can be done by physically controlling the thumb reader, for instance having a guard at the reader to make sure no tampering or fake thumbs are used. In remote entry situations, logical liveness tests can be performed to verify that the submitted data is from a live subject.

Attacks that involve making the system falsely deny or accept a request take advantage of either the low degrees of freedom in the characteristic being tested, or improper system tuning. Degrees of freedom relate to measurable differences between biometric readings, with more degrees of freedom indicating a more unique biometric. Facial recognition systems, for instance, may have only nine degrees of freedom while other biometric systems have over one hundred. Similar faces may be used to fool the system into improperly authenticating an individual. Similar irises, however, are difficult to find and even more difficult to fool a system into improperly authenticating.

Attacks against system tuning also exist. Any biometric system has rates at which it will falsely

accept a reading and falsely reject a reading. The two rates are inseparable; for any given system improving one worsens the other. Systems that are tuned to maximize user convenience typically have low rates of false rejection and high rates of false acceptance. Those systems may be more open to successful attack.

Authenticator Reissuance

Authorized users may need to have authenticators reissued. Many situations create that need, such as the user forgetting the shared secret, losing a token, or the change of a biometric identifier. Prior to reissuing an authenticator, institutions should appropriately verify the identity of the receiving individual. The strength of the verification should be appropriate to mitigate the risk of impersonation. For example, the comparison of Internet-banking customer responses to questions regarding readily available public information generally is not an adequate risk mitigator.

Behavioral Authentication

Behavioral authentication is the assurance gained from comparing connection-related and activity-related information with expectations. For example, many institutions may expect Internet banking activity from certain Internet Protocol (IP) ranges to use certain user agents, to traverse the Web site in a certain manner, and to submit transactions that have certain characteristics. Although behavioral authentication does not provide strong assurance that individuals are who they claim to be, it may provide a strong indication that authenticators presented are from an imposter. Accordingly, behavioral authentication is frequently useful to supplement other means of authentication.

Device Authentication

Device authentication typically takes place either as a supplement to the authentication of individuals or when assurance is needed that the device is authorized to be on the network.

Devices are authenticated through either shared secrets, such as pre-shared keys, or the use of PKI. Authentication can take place at the network level and above. At the network level, IPv6IPv6 is one of two Internet protocols in widespread use. The other is IPv4.has the built-in ability to authenticate each device.

Device authentication is subject to the same shared-secret and PKI weaknesses as user authentication, and is subject to similar offsetting controls. Additionally, similar to user authentication, if the device is under the attacker's control or if the authentication mechanism has been compromised, communications from the device should not be trusted.

Mutual Authentication

Mutual authentication occurs when all parties to a communication authenticate themselves to the other parties. Authentications can be single or multifactor. An example of a mutual authentication is the identification of an Internet banking user to the institution, the display of a shared secret from the institution to the user, and the presentation of a shared secret from the user back to the institution. An advantage of mutual authentication is the assurance that communications are between trusted parties. However, various attacks, such as man-in-the-middle attacks, can thwart mutual authentication schemes.

Authentication for Single Sign-On Protocols

Several single sign-on protocols are in use. Those protocols allow clients to authenticate

themselves once to obtain access to a range of services. An advantage of single sign-on systems is that users do not have to remember or possess multiple authentication mechanisms, potentially allowing for more complex authentication methods and fewer user-created weaknesses. Disadvantages include the broad system authorizations potentially tied to any given successful authentication, the centralization of authenticators in the single sign-on server, and potential weaknesses in the single sign-on technologies.

When single sign-on systems allow access for a single log-in to multiple instances of sensitive data or systems, financial institutions should employ robust authentication techniques, such as multi-factor, PKI, and biometric techniques. Financial institutions should also employ additional controls to protect the authentication server and detect attacks against the server and server communications.

Examples of Common Authentication Weaknesses, Attacks, and Offsetting Controls

All authentication methodologies display weaknesses. Those weaknesses are of both a technical and a nontechnical nature. Many of the weaknesses are common to all mechanisms. Examples of common weaknesses include warehouse attacks, social engineering, client attacks, replay attacks, man-in-the-middle attacks, and hijacking.

Warehouse attacks result in the compromise of the authentication storage system and the theft of the authentication data. Frequently, the authentication data is encrypted; however, dictionary attacks make decryption of even a few passwords in a large group a trivial task. A dictionary attack uses a list of likely authenticators, such as passwords, runs the likely authenticators through the encryption algorithm, and compares the result to the stolen, encrypted authenticators. Any matches are easily traceable to the pre-encrypted authenticator.

Dictionary and brute forceAn attack that tries all possible combinations of the allowed character set. attacks are viable due to the speeds with which comparisons are made. As microprocessors increase in speed, and technology advances to ease the linking of processors across networks, those attacks will be even more effective. Because those attacks are effective, institutions should take great care in securing their authentication databases. Institutions that use one-way hashes should consider the insertion of secret bits (also known as "salt") to increase the difficulty of decrypting the hash. The salt has the effect of increasing the number of potential authenticators that attackers must check for validity, thereby making the attacks more time consuming and creating more opportunity for the institution to identify and react to the attack.

Warehouse attacks typically compromise an entire authentication mechanism. Should such an attack occur, the financial institution might have to deny access to all or nearly all users until new authentication devices can be issued (e.g. new passwords). Institutions should consider the effects of such a denial of access, and appropriately plan for large-scale re-issuances of authentication devices.

Social engineering involves an attacker obtaining authenticators by simply asking for them. For instance, the attacker may masquerade as a legitimate user who needs a password reset or as a contractor who must have immediate access to correct a system performance problem. By using persuasion, being aggressive, or using other interpersonal skills, the attackers encourage a legitimate user or other authorized person to give them authentication credentials. Controls against these attacks involve strong identification policies and employee training.

Client attacks are an area of vulnerability common to all authentication mechanisms. Passwords, for instance, can be captured by hardware- or software-based keystroke capture mechanisms. PKI private keys could be captured or reverse-engineered from their tokens. Protection against these attacks primarily consists of physically securing the client systems, and, if a shared secret is used,

changing the secret on a frequency commensurate with risk. While physically securing the client system is possible within areas under the financial institution's control, client systems outside the institution may not be similarly protected.

Replay attacks occur when an attacker eavesdrops and records the authentication as it is communicated between a client and the financial institution system and then later uses that recording to establish a new session with the system and masquerade as the true user. Protections against replay attacks include changing cryptographic keys for each session, using dynamic passwords, expiring sessions through the use of time stamps, expiring PKI certificates based on dates or number of uses, and implementing liveness tests for biometric systems.

Man-in-the-middle attacks place the attacker's computer in the communication line between the server and the client. The attacker's machine can monitor and change communications. Controls against man-in-the-middle attacks include prevention through host and client hardening, appropriate hardening and monitoring of domain name service (DNS) servers and other network infrastructure, authentication of the device communicating with the server, and the use of PKI.

Hijacking is an attacker's use of an authenticated user's session to communicate with system components. Controls against hijacking include encryption of the user's session and the use of encrypted cookies or other devices to authenticate each communication between the client and the server.

Network Access

Action Summary

Financial institutions should secure access to their computer networks through multiple layers of access controls to protect against unauthorized access. Institutions should

- Group network servers, applications, data, and users into security domains (e.g., untrusted external networks, external service providers, or various internal user systems);
- Establish appropriate access requirements within and between each security domain;
- Implement appropriate technological controls to meet those access requirements consistently; and
- Monitor cross-domain access for security policy violations and anomalous activity.

Network security requires effective implementation of several control mechanisms to adequately secure access to systems and data. Financial institutions must evaluate and appropriately implement those controls relative to the complexity of their network. Many institutions have increasingly complex and dynamic networks stemming from the growth of distributed computing.

Security personnel and network administrators have related but distinct responsibilities for ensuring secure network access across a diverse deployment of interconnecting network servers, file servers, routers, gateways, and local and remote client workstations. Security personnel typically lead or assist in the development of policies, standards, and procedures, and monitor compliance. They also lead or assist in incident-response efforts. Network administrators implement the policies, standards, and procedures in their day-to-day operational role.

Internally, networks can host or provide centralized access to mission-critical applications and information, making secure access an organizational priority. Externally, networks integrate institution and third-party applications that grant customers and insiders access to their financial information and Web-based services. Financial institutions that fail to restrict access properly expose themselves to increased operational, reputation, and legal risk from threats including the theft of customer information, data alteration, system misuse, or denial-of-service attacks.

Computer networks often extend connectivity far beyond the financial institution and its data center. Networks provide system access and connectivity between business units, affiliates, TSPs, business partners, customers, and the public. This increased connectivity requires additional controls to segregate and restrict access between various groups and information users.

An effective approach to securing a large network involves dividing the network into logical security domains. A logical security domain is a distinct part of a network with security policies that differ from other domains, and perimeter controls enforcing access at a network level. The differences may be far broader than network controls, encompassing personnel, host, and other issues.

Before establishing security domains, financial institutions should map and configure the network to identify and control all access points. Network configuration considerations could include the following actions:

- Identifying the various applications and systems accessed via the network,
- Identifying all access points to the network including various telecommunications channels (e.g., wireless, Ethernet, frame relay, dedicated lines, remote dial-up access, extranets, Internet),
- Mapping the internal and external connectivity between various network segments,
- Defining minimum access requirements for network services (i.e., most often referenced as a network services access policy), and
- Determining the most appropriate network configuration to ensure adequate security and performance.

With a clear understanding of network connectivity, the financial institution can avoid introducing security vulnerabilities by minimizing access to less-trusted domains and employing encryption for less secure connections. Institutions can then determine the most effective deployment of protocols, filtering routers, firewalls, gateways, proxy servers, and/or physical isolation to restrict access. Some applications and business processes may require complete segregation from the corporate network (e.g., no connectivity between corporate network and wire transfer system). Others may restrict access by placing the services that must be accessed by each zone in their own security domain, commonly called a DMZ.

Security domains are bounded by perimeters. Typical perimeter controls include firewalls that operate at different network layers, malicious code prevention, outbound filtering, intrusion detection and prevention devices, and controls over infrastructure services such as DNS. The perimeter controls may exist on separate devices or be combined or consolidated on one or more devices. Consolidation on a single device could improve security by reducing administrative overhead. However, consolidation may increase risk through a reduced ability to perform certain functions and the existence of a single point of failure.

Additionally, devices that combine prevention and detection present unique risks. Traditionally, if a prevention device fails, the detection device may alert on any resulting malicious activity. If the detection device fails, the prevention device still may function. If both functions are on the same device, and the device fails, the otherwise protected part of the institution's network may be exposed.

Firewalls

A firewallFor additional firewall explanations, see NIST Special Publication 800-41, "Guidelines on Firewalls and Firewall Policy." is a collection of components (computers, routers, and software) that mediate access between different security domains. All traffic between the security domains must pass through the firewall, regardless of the direction of the flow. Since the firewall serves as an access control point for traffic between security domains, they are ideally situated to inspect and block traffic and coordinate activities with network intrusion detection systems (IDSs).

Financial institutions have four primary firewall types from which to choose: packet filtering, stateful inspection, proxy servers, and application-level firewalls. Any product may have characteristics of one or more firewall types. The selection of firewall type is dependent on many characteristics of the security zone, such as the amount of traffic, the sensitivity of the systems and data, and applications. Additionally, consideration should be given to the ease of firewall administration, degree of firewall monitoring support through automated logging and log analysis, and the capability to provide alerts for abnormal activity.

Typically, firewalls block or allow traffic based on rules configured by the administrator. Rulesets can be static or dynamic. A static ruleset is an unchanging statement to be applied to packet header, such as blocking all incoming traffic with certain source addresses. A dynamic ruleset often is the result of coordinating a firewall and an IDS. For example, an IDS that alerts on malicious activity may send a message to the firewall to block the incoming IP address. The firewall, after ensuring the IP is not on a "white list"A whitelist contains the IP addresses that should always be allowed. Whitelists are important to guard against a denial of service resulting from an attacker using the IP of a service provider or other critical network connection., creates a rule to block the IP. After a specified period of time the rule expires and traffic is once again allowed from that IP.

Firewalls are subject to failure. When firewalls fail, they typically should fail closed, blocking all traffic, rather than failing open and allowing all traffic to pass.

Packet Filter Firewalls

Packet filter firewalls evaluate the headers of each incoming and outgoing packet to ensure it has a valid internal address, originates from a permitted external address, connects to an authorized protocol or service, and contains valid basic header instructions. If the packet does not match the pre-defined policy for allowed traffic, then the firewall drops the packet. Packet filters generally do not analyze the packet contents beyond the header information. Many routers contain access control lists (ACLs) that allow for packet-filtering capabilities.

Dynamic packet filtering incorporates stateful inspectionA technique that essentially verifies that inbound traffic is in response to requests initiated from inside the firewall. primarily for performance benefits. Before re-examining every packet, the firewall checks each packet as it arrives to determine whether it is part of an existing connection. If it verifies that the packet belongs to an established connection, then it forwards the packet without subjecting it to the firewall ruleset.

Weaknesses associated with packet filtering firewalls include the following:

- The system is unable to prevent attacks that exploit application-specific vulnerabilities and functions because the packet filter does not examine packet contents.
- Logging functionality is limited to the same information used to make access control decisions.

- Most do not support advanced user authentication schemes.
- Firewalls are generally vulnerable to attacks and exploitation that take advantage of vulnerabilities in network protocols.
- The firewalls are easy to misconfigure, which allows traffic to pass that should be blocked.

Packet filtering offers less security, but faster performance than application-level firewalls. The former are appropriate in high-speed environments where logging and user authentication with network resources are not as important. They also are useful in enforcing security zones at the network level. Packet filter firewalls are also commonly used in small office/home office (SOHO) systems and default operating system firewalls.

Institutions internally hosting Internet-accessible services should consider implementing additional firewall components that include application-level screening.

Stateful Inspection Firewalls

Stateful inspection firewalls are packet filters that monitor the state of the TCP connection. Each TCP session starts with an initial "handshake" communicated through TCP flags in the header information. When a connection is established the firewall adds the connection information to a table. The firewall can then compare future packets to the connection or state table. This essentially verifies that inbound traffic is in response to requests initiated from inside the firewall.

Proxy Server Firewalls

Proxy servers act as an intermediary between internal and external IP addresses and block direct access to the internal network. Essentially, they rewrite packet headers to substitute the IP of the proxy server for the IP of the internal machine and forward packets to and from the internal and external machines. Due to that limited capability, proxy servers are commonly employed behind other firewall devices. The primary firewall receives all traffic, determines which application is being targeted, and hands off the traffic to the appropriate proxy server. Common proxy servers are the domain name server (DNS), Web server (HTTP), and mail (SMTP) server. Proxy servers frequently cache requests and responses, providing potential performance benefits.

Additionally, proxy servers provide another layer of access control by segregating the flow of Internet traffic to support additional authentication and logging capability, as well as content filtering. Web and e-mail proxy servers, for example, are capable of filtering for potential malicious code and application-specific commands (see "Malicious Code"). They may implement anti-virus and anti-spam filtering, disallow connections to potentially malicious servers, and disallow the downloading of files in accordance with the institution's security policy.

Proxy servers are increasing in importance as protocols are tunneled through other protocols. For example, a protocol-aware proxy may be designed to allow Web server requests to port 80 of an external Web server, but disallow other protocols encapsulated in the port 80 requests.

Application-Level Firewalls

Application-level firewalls perform application-level screening, typically including the filtering capabilities of packet filter firewalls with additional validation of the packet content based on the application. Application-level firewalls capture and compare packets to state information in the connection tables. Unlike a packet filter firewall, an application-level firewall continues to examine each packet after the initial connection is established for specific application or services such as telnet, FTP, HTTP, SMTP, etc. The application-level firewall can provide additional screening of the packet payload for commands, protocols, packet length, authorization, content, or invalid headers. Application level firewalls provide the strongest level of security, but are slower

and require greater expertise to administer properly.

The primary disadvantages of application-level firewalls are as follows:

- The time required to read and interpret each packet slows network traffic. Traffic of certain types may have to be split off before the application-level firewall and passed through different access controls.
- Any particular firewall may provide only limited support for new network applications and protocols. They also simply may allow traffic from those applications and protocols to go through the firewall.

Firewall Services and Configuration

Firewalls may provide some additional services:

- Network address translation (NAT)-NAT readdresses outbound packets to mask the internal IP addresses of the network. Untrusted networks see a different host IP address from the actual internal address. NAT allows an institution to hide the topology and address schemes of its trusted network from untrusted networks.
- Dynamic host configuration protocol (DHCP)-DHCP assigns IP addresses to machines that will be subject to the security controls of the firewall.
- Virtual Private Network (VPN) gateways-A VPN gateway provides an encrypted tunnel between a remote external gateway and the internal network. Placing VPN capability on the firewall and the remote gateway protects information from disclosure between the gateways but not from the gateway to the terminating machines. Placement on the firewall, however, allows the firewall to inspect the traffic and perform access control, logging, and malicious code scanning.

One common firewall implementation in financial institutions hosting Internet applications is a DMZ, which is a neutral Internet accessible zone typically separated by two firewalls. One firewall is between the institution's private network and the DMZ and then another firewall is between the DMZ and the outside public network. The DMZ constitutes one logical security domain, the outside public network is another security domain, and the institution's internal network may be composed of one or more additional logical security domains. An adequate and effectively managed firewall can ensure that an institution's computer systems are not directly accessible to any on the Internet.

Firewall Policy

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. At a minimum, the policy should address

- Firewall topology and architecture,
- Type of firewall(s) being utilized,
- Physical placement of the firewall components,
- Monitoring firewall traffic,
- Permissible traffic (generally based on the premise that all traffic not expressly allowed is denied, detailing which applications can traverse the firewall and under what exact circumstances such activities can take place),

- Firewall updating,
- Coordination with security monitoring and intrusion response mechanisms,
- Responsibility for monitoring and enforcing the firewall policy,
- Protocols and applications permitted,
- Regular auditing of a firewall's configuration and testing of the firewall's effectiveness, and
- Contingency planning.

Financial institutions should also appropriately train, manage, and monitor their staffs to ensure the firewall policy is implemented properly. Alternatively, institutions can outsource the firewall management while ensuring that the outsourcer complies with the institution's specific firewall policy.

Firewalls are an essential control for a financial institution with an Internet connection and provide a means of protection against a variety of attacks. Firewalls should not be relied upon, however, to provide full protection from attacks. Institutions should complement firewalls with strong security policies and a range of other controls. In fact, firewalls are potentially vulnerable to attacks including

- Spoofing trusted IP addresses,
- Denial of service by overloading the firewall with excessive requests or malformed packets,
- Sniffing of data that is being transmitted outside the network,
- Hostile code embedded in legitimate HTTP, SMTP, or other traffic that meet all firewall rules,
- Attacks on unpatched vulnerabilities in the firewall hardware or software,
- Attacks through flaws in the firewall design providing relatively easy access to data or services residing on firewall or proxy servers, and
- Attacks against computers and communications used for remote administration.

Financial institutions can reduce their vulnerability to these attacks through network configuration and design, sound implementation of its firewall architecture that includes multiple filter points, active firewall monitoring and management, and integrated security monitoring. In many cases, additional access controls within the operating system or application will provide an additional means of defense.

Given the importance of firewalls as a means of access control, good practices include

- Hardening the firewall by removing all unnecessary services and appropriately patching, enhancing, and maintaining all software on the firewall unit (see "Systems Development, Acquisition, and Maintenance");
- Restricting network mapping capabilities through the firewall, primarily by blocking inbound ICMP (Internet Control Messaging Protocol) traffic;
- Using a ruleset that disallows all inbound and outbound traffic that is not specifically allowed;
- Using NAT and split DNS to hide internal system names and addresses from external networks (split DNS uses two domain name servers, one to communicate outside the network, and the other to offer services inside the network);
- Using proxy connections for outbound HTTP connections;
- Filtering malicious code;
- Backing up firewalls to internal media and not backing up the firewall to servers on protected networks;
- Logging activity, with daily administrator review (see "Logging and Data Collection");
- Using security monitoring devices and practices to monitor actions on the firewall and to monitor communications allowed through the firewall (see "Security Monitoring");
- Administering the firewall using encrypted communications and strong authentication,

accessing the firewall only from secure devices, and monitoring all administrative access;
- Limiting administrative access to few individuals; and
- Making changes only through well-administered change control procedures.

Malicious Code Filtering

Perimeters may contain proxy firewalls or other servers that act as a control point for Web browsing, e-mail, P2P, and other communications. Those firewalls and servers frequently are used to enforce the institution's security policy over incoming communications. Enforcement is through anti-virus, anti-spyware, and anti-spam filtering, the blocking of downloading of executable files, and other actions. To the extent that filtering is done on a signature basis, frequent updating of the signatures may be required.

Outbound Filtering

Perimeter servers also serve to inspect outbound communications for compliance with the institution's security policy. Perimeter routers and firewalls can be configured to enforce policies that forbid the origination of outbound communications from certain computers. Additionally, proxy servers could be configured to identify and block customer data and other data that should not be transmitted outside the security domain.

Network Intrusion Prevention Systems

Network Intrusion Prevention Systems (nIPS) are an access control mechanism that allow or disallow access based on an analysis of packet headers and packet payloads. They are similar to firewalls because they are located in the communications line, compare activity to preconfigured or preprogrammed decisions of what packets to pass or drop, and respond with pre-configured actions. The IPS units generally detect security events in a manner similar to IDS units (See "Activity Monitoring" in the Security Monitoring section of this booklet) and are subject to the same limitations. After detection, however, the IPS unit may take actions beyond simple alerting to potential malicious activity and logging of packets. For example, the IPS unit may block traffic flows from the offending host. The ability to sever communications can be useful when the activity can clearly be identified as malicious. When the activity cannot be clearly identified, for example where a false positive may exist, IDS-like alerting commonly is preferable to blocking.

Although IPS units are access control devices, many implement a security model that is different from firewalls. Firewalls typically allow only the traffic necessary for business purposes, or only "known good" traffic. IPS units typically are configured to disallow traffic that triggers signatures, or "known bad" traffic, while allowing all else. However, IPS units can be configured to more closely mimic a device that allows only "known good" traffic.

IPS units also contain a "white list" of IP addresses that should never be blocked. The list helps ensure that an attacker cannot achieve a denial of service by spoofing the IP of a critical host.

Quarantine

Quarantining a device protects the network from potentially malicious code or actions. Typically, a device connecting to a security domain is queried for conformance to the domain's security policy. If the device does not conform, it is placed in a restricted part of the network until it does conform. For example, if the patch level is not current, the device is not allowed into the security domain until the appropriate patches are downloaded and installed.

DNS Placement

Effective protection of the institution's DNS servers is critical to maintaining the security of the institution's communications. Much of the protection is provided by host security (See the "Systems Development, Acquisition, and Maintenance" section of this booklet). However, the placement of the DNS also is an important factor. The optimal placement is split DNS, where one firewalled DNS server serves public domain information to the outside and does not perform recursive queries, and a second DNS server, in an internal security domain and not the DMZ, performs recursive queries for internal users.

Wireless Issues

Wireless networks are difficult to secure because they do not have a well-defined perimeter or well-defined access points. Unlike wired networks, unauthorized monitoring and denial of service attacks can be performed without a physical wire connection. Additionally, unauthorized devices can potentially connect to the network, perform man-in-the-middle attacks, or connect to other wireless devices. To mitigate those risks, wireless networks rely on extensive use of encryption to authenticate users and devices and to shield communications. If a financial institution uses a wireless network, it should carefully evaluate the risk and implement appropriate additional controls. Examples of additional controls may include one or more of the following:

- Treating wireless networks as untrusted networks, allowing access through protective devices similar to those used to shield the internal network from the Internet environment;
- Using end-to-end encryption in addition to the encryption provided by the wireless connection;
- Using strong authentication and configuration controls at the access point and on all clients;
- Using an application server and dumb terminals;
- Shielding the area in which the wireless LAN operates to protect against stray emissions and signal interference; and
- Monitoring and responding to unauthorized wireless access points and clients.

Operating System Access

Action Summary

Financial institutions should secure access to the operating systems of all system components by

- Securing access to system utilities,
- Restricting and monitoring privileged access,
- Logging and monitoring user or program access to sensitive resources and alerting on security events,
- Updating the operating systems with security patches, and
- Securing the devices that can access the operating system through physical and logical means.

Financial institutions must control access to system software within the various network clients and servers as well as stand-alone systems. System software includes the operating system and system utilities. The computer operating system manages all of the other applications running on

the computer. Common operating systems include IBM zOS, OS/400, AIX, LINUX, various versions of Microsoft Windows, and Sun Solaris. Security administrators and IT auditors need to understand the common vulnerabilities and appropriate mitigation strategies for their operating systems. Application programs and data files interface through the operating system. System utilities are programs that perform repetitive functions such as creating, deleting, changing, or copying files. System utilities also could include numerous types of system management software that can supplement operating system functionality by supporting common system tasks such as security, system monitoring, or transaction processing.

System software can provide high-level access to data and data processing. Unauthorized access could result in significant financial and operational losses. Financial institutions should restrict privileged access to sensitive operating systems. While many operating systems have integrated access control software, third-party security software also is available. In the case of many mainframe systems, these programs are essential to ensure effective access control and can often integrate the security management of both the operating system and the applications. Network security software can allow institutions to improve the effectiveness of the administration and security policy compliance for a large number of servers often spanning multiple operating system environments. The critical aspects for access control software, whether included in the operating system or additional security software, are that management has the capability to

- Restrict access to sensitive or critical system resources or processes and have the capability, depending on the sensitivity, to extend protection at the program, file, record, or field level.
- Log user or program access to sensitive system resources including files, programs, processes, or operating system parameters.
- Filter logs for potential security events and provide adequate reporting and alerting capabilities.

Additional operating system access controls include the following actions:

- Ensure system administrators and security professionals have adequate expertise to securely configure and manage the operating system.
- Ensure effective authentication methods are used to restrict system access to both users and applications.
- Activate and utilize operating system security and logging capabilities and supplement with additional security software where supported by the risk assessment process.
- Restrict operating system access to specific terminals in physically secure and monitored locations.
- Lock or remove external drives from system consoles or terminals residing outside physically secure locations.
- Restrict and log access to system utilities, especially those with data altering capabilities.
- Restrict access to operating system parameters.
- Prohibit remote access to sensitive operating system functions, where feasible, and at a minimum require strong authentication and encrypted sessions before allowing remote support.
- Limit the number of employees with access to sensitive operating systems and grant only the minimum level of access required to perform routine responsibilities.
- Segregate operating system access, where possible, to limit full or root-level access to the system.
- Monitor operating system access by user, terminal, date, and time of access.
- Update operating systems with security patches and using appropriate change control mechanisms. (See "Systems Development, Acquisition, and Maintenance.")

Application Access

Action Summary

Financial institutions should control access to applications by

- Using authentication and authorization controls appropriately robust for the risk of the application,
- Monitoring access rights to ensure they are the minimum required for the user's current business needs,
- Using time-of-day limitations on access as appropriate,
- Logging access and security events, and
- Using software that enables rapid analysis of user activities.

Sensitive or mission-critical applications should incorporate appropriate access controls that restrict which application functions are available to users and other applications. The most commonly referenced applications from an examination perspective support the information processing needs of the various business lines. These computer applications allow authorized users or other applications to interface with the related database. Effective application access control can enforce both segregation of duties and dual control. Access rights to sensitive or critical applications and their databases should ensure that employees or applications have the minimum level of access required to perform their business functions. Effective application access control involves a partnership between the security administrators, the application programmers (including TSPs and vendors), and the business owners.

Some security software programs will integrate access control for the operating system and some applications. Such software is useful when applications do not have their own access controls, and when the institution wants to rely on the security software instead of the application's access controls. Examples of such security software products for mainframe computers include RACF, CA-ACF2, and CA-TopSecret. Institutions should understand the functionality and vulnerabilities of their application access control solutions and consider those issues in their risk assessment process.

Institution management should consider a number of issues regarding application access control. Many of these issues also could apply to oversight of operating system access:

- Implementing a robust authentication method consistent with the criticality and sensitivity of the application. Historically, the majority of applications have relied solely on user IDs and passwords, but increasingly applications are using other forms of authentication. Multi-factor authentication, such as token and PKI-based systems coupled with a robust enrollment process, can reduce the potential for unauthorized access.
- Maintaining consistent processes for assigning new user access, changing existing user access, and promptly removing access to departing employees.
- Communicating and enforcing the responsibilities of programmers (including TSPs and vendors), security administrators, and business line owners for maintaining effective application-access control. Business line managers are responsible for the security and privacy of the information within their units. They are in the best position to judge the legitimate access needs of their area and should be held accountable for doing so. However, they require support in the form of adequate security capabilities provided by the programmers or vendor and adequate direction and support from security administrators.

- Monitoring existing access rights to applications to help ensure that users have the minimum access required for the current business need. Typically, business application owners must assume responsibility for determining the access rights assigned to their staff within the bounds of the AUP. Regardless of the process for assigning access, business application owners should periodically review and approve the application access assigned to their staff.
- Setting time-of-day or terminal limitations for some applications or for the more sensitive functions within an application. The nature of some applications requires limiting the location and number of workstations with access. These restrictions can support the implementation of tighter physical access controls.
- Logging access and events (see "Log Transmission, Normalization, Storage, and Protection" in the Activity Monitoring section of this booklet).
- Easing the administrative burden of managing access rights by utilizing software that supports group profiles. Some financial institutions manage access rights individually and this approach often leads to inappropriate access levels. By grouping employees with similar access requirements under a common access profile (e.g., tellers, loan operations, etc.), business application owners and security administrators can better assign and oversee access rights. For example, a teller performing a two-week rotation as a proof operator does not need year-round access to perform both jobs. With group profiles, security administrators can quickly reassign the employee from a teller profile to a proof operator profile. Note that group profiles are used only to manage access rights; accountability for system use is maintained through individuals being assigned their own unique identifiers and authenticators.

Remote Access

Action Summary

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.

Many financial institutions provide employees, vendors, and others with access to the institution's network and computing resources through external connections. Those connections are typically established through modems, the Internet, or private communications lines. The access may be necessary to remotely support the institution's systems or to support institution operations at remote locations. In some cases, remote access is required periodically by vendors to make emergency program fixes or to support a system.

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:

- 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.
- Appropriately secure remote access devices against malware (see "Malicious Code Prevention").
- Appropriately and in a timely manner patch, update, and maintain all software on remote access devices.
- Use encryption to protect communications between the access device and the institution and to protect sensitive data residing on the access device.
- Periodically audit the access device configurations and patch levels.
- Use VLANs, network segments, directories, and other techniques to restrict remote access to authorized network areas and applications within the institution.
- Log remote access communications, analyze them in a timely manner, and follow up on anomalies.
- Centralize modem and Internet access to provide a consistent authentication process, and to subject the inbound and outbound network traffic to appropriate perimeter protections and network monitoring.
- Log and monitor the date, time, user, user location, duration, and purpose for all remote access.
- Require a two-factor authentication process for remote access (e.g., PIN-based token card with a one-time random password generator, or token-based PKI).
- Implement controls consistent with the sensitivity of remote use. For example, remote use to administer sensitive systems or databases may include the following controls:
  - Restrict the use of the access device by policy and configuration;
  - Require two-factor user authentication;
  - Require authentication of the access device;
  - Ascertain the trustworthiness of the access device before granting access;
  - Log and review all activities (e.g. keystrokes).
- If remote access is through modems:
  - Require an operator to leave the modems unplugged or disabled by default, to enable modems only for specific and authorized external requests, and disable the modem immediately when the requested purpose is completed.
  - Configure modems not to answer inbound calls, if modems are for outbound use only.
  - Use automated callback features so the modems only call one number (although this is subject to call forwarding schemes).
  - Install a modem bank where the outside number to the modems uses a different prefix than internal numbers and does not respond to incoming calls.

Physical And Environmental Protection

Action Summary

Financial institutions should define physical security zones and implement appropriate preventative and detective controls in each zone to protect against the risks of

- Physical penetration by malicious or unauthorized people,
- Damage from environmental contaminants, and
- Electronic penetration through active or passive electronic emissions.

The confidentiality, integrity, and availability of information can be impaired through physical access and damage or destruction to physical components. Conceptually, those physical security risks are mitigated through zone-oriented implementations. Zones are physical areas with differing physical security requirements. The security requirements of each zone are a function of the sensitivity of the data contained or accessible through the zone and the information technology components in the zone. For instance, data centers may be in the highest security zone, and branches may be in a much lower security zone. Different security zones can exist within the same structure. Routers and servers in a branch, for instance, may be protected to a greater degree than customer service terminals. Computers and telecommunications equipment within an operations center will have a higher security zone than I/O operations, with the media used by that equipment stored at yet a higher zone.

The requirements for each zone should be determined through the risk assessment. The risk assessment should include, but is not limited to, the following threats:

- Aircraft crashes
- Chemical effects
- Dust
- Electrical supply interference
- Electromagnetic radiation
- Explosives
- Fire
- Smoke
- Theft/Destruction
- Vibration/Earthquake
- Water
- Criminals
- Terrorism
- Political issues (e.g. strikes, disruptions)
- Any other threats applicable based on the entity's unique geographical location, building configuration, neighboring entities, etc.

Data Center Security

When selecting a site for the most important information systems components, one major objective is to limit the risk of exposure from internal and external sources. The selection process should include a review of the surrounding area to determine if it is relatively safe from exposure to fire, flood, explosion, or similar environmental hazards. Outside intruders can be deterred through the use of guards, fences, barriers, surveillance equipment, or other similar devices. Since access to key information system hardware and software should be limited, doors and windows must be secure. Additionally, the location should not be identified or advertised by signage or other indicators.

Detection devices, where applicable, should be utilized to prevent theft and safeguard the equipment. They should provide continuous coverage. Detection devices have two purposes- to alarm when a response is necessary and to support subsequent forensics. The alarm capability is useful only when a response will occur.

Some intruder detection devices available include

- Switches that activate an alarm when an electrical circuit is broken;
- Light and laser beams, ultraviolet beams and sound or vibration detectors that are invisible to the intruder, and ultrasonic and radar devices that detect movement in a room; and
- Closed-circuit television that allows visual observation and recording of actions.

Risks from environmental threats can be addressed through devices such as halon gas and halon replacements, smoke alarms, raised flooring, and heat sensors.

Physical security devices frequently need preventive maintenance to function properly. Maintenance logs are one control the institution can use to determine whether the devices are appropriately maintained. Periodic testing of the devices provides assurance that they are operating correctly.

Security guards should be properly instructed about their duties. The employees who acces secured areas should have proper identification and authorization to enter the area. All visitors should sign in and wear proper IDs so that they can be identified easily. Security guards should be trained to restrict the removal of assets from the premises and to record the identity of anyone removing assets. Consideration should be given to implementing a specific and formal authorization process for the removal of hardware and software from premises.

The following security zones should have access restricted to a need basis:

- Operations center
- Uninterrupted power supply
- Telecommunications equipment
- Media library

Cabinet and Vault Security

Protective containers are designed to meet either fire-resistant or burglar-resistant standards. Labels describing expected tolerance levels are usually attached to safes and vault doors. An institution should select the tolerance level based on the sensitivity and importance of the information being protected.

Physical Security in Distributed IT Environments

Hardware and software located in a user department are often less secure than that located in a computer room. Distributed hardware and software environments (e.g., local area networks or LANs) that offer a full range of applications for small financial institutions as well as larger organizations are commonly housed throughout the organization, without special environmental controls or raised flooring. In such situations, physical security precautions are often less sophisticated than those found in large data centers, and overall building security becomes more

important. Internal control procedures are necessary for all hardware and software deployed in distributed, and less secure, environments. The level of security surrounding any hardware and software should depend on the sensitivity of the data that can be accessed, the significance of applications processed, the cost of the equipment, and the availability of backup equipment.

Because of their portability and location in distributed environments, personal computers (PCs) often are prime targets for theft and misuse. The location of PCs and the sensitivity of the data and systems they access determine the extent of physical security required. For PCs in unrestricted areas such as a branch lobby, a counter or divider may provide the only barrier to public access. In these cases, institutions should consider securing PCs to workstations, locking or removing disk drives and unnecessary physical ports, and using screensaver passwords or automatic timeouts. Employees also should have only the access to PCs and data they need to perform their job. The sensitivity of the data processed or accessed by the computer usually dictates the level of control required. The effectiveness of security measures depends on employee awareness and enforcement of these controls.

An advantage of PCs is that they can operate in an office environment, providing flexible and informal operations. However, as with larger systems, PCs are sensitive to environ mental factors such as smoke, dust, heat, humidity, food particles, and liquids. Because they are not usually located within a secure area, policies should be adapted to provide protection from ordinary contaminants.

Other environmental problems to guard against include electrical power surges and static electricity. The electrical power supply in an office environment is sufficient for a PC's requirements. However, periodic fluctuations in power (surges) can cause equipment damage or loss of data. PCs in environments that generate static electricity are susceptible to static electrical discharges that can cause damage to PC components or memory.

Physical security for distributed IT, particularly LANs that are usually PC-based, is slightly different than for mainframe platforms. With a network there is often no centralized computer room. In addition, a network often extends beyond the local premises. There are certain components that need physical security. These include the hardware devices and the software and data that may be stored on the file servers, PCs, or removable media (tapes and disks). As with more secure IT environments, physical network security should prevent unauthorized personnel from accessing LAN devices or the transmission of data. In the case of wire-transfer clients, more extensive physical security is required.

Physical protection for networks as well as PCs includes power protection, physical locks, and secure work areas enforced by security guards and authentication technologies such as magnetic badge readers. Physical access to the network components (i.e., files, applications, communications, etc.) should be limited to those who require access to perform their jobs. Network workstations or PCs should be password protected and monitored for workstation activity.

Network wiring requires some form of protection since it does not have to be physically penetrated for the data it carries to be revealed or contaminated. Examples of controls include using a conduit to encase the wiring, avoiding routing through publicly accessible areas, and avoiding routing networking cables in close proximity to power cables. The type of wiring can also provide a degree of protection; signals over fiber, for instance, are less susceptible to interception than signals over copper cable.

Network security also can be compromised through the capture of radio frequency emissions. Frequency emissions are of two types, intentional and unintentional. Intentional emissions are those broadcast, for instance, by a wireless network. Unintentional emissions are the normally

occurring radiation from monitors, keyboards, disk drives, and other devices. Shielding is a primary control over emissions. The goal of shielding is to confine a signal to a defined area. An example of shielding is the use of foil-backed wallboard and window treatments. Once a signal is confined to a defined area, additional controls can be implemented in that area to further minimize the risk that the signal will be intercepted or changed.

Encryption

Action Summary

Financial institutions should employ encryption to mitigate the risk of disclosure or alteration of sensitive information in storage and transit.

- Encryption implementations should include Encryption strength sufficient to protect the information from disclosure until such time as disclosure poses no material risk,
- Effective key management practices,
- Robust reliability, and
- Appropriate protection of the encrypted communication's endpoints.

Encryption is used to secure communications and data storage, particularly authentication credentials and the transmission of sensitive information. It can be used throughout a technological environment, including the operating systems, middleware, applications, file systems, and communications protocols.

Encryption can be used as a preventive control, a detective control, or both. As a prevention control, encryption acts to protect data from disclosure to unauthorized parties. As a detective control, encryption is used to allow discovery of unauthorized changes to data and to assign responsibility for data among authorized parties. When prevention and detection are joined, encryption is a key control in ensuring confidentiality, data integrity, and accountability.

Properly used, encryption can strengthen the security of an institution's systems. Encryption also has the potential, however, to weaken other security aspects. For instance, encrypted data drastically lessens the effectiveness of any security mechanism that relies on inspections of the data, such as anti-virus scanning and intrusion detection systems. When encrypted communications are used, networks may have to be reconfigured to allow for adequate detection of malicious code and system intrusions.

Although necessary, encryption carries the risk of making data unavailable should anything go wrong with data handling, key management, or the actual encryption. For example, a loss of encryption keys or other failures in the encryption process can deny the institution access to the encrypted data. The products used and administrative controls should contain robust and effective controls to ensure reliability.

Financial institutions should employ an encryption strength sufficient to protect information from disclosure until such time as the information's disclosure poses no material threat. For instance, authenticators should be encrypted at a strength sufficient to allow the institution time to detect and react to an authenticator theft before the attacker can decrypt the stolen authenticators.

Decisions regarding what data to encrypt and at what points to encrypt the data are typically based on the risk of disclosure and the costs and risks of encryption. The costs include potentially significant overhead costs on hosts and networks. Generally speaking, authenticators are encrypted whether on public networks or on the financial institution's network. Sensitive information is also encrypted when passing over a public network and also may be encrypted within the institution.

Encryption cannot guarantee data security. Even if encryption is properly implemented, for example, a security breach at one of the endpoints of the communication can be used to steal the data or allow an intruder to masquerade as a legitimate system user.

How Encryption Works

In general, encryption functions by taking data and a variable, called a "key" and processing those items through a fixed algorithm to create the encrypted text. The strength of the encrypted text is determined by the entropy, or degree of uncertainty, in the key and the algorithm. Key length and key selection criteria are important determinants of entropy. Greater key lengths generally indicate more possible keys. More important than key length, however, is the potential limitation of possible keys posed by the key selection criteria. For instance, a 128-bit key has much less than 128 bits of entropy if it is selected from only certain letters or numbers. The full 128 bits of entropy will only be realized if the key is randomly selected across the entire 128-bit range.

The encryption algorithm is also important. Creating a mathematical algorithm that does not limit the entropy of the key and testing the algorithm to ensure its integrity are difficult. Since the strength of an algorithm is related to its ability to maximize entropy instead of its secrecy, algorithms are generally made public and subject to peer review. The more that the algorithm is tested by knowledgeable worldwide experts, the more the algorithm can be trusted to perform as expected. Examples of public algorithms are AES, DES and Triple DES, HSA-1, and RSA.

Encryption Key Management

Since security is primarily based on the encryption keys, effective key management is crucial. Effective key management systems are based on an agreed set of standards, procedures, and secure methods that addressSource: ISO 17799, 10.3.5.2

- Generating keys for different cryptographic systems and different applications;
- Generating and obtaining public keys;
- Distributing keys to intended users, including how keys should be activated when received;
- Storing keys, including how authorized users obtain access to keys;
- Changing or updating keys, including rules on when keys should be changed and how this will be done;
- Dealing with compromised keys;
- Revoking keys and specifying how keys should be withdrawn or deactivated;
- Recovering keys that are lost or corrupted as part of business continuity management;
- Archiving keys;
- Destroying keys;
- Logging the auditing of key management-related activities; and
- Instituting defined activation and deactivation dates, limiting the usage period of keys.

Secure key management systems are characterized by the following precautions:

- Key management is fully automated (e.g., personnel do not have the opportunity to expose a key or influence the key creation).
- No key ever appears unencrypted.
- Keys are randomly chosen from the entire key space, preferably by hardware.
- Key-encrypting keys are separate from data keys. No data ever appears in clear text that was encrypted using a key-encrypting key. (A key-encrypting key is used to encrypt other keys, securing them from disclosure.)
- All patterns in clear text are disguised before encrypting.
- Keys with a long life are sparsely used. The more a key is used, the greater the opportunity for an attacker to discover the key.
- Keys are changed frequently. The cost of changing keys rises linearly while the cost of attacking the keys rises exponentially. Therefore, all other factors being equal, changing keys increases the effective key length of an algorithm.
- Keys that are transmitted are sent securely to well-authenticated parties.
- Key-generating equipment is physically and logically secure from construction through receipt, installation, operation, and removal from service.

Encryption Types

Three types of encryption exist: the cryptographic hash, symmetric encryption, and asymmetric encryption.

A cryptographic hash reduces a variable-length input to a fixed-length output. The fixed-length output is a unique cryptographic representation of the input. Hashes are used to verify file and message integrity. For instance, if hashes are obtained from key operating system binaries when the system is first installed, the hashes can be compared to subsequently obtained hashes to determine if any binaries were changed. Hashes are also used to protect passwords from disclosure. A hash, by definition, is a one-way encryption. An attacker who obtains the password cannot run the hash through an algorithm to decrypt the password. However, the attacker can perform a dictionary attack, feeding all possible password combinations through the algorithm and look for matching hashes, thereby deducing the password. To protect against that attack, "salt," or additional bits, are added to the password before encryption. The addition of the bits means the attacker must increase the dictionary to include all possible additional bits, thereby increasing the difficulty of the attack.

Symmetric encryption is the use of the same key and algorithm by the creator and reader of a file or message. The creator uses the key and algorithm to encrypt, and the reader uses both to decrypt. Symmetric encryption relies on the secrecy of the key. If the key is captured by an attacker, either when it is exchanged between the communicating parties, or while one of the parties uses or stores the key, the attacker can use the key and the algorithm to decrypt messages or to masquerade as a message creator.

Asymmetric encryption lessens the risk of key exposure by using two mathematically related keys, the private key and the public key. When one key is used to encrypt, only the other key can decrypt. Therefore, only one key (the private key) must be kept secret. The key that is exchanged (the public key) poses no risk if it becomes known. For instance, if individual A has a private key and publishes the public key, individual B can obtain the public key, encrypt a message to individual A, and send it. As long as individual A keeps his private key secure from discovery, only individual A will be able to decrypt the message.

Examples of Encryption Uses

Asymmetric encryption is the basis of public key infrastructure. In theory, PKI allows two parties who do not know each other to authenticate each other and maintain the confidentiality, integrity, and accountability for their messages. PKI rests on both communicating parties having a public and a private key, and keeping their public keys registered with a third party they both trust, called the certificate authority, or CA. The use of and trust in the third party is a key element in the authentication that takes place. For example, assume individual A wants to communicate with individual B. A first hashes the message, and encrypts the hash with A's private key. Then A obtains B's public key from the CA and encrypts the message and the hash with B's public key. Obtaining B's public key from the trusted CA provides A assurance that the public key really belongs to B and not someone else. Using B's public key ensures that the message will only be able to be read by B. When B receives the message, the process is reversed. B decrypts the message and hash with B's private key, obtains A's public key from the trusted CA, and decrypts the hash again using A's public key. At that point, B has the plain text of the message and the hash performed by A. To determine whether the message was changed in transit, B must re-perform the hashing of the message and compare the newly computed hash to the one sent by A. If the new hash is the same as the one sent by A, B knows that the message was not changed since the original hash was created (integrity). Since B obtained A's public key from the trusted CA and that key produced a matching hash, B is assured that the message came from A and not someone else (authentication).

Various communication protocols use both symmetric and asymmetric encryption. Transaction layer security (TLS), the successor to Secure Socket Layer (SSL) uses asymmetric encryption for authentication, and symmetric encryption to protect the remainder of the communications session. TLS can be used to secure electronic banking and other transmissions between the institution and the customer. TLS may also be used to secure e-mail, telnet, and FTP sessions. A wireless version of TLS is called WTLS, for wireless transaction layer security.

IPSec is a complex aggregation of protocols that together provide authentication and confidentiality services to individual IP packets. It can be used to create a VPN over the Internet or other untrusted network, or between any two computers on a trusted network. Since IPSec has many configuration options, and can provide authentication and encryption using different protocols, implementations between vendors and products may differ.

SSL and TLS are frequently used to establish encrypted tunnels between the financial institution and Internet banking users. They are also used to provide a different type of VPN than that provided by IPSec.

Secure Shell (SSH) is frequently used for remote server administration. SSH establishes an encrypted tunnel between a SSH client and a server, as well as authentication services.

Encryption may also be used to protect data in storage. The implementation may encrypt a file, a directory, a volume, or a disk.

Malicious Code Prevention

Action Summary

Financial institutions should protect against the risk of malicious code by implementing appropriate controls at the host and network level to prevent and detect malicious code, as well as engage in appropriate user education.

Malicious code is any program that acts in unexpected and potentially damaging ways. Common types of malicious code are viruses, worms, Trojan horses, monitoring programs such as spyware, and cross-site scripts. The functions of each were once mutually exclusive; however, developers combined functions to create more powerful malicious code. Malicious code can

- Replicate itself within a computer and transmit itself between computers.
- Change, delete, or insert data, transmit data outside the institution, and insert backdoors into institution systems.
- Attack institutions at either the server or the client level.
- Attack routers, switches, and other parts of the institution infrastructure.

Malicious code can also monitor users in many ways, such as logging keystrokes and transmitting screenshots to the attacker.

Typically malicious code is mobile, using e-mail, Instant Messenger, and other peer-to-peer (P2P) applications, or active content attached to Web pages as transmission mechanisms. The code also can be hidden in programs that are downloaded from the Internet or brought into the institution on diskette. At times, the malicious code can be created on the institution's systems either by intruders or by authorized users. The code can also be introduced to a Web server in numerous ways, such as entering the code in a response form on a Web page.

Malicious code does not have to be targeted at the institution to damage the institution's systems or steal the institution's data. Most malicious code is general in application, potentially affecting all Internet users with whatever operating system or application the code needs to function.

Controls to Protect Against Malicious Code

Typical controls to protect against malicious code use technology, policies and procedures, and training, all applied in a layered manner from perimeters inward to hosts and data. The controls are of the preventative and detective/corrective variety. Controls are applied at the host, network, and user levels:

Host Level

- Host hardening, including patch application and security-minded configurations of the operating system (OS), browsers, and other network-aware software.
- Host IPS, including anti-virus, anti-spyware, and anti-rootkitRootkits can enable the hiding and surreptitious execution of malicious code. software. An additional technology is software that limits applications calls to the OS to the minimum necessary for the application to function.
- Integrity checking software, combined with strict change controls and configuration management.
- Application of known-good configurations at boot-up.
- Periodic auditing of host configurations, both manual and automated.

Network Level

- Limiting the transfer of executable files through the perimeter.
- IDS and IPS monitoring of incoming and outgoing network traffic, including anti-virus, anti-spyware and signature and anomaly-based traffic monitors.
- Routing ACLs that limit incoming and outgoing connections as well as internal connections to those necessary for business purposes.
- Proxy servers that inspect incoming and outgoing packets for indicators of malicious code and block access to known or suspected malware distribution servers.
- Filtering to protect against attacks such as cross-site scripting and SQL injection.

User Level

- User education in awareness, safe computing practices, indicators of malicious code, and response actions.

Systems Development, Acquisition, and Maintenance

Action Summary

Financial institutions should ensure that systems are developed, acquired, and maintained with appropriate security controls. The steps include

- Ensuring that systems are developed and implemented with appropriate security features enabled;
- Ensuring that software is trustworthy by implementing appropriate controls in the development process, reviewing source code, reviewing the history and reputation of vendors and third party developers, and implementing appropriate controls outside of the software to mitigate the unacceptable risks from any deficiencies;
- Maintaining appropriately robust configuration management and change control processes; and
- Establishing an effective patch process.

Software is the most important building block in a financial institution's technology infrastructure. Software should provide the security controls required by the institution, be protected from inappropriate use, and be maintained at a required level of trustworthiness.

Software Development and Acquisition

Financial institutions obtain software through self-development, contracted development, the purchase of pre-written code, or variations of those development and acquisition approaches. The security issues associated with the approaches involve the security controls built into the code and the trustworthiness of the code that is placed into the financial institution's environment. The security features of the code can be assessed regardless of the means of development or acquisition. The trustworthiness of the code, however, is ascertained differently depending on the

availability of information necessary to perform an assessment.

Test data consisting of institution data or customer data frequently is used in development tests or certifications. Appropriate risk mitigation techniques should be employed to protect that data from unauthorized disclosure. As a general principal, the risk of disclosure should be no greater than in the production environment. Techniques to achieve that goal can include altering the data so it is no longer identified with a customer and performing the test in an environment whose controls are as strong as those employed in the production environment.

Security Control Requirements

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.See http://www.commoncriteriaportal.org 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.

Development projects should consider automated controls for incorporation into the application and the need to determine supporting manual controls. Financial institutions can implement appropriate security controls with greater cost effectiveness by designing them into the original software rather than making subsequent changes after implementation.

The institution's development, acquisition, and audit policies should include guidelines describing the involvement of internal audit in development or acquisition activities as a means of independently verifying the adequacy of the security requirements as they are developed and implemented. For more information, refer to the "Development and Acquisition" and "Audit" booklets in the FFIEC IT Examination Handbook.

Development environments should be appropriately secured as a part of the overall institution environment. Appropriate security generally is a function of the risks of information exposure and the risks that unexpected capabilities will be incorporated into projects delivered to the production environment. Monitoring of the development environment can assist in assuring that the implemented controls are functioning properly.

Security Controls in Application Software

Application development should incorporate appropriate security controls, audit trails, and activity logs. Typical application access controls are addressed in earlier sections. Application security controls should also include validation controls for data entry and data processing. Data entry validation controls include access controls over entry and changes to data, error checks, review of suspicious or unusual data, and dual entry or additional review and authorization for highly sensitive transactions or data. Data processing controls include batch control totals, hash totals of data for comparison after processing, identification of any changes made to data outside the application (e.g., data-altering utilities), and job control checks to ensure programs run in correct sequence (see the "Operations" booklet in the FFIEC IT Examination Handbook for additional considerations).

Some applications will require the integration of additional authentication and encryption controls to ensure integrity and confidentiality of the data. As customers and merchants originate an increasing number of transactions, authentication and encryption become increasingly important to ensure non-repudiation of transactions.

Remote access to applications by customers and others increases risks. Steps to mitigate those risks include network, host, and application layer architecture considerations. Network and host controls are necessary to mitigate the risk from potential flaws in applications. Software trustworthiness is an important component in that consideration. Additionally, ongoing risk assessments should consider the adequacy of application level controls in light of changing threat, network, and host environments.

Software Trustworthiness

Software can contain erroneous or intentional code that introduces covert channels, backdoors, and other security risks into systems and applications. These hidden access points can provide unauthorized access to systems or data, unauthorized communications capabilities, and unauthorized abilities to change the software. Because those unauthorized abilities can circumvent the financial institution's control structure, financial institutions should assess the trustworthiness of the software in their environments and implement appropriate controls to mitigate any unacceptable risk. The additional controls can exist at various levels, including the network, host, and application layers.

Assessment of both self-developed and purchased software should consider the development process, the source code, and the history and reputation of the developers or vendors. Generally speaking, software whose development process and source is available to the institution can be more effectively evaluated than other software.

Development Process

The development process provides important indicators of code trustworthiness. The primary indicators are the extent to which security is incorporated within development and personnel processes, and the level of process maturity. Specific features include:

- Establishment of security requirements, considering the current and expected threat, network, and host environments;
- Establishment of functional requirements and acceptance criteria;
- Use of secure coding standards;
- Tests and reviews for compliance with security requirements;
- Background checks on employees and code development and testing processes;
- Signed nondisclosure agreements to protect the financial institution's rights to source code and customer data as appropriate;
- Restrictions on developer write-access to production source code and systems, and monitoring developer access to development systems; and,
- Physical security over developer work areas, including restrictions on media taken to and from the work area.

Process maturity is an important indicator because mature processes result in a more controlled code development. For a greater discussion of development processes, see the "Development and Acquisition" booklet in the FFIEC IT Examination Handbook.

Source Code Review

Source code also provides indicators of code trustworthiness. Code that has been subjected to

independent security reviews is generally more trustworthy than code that has not. Source code reviews can be automated or manual. Automated reviews typically look for common coding errors that could have security implications, but can lack the detail of a manual review. Manual reviews can be more detailed but may be unreliable due to the tedious nature of the task and the varying capabilities of the reviewers. Taken together, both automated and manual code review can mitigate some risk from coding errors. However, source code reviews cannot protect against the introduction of unexpected and unauthorized capabilities in the compiling or other manipulation of code.

History and Reputation

Financial institutions that purchase pre-written software are frequently not provided the opportunity to evaluate the development process or the source code of the software they introduce into their environment. In such situations, the institutions rely on the proxy of vendor history and reputation. History and reputation are also important when code is developed by the institution's employees. Important indicators include:

Vulnerability history of other software from the same source, including earlier versions of the software under consideration by the financial institution;
Timeliness, thoroughness, and candidness of the response to security issues; and
Quality and functionality of the corrective security patches.
Assessment Follow-up Actions
Should the assessment indicate the software is not sufficiently trustworthy to be implemented in the current environment, additional controls may be implemented at the host or network level. Those controls generally limit access to the software and the host, limit the software's access to other host and network resources, monitor the software's actions on the host, or monitor network communications.

Systems Maintenance

Financial institutions that introduce trustworthy systems into their environment should ensure that the systems retain that trustworthiness over time.

Essential control elements are the development of appropriately hardened systems, usage of standard builds, the appropriate updating of builds and deployed systems through patch management, and the controlled introduction of changes into the institution's environment.

Hardening
Financial institutions use commercial off-the-shelf (COTS) software for operating systems and applications. COTS systems generally provide more functions than are required for the specific purposes for which they are employed. For example, a default installation of a server operating system may install mail, Web, and file-sharing services on a system whose sole function is a DNS server. Unnecessary software and services represent a potential security weakness. Their presence increases the potential number of discovered and undiscovered vulnerabilities present in the system. Additionally, system administrators may not install patches or monitor the unused software and services to the same degree as operational software and services. Protection against those risks begins when the systems are constructed and software installed through a process that is referred to as hardening a system.

When deploying off-the-shelf software, management should harden the resulting system. Hardening includes the following actions:

- Determining the purpose of the system and minimum software and hardware requirements;
- Documenting the minimum hardware, software, and services to be included on the system;
- Installing the minimum hardware, software, and services necessary to meet the requirements using a documented installation procedure;
- Installing necessary patches;
- Installing the most secure and up-to-date versions of applications;
- Configuring privilege and access controls by first denying all, then granting back the minimum necessary to each user;
- Configuring security settings as appropriate, enabling allowed activity, and disallowing other activity;
- Enabling logging;
- Creating cryptographic hashes of key files;
- Archiving the configuration and checksums in secure storage prior to system deployment;
- Testing the system to ensure a secure configuration;
- Using secure replication procedures for additional, identically configured systems, making configuration changes on a case-by-case basis;
- Changing all default passwords; and
- Testing the resulting systems.

After deployment, COTS systems may need updating with current security patches. Additionally, the systems should be periodically audited to ensure that the software present on the systems is authorized and properly configured.

Standard Builds

Consistency in system configuration makes security easier to implement and maintain. Standard builds allow one documented configuration to be applied to multiple computers in a controlled manner. One financial institution may have many standard builds.

Through the use of standard builds, an institution simplifies

- Hardware and software inventories
- Updating and patching systems
- Restoring systems in the event of a disaster or outage
- Investigating anomalous activity
- Auditing configurations for conformance with the approved configuration.

An institution may not be able to meet all of its requirements from its standard builds. The use of a non-standard build is typically documented and approved, with appropriate changes made to patch management and disaster recovery plans.

Patch Management

Software support should incorporate a process to update and patch operating system and application software for new vulnerabilities. Frequently, security vulnerabilities are discovered in operating systems and other software after deployment. Vendors often issue software patches to correct those vulnerabilities. Financial institutions should have an effective monitoring process to identify new vulnerabilities in their hardware and software. Monitoring involves such actions as the receipt and analysis of vendor and governmental alerts and security mailing lists. Once identified, secure installation of those patches requires a process for obtaining, testing, and installing the patch.

All patches are not equally important. Financial institutions should have a process to evaluate the patches against the threat and network environment and to prioritize patch application across classes of computers. Should the institution decide not to apply an otherwise important patch to any particular computer, the decision should be documented with appropriate conforming changes

made to inventory records and disaster recovery plans.

Patches make direct changes to the software and configuration of each system to which they are applied. They may degrade system performance, introduce new vulnerabilities, or reintroduce old vulnerabilities. The following actions can help ensure patches do not compromise the security of systems:

- Obtain the patch from a known, trusted source
- Verify the integrity of the patch through such means as comparisons of cryptographic hashes to ensure the patch obtained is the correct, unaltered patch
- Apply the patch to an isolated test system and verify that the patch (1) is compatible with other software used on systems to which the patch will be applied, (2) does not alter the system's security posture in unexpected ways, such as altering log settings, and (3) corrects the pertinent vulnerability
- Plan the patch roll-out to appropriately mitigate the risks to changing systems and address non-standard systems or systems with unique configuration considerations
- Use the change control process to update production systems:
  - Back up production systems prior to applying the patch
  - Apply the patch to production systems using secure methods, and update the cryptographic checksums of key files as well as that system's software archive
  - Test the resulting system for known vulnerabilities
- Update standard builds
- Create and document an audit trail of all changes
- Seek additional expertise as necessary to maintain a secure computing environment

Controlled Changes to the Environment
Financial institutions should have an effective process to introduce application and system changes into their environments. The process should encompass developing, implementing, and testing changes to both internally developed software and acquired software. Weak procedures can corrupt applications and introduce new security vulnerabilities. Control considerations relating to security include the following:

- Restricting changes to authorized users;
- Reviewing the impact changes will have on security controls;
- Identifying all system components that are affected by the changes;
- Ensuring the application or system owner has authorized changes in advance;
- Maintaining strict version control of all software updates; and
- Maintaining an audit trail of all changes

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.

Personnel Security

Action Summary

Financial institutions should mitigate the risks posed by internal users by

- Performing appropriate background checks and screening of new employees;
- Obtaining agreements covering confidentiality, nondisclosure, and authorized use;
- Using job descriptions, employment agreements and training to increase accountability for security; and
- Providing training to support awareness and policy compliance.

Application owners grant legitimate users system access necessary to perform their duties; security personnel enforce access rights in accordance with institution standards. Because of their internal access levels and intimate knowledge of financial institution processes, authorized users pose a potential threat to systems and data. Employees, contractors, or third-party employees can exploit their legitimate computer access for malicious, fraudulent, or economic reasons. Additionally, the degree of internal access granted to some users increases the risk of accidental damage or loss of information and systems. Risk exposures from internal users include

- Altering data,
- Deleting production and back-up data,
- Disrupting systems,
- Destroying systems,
- Misusing systems for personal gain or to damage the institution,
- Holding data hostage, and
- Stealing strategic or customer data for corporate espionage or fraud schemes.

Background Checks and Screening

Financial institutions should have a process to verify job application information on all new employees. The sensitivity of a particular job or access level may warrant additional background and credit checks. Institutions should verify that contractors are subject to similar screening procedures. Typically, the minimum verification considerations include

- Character references;
- Confirmation that the prospective employee was never convicted of a criminal offense, as detailed in 12 USC 1829;Twelve USC 1829 prohibits an insured depository institution from allowing a person who has been convicted of any criminal offense at the local, state, or Federal level, involving dishonesty or a breach of trust, or money laundering, or has agreed to enter into a pretrial diversion or similar program in connection with a prosecution for such offense, to participate directly or indirectly, in the conduct of the affairs of the institution.
- Confirmation of prior experience, academic record, and professional qualifications; and
- Confirmation of identity from government issued identification.

After employment, managers should remain alert to changes in employees' personal circumstances that could increase incentives for system misuse or fraud.

Agreements: Confidentiality, Non-Disclosure, and Authorized Use

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.Under the GLBA, a financial institution shall design its information security program to ensure the confidentiality of customer information. 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.

Authorized-use agreements are discussed in the "Access Rights Administration" section of this booklet.

Job Descriptions

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.

Training

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, log-on 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.

Data Security

Action Summary

Financial institutions should control and protect access to paper, film and computer-based media to avoid loss or damage. Institutions should

- Establish and ensure compliance with policies for handling and storing information,
- Ensure safe and secure disposal of sensitive media, and
- Secure information in transit or transmission to third parties.

The primary objective of information security is to protect the confidentiality, integrity, and availability of the institution's information assets. All of the controls discussed so far, whether at the perimeters, network or host levels, or embodied in actions taken by people, contribute to the achievement of that objective. However, not all data in an institution require the same protections as other data, and not all data remain within the institution's physical perimeter.

Theory and Tools

Data security theory seeks to establish uniform risk-based requirements for the protection of data elements. To ensure that the protection is uniform within and outside of the institution, tools such as data classifications and protection profiles can be used. Data classification is the identification and organization of information according to its criticality and sensitivity. The classification is linked to a protection profile. A protection profile is a description of the protections that should be afforded to data in each classification. The profile is used both to develop and assess controls within the institution and to develop contractual controls and requirements for those outside the institution who may process, store, or otherwise use that data.

Protection profiles are also useful when data is transported. That may occur, for example, when back-up tapes are moved offsite, when a laptop is removed from the institution, or whenever removable media is used to store the data. The profile should indicate when logical controls such as encryption are necessary; describe the required controls; and address the contractual, physical, and logical controls around transportation arrangements.

Protection profiles should also address the protection of the media that contains the information.

Over time, protection profiles should be reviewed and updated. The review and updating should address new data storage technologies, new protective controls, new methods of attack as they appear, and changes in data sensitivity.

Practical Application

Data classification and protection profiles are complex to implement when the network or storage is viewed as a utility. Because of that complexity, some institutions treat all information at that level as if it were of the highest sensitivity and implement encryption as a protective measure. The complexity in implementing data classification in other layers or in other aspects of an institution's operation may result in other risk mitigation procedures being used. Adequacy is a function of the extent of risk mitigation, and not the procedure or tool used to mitigate risk.

Policies regarding media handling, disposal, and transit should be implemented to enable the use of protection profiles and otherwise mitigate risks to data. If protection profiles are not used, the policies should accomplish the same goal as protection profiles, which is to deliver the same

degree of residual risk without regard to whether the information is in transit or storage, who is directly controlling the data, or where the storage may be.

Handling and Storage

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.

The storage of data in portable devices, such as laptops and PDAs, poses unique problems. Those devices may be removed from the institution and not protected by any physical security arrangements. Additionally, the devices may be lost or stolen. Mitigation of those risks typically involves encryption of sensitive data, host-provided access controls, homing beacons, and remote deletion capabilities. The latter two controls can be Internet-based. Homing beacons send a message to the institution whenever they are connected to a network and enable recovery of the device. Remote deletion uses a similar communication to the institution, and also enables a communication from the institution to the device that commands certain data to be deleted.

Disposal

Financial institutions need appropriate disposal procedures for both electronic and paper-based media. Designating a single individual, department, or function to be responsible for disposal facilitates accountability and promotes compliance with disposal policies. Policies should prohibit employees from discarding media containing sensitive information along with regular garbage to avoid accidental disclosure. Many institutions shred paper-based media on site and others use collection and disposal services to ensure the media is rendered unreadable and unlikely to be reconstructed. Institutions that contract with third parties should use care in selecting vendors to ensure adequate employee background checks, controls, and experience. Contracts with third-party disposal firms should address acceptable disposal procedures. The disposal of customer and consumer information should meet the requirements of the 501(b) guidelines.

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 destroys data by replacing that data with new, random data. The replacement is accomplished by writing the new data to the disk sectors that hold the data being destroyed. To be effective, overwriting may have to be performed many times.Overwriting may be preferred when the media will be re-used. 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.

Transit

Financial institutions should maintain the security of media while in transit or when shared with third parties. Policies should include

- Contractual requirements that incorporate necessary risk-based controls,
- Restrictions on the carriers used and procedures to verify the identity of couriers,
- Requirements for appropriate packaging to protect the media from damage,
- Use of encryption for transmission or transport of sensitive information,
- Tracking of shipments to provide early indications of loss or damage,
- Security reviews or independent security reports of receiving companies, and
- Use of nondisclosure agreements between couriers and third parties.

Financial institutions should address the security of their back-up tapes at all times, including when the tapes are in transit from the data center to off-site storage.

Service Provider Oversight

Action Summary

Financial institutions should exercise their security responsibilities for outsourced operations through

- Appropriate due diligence in service provider research and selection,
- Contractual assurances regarding security responsibilities, controls, and reporting,
- Nondisclosure agreements regarding the institution's systems and data,
- Independent review of the service provider's security though appropriate audits and tests, and
- Coordination of incident response policies and contractual notification requirements.

Many financial institutions outsource some aspect of their operations. Although outsourcing arrangements often provide a cost-effective means to support the institution's technology needs, the ultimate responsibility and risk rests with the institution. Financial institutions are required under the 501(b) guidelines to ensure service providers have implemented adequate security controls to safeguard customer information. The guidelines require institutions to

- Exercise appropriate due diligence in selecting service providers,
- Require service providers by contract to implement appropriate security controls to comply with the guidelines, and
- Monitor service providers to confirm that they are maintaining those controls when indicated by the institution's risk assessment.

Financial institutions should implement these same precautions in all TSP relationships based on the level of access to systems or data for safety and soundness reasons, in addition to the privacy requirements.

Financial institutions should evaluate the following security considerations when selecting a service provider:

- Service provider references and experience,
- Security expertise of TSP personnel,
- Background checks on TSP personnel,
- Contract assurances regarding security responsibilities and controls,
- Nondisclosure agreements covering the institution's systems and data,
- Ability to conduct audit coverage of security controls or obtain adequate reports of security testing from independent third parties, and
- Clear understanding of the provider's security incidence response policy and assurance that the provider will communicate security incidents promptly to the institution when its systems or data were potentially compromised.

Financial institutions should ensure TSPs implement and maintain controls sufficient to appropriately mitigate risk. In higher-risk relationships the institution by contract may prescribe minimum control and reporting standards, obtain the right to require changes to standards as external and internal environments change, and obtain access to the TSP for institution or independent third-party evaluations of the TSP's performance against the standard. In lower risk relationships the institution may prescribe the use of standardized reports, such as trust services reports or a Statement of Auditing Standards 70 (SAS 70) report.

Trust Services

The American Institution of Certified Public Accountants created two trust services, WebTrust and SysTrust, to address the risks and opportunities of information technology. WebTrust reports provide assurance related to e-commerce systems. SysTrust reports provide assurance on the reliability of systems. In each service, certified public accountants are engaged by the TSP to evaluate, test, and report on whether a system meets certain principles and associated evaluation criteria. One of those principles is security.

WebTrust and SysTrust reports differ from a SAS 70 report in many important respects. The primary difference is that the evaluation criteria are uniform for all WebTrust and SysTrust reports.

Institutions that consider using WebTrust and SysTrust reports as a part of their monitoring of service provider performance should consider whether the review criteria for security are sufficiently rigorous for the institution's needs, whether the scope of the review is adequate for the institution's needs, and whether additional monitoring is required.

See the Third-Party Reviews of Technology Service Providers section of the FFIEC IT Examination Handbook, "Audit" for more detailed information on this topic.

SAS 70 Reports

Frequently TSPs or user groups will contract with an accounting firm to report on internal controls, including security, using SAS 70. SAS 70 is an auditing standard developed by the American Institute of Certified Public Accountants. SAS 70 focuses on controls and control objectives. It allows for two types of reports. A SAS 70 Type I report gives the service

provider's description of controls at a specific time, and an auditor's report. The auditor's report will provide an opinion on whether the control description fairly presents the relevant aspects of the controls, and whether the controls were suitably designed for their purpose.

A SAS 70 Type II report expands upon a Type I report by addressing whether the controls were functioning. It provides a description of the auditor's tests of the controls. It also provides an expanded auditor's report that addresses whether the controls that were tested were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives were achieved during the specified period.

Financial institutions should carefully and critically evaluate whether a SAS 70 report adequately supports their oversight responsibilities. The report may not provide a thorough test of security controls and security monitoring unless requested by the TSP. It may not address the effectiveness of the security process in continually mitigating changing risks. Additionally, the SAS 70 report may not address whether the TSP is meeting the institution's specific risk mitigation requirements. Therefore, the contracting oversight exercised by financial institutions may require additional tests, evaluations, and reports to appropriately oversee the security program of the service provider. See the Third-Party Reviews of Technology Service Providers section in the FFIEC IT Examination Handbook, "Audit" for more detailed information on this topic.

Business Continuity Considerations

Action Summary

Financial institutions should consider

- Identification of personnel with key security roles during a continuity plan implementation, and training personnel in those roles; and
- Security needs for back-up sites and alternate communication networks.

Events that trigger the implementation of a business continuity plan may have significant security implications. Depending on the event, some or all of the elements of the security environment may change. Different people may be involved in operations, at different physical locations, using similar but different machines and software which may communicate over different communications lines. Different tradeoffs may exist between availability, integrity, confidentiality, and accountability, with a different appetite for risk on the part of management.

Business continuity plans should be reviewed as an integral part of the security process. Risk assessments should consider the changing risks that appear in business continuity scenarios and the different security posture that may be established. Strategies should consider the different risk environment and the degree of risk mitigation necessary to protect the institution in the event the continuity plans must be implemented. The implementation should consider the training of appropriate personnel in their security roles, and the implementation and updating of technologies and plans for back-up sites and communications networks. These security considerations should be integrated with the testing of business continuity plan implementations. For more information, see the "Business Continuity Planning" booklet of the FFIEC IT Examination Handbook.

Insurance

Action Summary

Financial institutions should carefully evaluate the extent and availability of coverage in relation to the specific risks they are seeking to mitigate.

Financial institutions use insurance coverage as an effective method to transfer risks from themselves to insurance carriers. Coverage is increasingly available to cover risks from security breaches or denial of service attacks. Several insurance companies offer e-commerce insurance packages that can reimburse financial institutions for losses from fraud, privacy breaches, system downtime, or incident response. When evaluating the need for insurance to cover information security threats, financial institutions should understand the following points:

- Insurance is not a substitute for an effective security program.
- Traditional fidelity bond coverage may not protect from losses related to security intrusions.
- Availability, cost, and covered risks vary by insurance company.
- Availability of new insurance products creates a more dynamic environment for these factors.
- Insurance cannot adequately cover the reputation and compliance risk related to customer relationships and privacy.
- Insurance companies typically require companies to certify that certain security practices are in place.

Insurance coverage is rapidly evolving to meet the growing number of security-related threats. Coverage varies by insurance company, but currently available insurance products may include coverage for the following risks:

- Vandalism of financial institution Web sites;
- Denial-of-service attacks;
- Loss of income;
- Computer extortion associated with threats of attack or disclosure of data;
- Theft of confidential information;
- Privacy violations;
- Litigation (breach of contract);
- Destruction or manipulation of data (including viruses);
- Fraudulent electronic signatures on loan agreements;
- Fraudulent instructions through e-mail;
- Third-party risk from companies responsible for security of financial institution systems or information;
- Insiders who exceed system authorization; and
- Incident response costs related to the use of negotiators, public relations consultants, security and computer forensic consultants, programmers, replacement systems, etc.

Financial institutions can attempt to insure against these risks through existing blanket bond insurance coverage added on to existing policies in order to address specific threats. It is important that financial institutions understand the extent of coverage and the requirements

governing the reimbursement of claims. For example, financial institutions should understand the extent of coverage available in the event of security breaches at a third-party service provider. In such a case, the institution may want to consider contractual requirements that require service providers to maintain adequate insurance to cover security incidents.

When considering supplemental insurance coverage for security incidents, the institution should assess the specific threats in light of the impact these incidents will have on its financial, operational, and reputation risk profiles. Obviously, when a financial institution contracts for additional coverage, it should ensure that it is aware of and prepared to comply with any required security controls both at inception of the coverage and over the term of the policy.

Security Monitoring

Action Summary

Financial institutions should gain assurance of the adequacy of their risk mitigation strategy and implementation by

- Monitoring network and host activity to identify policy violations and anomalous behavior;
- Monitoring host and network condition to identify unauthorized configuration and other conditions which increase the risk of intrusion or other security events;
- Analyzing the results of monitoring to accurately and quickly identify, classify, escalate, report, and guide responses to security events; and
- Responding to intrusions and other security events and weaknesses to appropriately mitigate the risk to the institution and its customers, and to restore the institution's systems.

Security monitoring focuses on the activities and condition of network traffic and network hosts. Activity monitoring is primarily performed to assess policy compliance, identify non-compliance with the institution's policies, and identify intrusions and support an effective intrusion response. Because activity monitoring is typically an operational procedure performed over time, it is capable of providing continual assurance.

Monitoring of condition is typically performed in periodic testing. The assurance provided by condition monitoring can relate to the absence of an intrusion, the compliance with authorized configurations, and the overall resistance to intrusions. Condition monitoring does not provide continual assurance, but relates to the point in time of the test.

Risk drives the degree of monitoring. In general, risk increases with system accessibility and the sensitivity of data and processes. For example, a high-risk system is one that is remotely accessible and allows direct access to funds, fund transfer mechanisms, or sensitive customer data. Information-only Web sites that are not connected to any internal institution system or transaction-capable service are lower-risk systems. Information systems that exhibit high risks

should be subject to more rigorous monitoring than low-risk systems.

A financial institution's security monitoring should, commensurate with the risk, be able to identify control failures before a security incident occurs, detect an intrusion or other security incident in sufficient time to enable an effective and timely response, and support post-event forensics activities.

Architecture Issues

Financial institution networks should be designed to support effective monitoring. Design considerations include

- Network traffic policies that address the allowed communications between computers or groups of computers,
- Security domains that implement the policies,
- Sensor placement to identify policy violations and anomalous traffic,
- The nature and extent of logging,
- Log storage and protection, and
- Ability to implement additional sensors on an ad hoc basis.

Activity Monitoring

Activity monitoring consists of host and network data gathering, and analysis. Host data is gathered and recorded in logs and includes performance and system events of security significance. Host performance is important to identify anomalous behavior that may indicate an intrusion. Security events are important both for the identification of anomalous behavior and for enforcing accountability. Examples of security events include operating system access, privileged access, creation of privileged accounts, configuration changes, and application access. Privileged access may be subject to keystroke recording. Sensitive applications should have their own logging of significant events.

Host activity recording is typically limited by the abilities of the operating system and application.

Network data gathering is enabled by sensors that typically are placed at control points within the network. For example, a sensor could record traffic that is allowed through a firewall into the DMZ, and another sensor could record traffic between the DMZ and the internal network. As another example, a sensor could be placed on a switch that controls a subnet on the internal network and record all activity into and out of the subnet.

Network data gathering is governed by the nature of network traffic. The activity recorded can range from parts of headers to full packet content. Packet header information supports traffic analysis and provides such details as the endpoints, length, and nature of network communication. Packet header recording is useful even when packet contents are encrypted. Full packet content provides the exact communications traversing the network in addition to supporting traffic analysis. Full packet content recording allows for a more complete analysis, but entails additional collection, storage, and retrieval costs.

Many types of network sensors exist. Sensors built into some popular routers record activity from packet headers. Host-based sniffer software can be used on a device that does not have an IP address. Some sensors are honeypots, or hosts configured to respond to network communications similar to other hosts, but exist only for the purpose of capturing communications. Other sensors contain logic that performs part of the analysis task, alerting on the similarity between observed traffic and preconfigured rules or patterns. Those sensors are known as "Intrusion Detection Systems."

Network Intrusion Detection Systems

Network intrusion detection systems (nIDS) combine the detection and logging of potential attacks with pre-defined response actions. These systems use one of two detection methodologies, signature and anomaly detection. For response, the nIDS can perform one of several actions according to its configuration. A passive nIDS could be configured to notify institution personnel, log the attack identification, and log packets related to the possible attack. A reactive IDS adds the capability to interact with the firewall to block communications from the user or IP address associated with the potential attack. Conceptually, the reactive IDS is very similar to an intrusion prevention system (IPS), discussed in the "Access Control" section of this booklet.

To use a nIDS effectively, an institution should have a sound understanding of the detection capability and the effect of placement, tuning, and other network defenses on the detection capability.

The signature-based detection methodology reads network packets and compares the content of the packets against signatures, or unique characteristics, of known attacks. When a match is recognized between current readings and a signature, the nIDS generates an alert.

Signatures may take several forms. The simplest form is the URL submitted to a Web server, where certain references, such as cmd.exe, are indicators of an attack. The nature of traffic to and from a server can also serve as a signature. An example is the length of a session and amount of traffic passed.

A weakness in the signature-based detection method is that a signature must exist for an alert to be generated. Signatures are written to either capture known exploits, or access to suspected vulnerabilities. Vulnerability-based detection is generally broader based, alerting on many exploits for the same vulnerability and potentially alerting on exploits that are not yet known. Exploit-based signatures, however, are based on specific exploits and may not alert when a new or previously unknown exploit is attempted.

Attacks that generate different signatures from what the institution includes in its nIDS will not be detected. This problem can be particularly acute if the institution does not continually update its signatures to reflect lessons learned from attacks on itself and others, as well as developments in attack tool technologies. It can also pose problems when the signatures only address known attacks. Another weakness is in the capacity of the nIDS to read traffic. If the nIDS falls behind in reading network traffic, traffic may be allowed to bypass the nIDS.IDS units that have a traffic rating, such as gigabit IDS, may allow traffic to bypass when traffic reaches a fraction of their rating. That traffic may contain attacks that would otherwise cause the nIDS to issue an alert.

The anomaly-based detection method generally detects deviations from a baseline. The baseline can be either protocol-based, or behavior-based. The protocol-based baseline detects differences between the detected packets for a given protocol and the Internet's RFCs (Requests for

Comment) pertaining to that protocol. For example, a header field could exceed the RFC-established expected size.

The behavior-based anomaly detection method creates a statistical profile of normal activity on the host or network. Normal activity generally is measured based on the volume of traffic, protocols in use, and connection patterns between various devices. Boundaries for activity are established based on that profile. When current activity exceeds the boundaries, an alert is generated. Weaknesses in this system involve the ability of the system to accurately model activity, the relationship between valid activity in the period being modeled and valid activity in future periods, and the potential for malicious activity to take place while the modeling is performed. This method is best employed in environments with predictable, stable activity.

Anomaly detection can be an effective supplement to signature-based methods by signaling attacks for which no signature yet exists. Proper placement of nIDS sensorsThe sensor gathers information for analysis by the detection engine. is a strategic decision determined by the information the institution is trying to obtain. Placement outside the firewall will deliver IDS alarms related to all attacks, even those that are blocked by the firewall. With this information, an institution can develop a picture of potential adversaries and their expertise based on the probes they issue against the network.

Because the placement is meant to gain intelligence on attackers rather than to alert on attacks, tuning generally makes the nIDS less sensitive than if it is placed inside the firewall. A nIDS outside the firewall will generally alert on the greatest number of unsuccessful attacks. nIDS monitoring behind the firewall is meant to detect and alert on hostile intrusions. Multiple nIDS units can be used, with placement determined by the expected attack paths to sensitive data. Generally speaking, the closer the nIDS is to sensitive data, the more important the tuning, monitoring, and response to nIDS alerts. The National Institute of Standards and Technology (NIST) recommends network intrusion detection systems "at any location where network traffic from external entities is allowed to enter controlled or private networks."NIST Special Publication 800-41

"Tuning" refers to the creation of signatures and alert filters that can distinguish between normal network traffic and potentially malicious traffic. Tuning also involves creating and implementing different alerting and logging actions based on the severity of the perceived attack. Proper tuning is essential to both reliable detection of attacks and the enabling of a priority-based response. Tuning of some signature-based units for any particular network may take an extended period of time and involve extensive analysis of expected traffic. If a nIDS is not properly tuned, the volume of alerts it generates may degrade the intrusion identification and response capability.

Switched networks pose a problem for network IDS. Switches ordinarily do not broadcast traffic to all ports, and a nIDS may need to see all traffic to be effective. When switches do not have a port that receives all traffic, the financial institution may have to alter their network to include a hub or other device to allow the IDS to monitor traffic.

Encryption poses a potential limitation for a nIDS. If traffic is encrypted, the nIDS's effectiveness may be limited to anomaly detection based on unencrypted header information. This limitation can by overcome by decrypting packets within the IDS at rates commensurate with the flow of traffic. Decryption is a device-specific feature that is not incorporated into all nIDS units.

All nIDS detection methods result in false positives (alerts where no attack exists) and false negatives (no alert when an attack does take place). While false negatives are obviously a concern, false positives can also hinder detection. When security personnel are overwhelmed with the number of false positives, they may look at the nIDS reports with less vigor, allowing real attacks to be reported by the nIDS but not researched or acted upon. Additionally, they may

tune the nIDS to reduce the number of false positives, which may increase the number of false negatives. Risk-based testing is necessary to ensure the detection capability is adequate.

Honeypots

A honeypot is a network device that the institution uses to attract attackers to a harmless and monitored area of the network. Honeypots have three key advantages over network and host IDSs. Since the honeypot's only function is to be attacked, any network traffic to or from the honeypot potentially signals an intrusion. Monitoring that traffic is simpler than monitoring all traffic passing a network IDS. Honeypots also collect very little data, and all of that data is highly relevant. Network IDSs gather vast amounts of traffic which must be analyzed, sometimes manually, to generate a complete picture of an attack. Finally, unlike an IDS, a honeypot does not pass packets without inspection when under a heavy traffic load.

Honeypots have two key disadvantages. First, they are ineffective unless they are attacked. Consequently, organizations that use honeypots for detection usually make the honeypot look attractive to an attacker. Attractiveness may be in the name of the device, its apparent capabilities, or in its connectivity. Since honeypots are ineffective unless they are attacked, they are typically used to supplement other intrusion detection capabilities.

The second key disadvantage is that honeypots introduce the risk of being compromised without triggering an alarm, thereby becoming staging grounds for attacks on other devices. The level of risk is dependent on the degree of monitoring, capabilities of the honeypot, and its connectivity. For instance, a honeypot that is not rigorously monitored, that has excellent connectivity to the rest of the institution's network, and that has varied and easy-to-compromise services presents a high risk to the confidentiality, integrity, and availability of the institution's systems and data. On the other hand, a honeypot that is rigorously monitored and whose sole capability is to log connections and issue bogus responses to the attacker, while signaling outside the system to the administrator, demonstrates much lower risk.

Host Intrusion Detection Systems

Host intrusion detection systems (hIDS) also use signature-based and anomaly-based methods. Popular hIDSs include anti-virus and anti-spyware programs (See the "Malicious Code Prevention" section of this booklet), as well as file integrity checkers.

A file integrity checker creates a hash of key binaries, and periodically compares a newly generated hash against the original hash. Any mismatch signals a change to the binary, a change that could be the result of an intrusion. Successful operation of this method involves protection of the original binaries from change or deletion and protection of the host that compares the hashes. If attackers can substitute a new hash for the original, an attack may not be identified. Similarly, if an attacker can alter the host performing the comparison so that it will report no change in the hash, an attack may not be identified.

An anomaly-based method monitors the application program calls to the operating system for unexpected or unwanted behavior, such as a Web server calling a command line interface, and alerts when unexpected calls are made.

Attackers can defeat host-based IDS systems using kernel modules. A kernel module is software that attaches itself to the operating system kernel. From there, it can redirect and alter

communications and processing, hiding files, processes, registry keys, and other information. With the proper kernel module, an attacker can force a comparison of hashes to always report a match and provide the same cryptographic fingerprint of a file, even after the source file was altered. Kernel modules can also hide the use of the application program interfaces. Detection of kernel modules can be extremely difficult. Detection is typically performed through another kernel module or applications that look for anomalies left behind when the kernel module is installed.

Some host-based IDS units address the difficulty of performing intrusion detection on encrypted traffic. Those units position their sensors between the decryption of the IP packet and the execution of any commands by the host. This host-based intrusion detection method is particularly appropriate for Internet banking servers and other servers that communicate over an encrypted channel. Kernel modules, however, can defeat these host-based IDS units.

Host-based intrusion detection systems are recommended by the NIST for all mission-critical systems, even those that should not allow external access.NIST Special Publication 800-41.

Log Transmission, Normalization, Storage, and Protection

Network and host activities typically are recorded on the host and sent across the network to a central logging facility. The data that arrives at the logging facility is in the format of the software that recorded the activity. The logging facility may process the logging data into a common format. That process is called normalization. Normalized data frequently enables timely and effective log analysis.

Log files are critical to the successful investigation and prosecution of security incidents and can potentially contain sensitive information. Intruders will often attempt to conceal any unauthorized access by editing or deleting log files. Therefore, institutions should strictly control and monitor access to log files whether on the host or in a centralized logging facility. Some considerations for securing the integrity of log files include

- Encrypting log files that contain sensitive data or that are transmitting over the network;
- Ensuring adequate storage capacity to avoid gaps in data gathering;
- Securing back-up and disposal of log files;
- Logging the data to a separate, isolated computer;
- Logging the data to write-only media like a write-once/read-many (WORM) disk or drive; and
- Setting logging parameters to disallow any modification to previously written data.

Condition Monitoring

Condition monitoring tools include self-assessments, metrics, and independent tests.

Self Assessments

Self-assessments are useful in providing a warning flag to line management so problems can be addressed before they arise in testing reports. Self-assessments may be performed by operations personnel or by vendors under the direction of those at the institution who are responsible for the

systems being assessed. Self-assessments may use tools and techniques similar to independently performed audits and penetration tests, and include:

- Assessing conformance to policies and procedures, including service provider oversight;
- Scanning for technical vulnerabilities;
- Verifying that device and network configurations are authorized and changes are properly processed;
- Verifying that information is stored only where authorized;
- Reviewing the adequacy of the risk assessment and monitoring plans; and
- Reviewing test results.

Metrics

Metrics can be used to measure security policy implementation, the effectiveness and efficiency of security services delivery, and the impact of security events on business processes. The measurement of security characteristics can allow management to increase control and drive improvements to the security process.

Metrics may not measure conformance to policy directly. Policies frequently are general statements that lack the specificity necessary for measurement. Metrics generally are formed to measure conformance to the standards and procedures that are used to implement policies. Those standards may be developed by the institution, developed or recognized by the financial institution industry (e.g. BITS), or developed or recognized for business in general. An example of the third is ISO 17799.

The adoption of standards, however, does not mean that a metrics system can or should be instituted. Metrics are best used in mature security processes, when

- Information measures are quantifiable and readily obtainable, and
- Processes are repeatable.

The degree to which a security metrics program mitigates risk is a function of the comprehensiveness and accuracy of the measurements and the analysis and use of those measurements. The measurements should be sufficient to justify security decisions that affect the institution's security posture, allocate resources to security-related tasks, and provide a basis for security-related reports.

Independent Tests

Independent tests include penetration tests, audits, and assessments. Independence provides credibility to the test results. To be considered independent, testing personnel should not be responsible for the design, installation, maintenance, and operation of the tested system, or the policies and procedures that guide its operation. The reports generated from the tests should be prepared by individuals who also are independent of the design, installation, maintenance, and operation of the tested system.

Penetration tests, audits, and assessments can use the same set of tools in their methodologies. The nature of the tests, however, is decidedly different. Additionally, the definitions of penetration test and assessment, in particular, are not universally held and have changed over time.

Penetration Tests. A penetration test subjects a system to the real-world attacks selected and conducted by the testing personnel. The benefit of a penetration test is that it identifies the extent to which a system can be compromised before the attack is identified and assesses the response mechanism's effectiveness. Because a penetration test seldom is a comprehensive test of the system's security, it should be combined with other monitoring to validate the effectiveness of the security process.

Audits. Auditing compares current practices against a set of standards. Industry groups or institution management may create those standards. Institution management is responsible for demonstrating that the standards it adopts are appropriate for the institution.

Assessments. An assessment is a study to locate security vulnerabilities and identify corrective actions. An assessment differs from an audit by not having a set of standards to test against. It differs from a penetration test by providing the tester with full access to the systems being tested. Assessments may be focused on the security process or the information system. They may also focus on different aspects of the information system, such as one or more hosts or networks.

Key Factors

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.The quarterly auditing and verification need not be by an independent source. See NIST Special Publication 800-41. 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.

Analysis and Response

The analysis and response to activity and condition monitoring is performed differently in financial institutions of different size and complexity. Smaller and less complex institutions may assign operational personnel to the analysis and response function. Larger and more complex institutions may maintain a security response center that receives and analyzes the data flows as activity occurs. Additionally, institutions of all sizes may outsource various aspects of the analysis and response function, such as activity monitoring. Outsourcing does not relieve the institution of the responsibility for ensuring that control failures are identified before a security incident occurs, an intrusion or other security incident is detected in sufficient time to enable an effective and timely response, and post-event forensics activities are supported.

Security Incidents

An internal security response center serves as a central location for the analysis and investigation of potential security incidents. To serve in that role, the security response center should consider, evaluate, and respond to both external threats and internal vulnerabilities. Sources of external threat information include industry information sharing and analysis centers (ISACs), Infraguard, mailing lists, and commercial reporting services. Internal vulnerability information is available from condition reporting and activity monitoring. Security response centers should be able to access all relevant internal vulnerability information in a read-only manner. That data may reside in centralized log repositories, on the devices that perform the logging, and in results of self-assessments and independent tests. Security response centers also should have available tools to analyze the logs and to perform ad hoc activity monitoring. Other additional and useful data sources are reports of anomalies in both network and host performance and the end-user experience. The latter relates both to internal users as well as contractors and customers who use the institution's systems.

Because the identification of incidents requires monitoring and management, response centers frequently use SIM (security information management) tools to assist in the data collection, analysis, classification, and reporting of activities related to security incidents.

The security response center should be governed by policies and procedures that address security incidents:

- 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.
- Classification policies should be sufficiently clear to enable timely classification of incidents into different levels of severity. Response and reporting levels should be commensurate with the severity levels.
- Escalation policies should address when different personnel within the organization will be contacted about the incident, and the responsibility those personnel have in incident analysis and response.
- Reporting policies should address internal and external reporting, including coordination with service providers and reporting to industry ISACs.

Additionally, a policy should address who is empowered to declare an incident to be an intrusion.

The effectiveness of a security incident response center also is a function of the training and expertise of the security analysts. A financial institution should ensure that its analysts are sufficiently trained to appropriately analyze network and host activity and to use the monitoring and analysis tools made available to them.

Intrusion Response

The goal of intrusion response is to minimize damage to the institution and its customers through containment of the intrusion, the restoration of systems, and providing assistance to customers.

The response primarily involves people rather than technologies. The quality of intrusion response is a function of the institution's culture, policies and procedures, and training.

Preparation determines the success of any intrusion response. This involves defining the policies and procedures that guide the response, assigning responsibilities to individuals, providing appropriate training, formalizing information flows, and selecting, installing, and understanding the tools used in the response effort. Key considerations that directly affect the institution's policies and procedures include the following:

- How to balance concerns regarding availability, confidentiality, and integrity for devices and data of different sensitivities. This consideration is a key driver for a containment strategy and may involve legal and liability considerations. An institution may decide that some systems must be disconnected or shut down at the first sign of intrusion, while others must be left on line.
- When and under what circumstances to invoke the intrusion response activities, and how to ensure that the proper personnel are notified and available.
- How to control the frequently powerful intrusion identification and response tools.
- When to involve outside experts and how to ensure the proper expertise will be available when needed. This consideration addresses both the containment and the restoration strategy.
- When and under what circumstances to notify and involve regulators, customers, and law enforcement. This consideration drives certain monitoring decisions, decisions regarding evidence-gathering and preservation, and communications considerations.
- Which personnel have authority to perform what actions in containment of the intrusion and restoration of the systems. This consideration affects the internal communications strategy, the commitment of personnel, and procedures that escalate involvement and decisions within the organization.

- How and what to communicate outside the organization, whether to law enforcement, supervisory agencies, customers, service providers, potential victims, and others. This consideration drives the communication strategy and is a key component in mitigating reputation risk.
- How to document and maintain the evidence, decisions, and actions taken.
- What criteria must be met before compromised services, equipment, and software are returned to the network.
- How to learn from the intrusion and use those lessons to improve the institution's security.
- How and when to prepare and file a Suspicious Activities Report (SAR).

Successful implementation of any response policy and procedure requires the assignment of responsibilities and training. Some organizations formalize the response program with the creation of a computer security incident response team (CSIRT). The CSIRT is typically tasked with performing, coordinating, and supporting responses to security incidents. Due to the wide range of technical and nontechnical issues that are posed by an intrusion, typical CSIRT membership includes individuals with a wide range of backgrounds and expertise, from many different areas within the institution. Those areas include management, legal, public relations, as well as information technology. Other organizations may outsource some of the CSIRT functions, such as forensic examinations. When CSIRT functions are outsourced, institutions should ensure that the service provider follows the institution's policies and maintains the confidentiality of data.

Institutions should assess the adequacy of their preparations through testing.

While containment strategies between institutions can vary, they typically contain the following broad elements:

- Isolation of compromised systems, or enhanced monitoring of intruder activities;
- Search for additional compromised systems;
- Collection and preservation of evidence; and
- Communication with effected parties, the primary regulator, and law enforcement.

Restoration strategies should address the following:

- Elimination of an intruder's means of access;
- Restoration of systems, programs and data to known good state;
- Filing of a SAR (guidelines for filing are included in individual agency guidance), and
- Initiation of customer notification and assistance activities consistent with interagency guidance.

Outsourced Systems

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.

Security Process Monitoring and Updating

Action Summary

Financial institutions should continuously gather and analyze information regarding new threats and vulnerabilities, actual attacks on the institution or others, and the effectiveness of the existing security controls. They should then use that information to update the risk assessment, strategy, and implemented controls.

A static security program provides a false sense of security and will become increasingly ineffective over time. Monitoring and updating the security program is an important part of the ongoing cyclical security process. Financial institutions should treat security as dynamic with active monitoring; prompt, ongoing risk assessment; and appropriate updates to controls. Institutions should continuously gather and analyze information regarding new threats and vulnerabilities, actual attacks on the institution or others, and the effectiveness of the existing security controls. They should use that information to update the risk assessment, strategy, and implemented controls. Updating the security program begins with the identification of the potential need to alter aspects of the security program and then recycles through the security process steps of risk assessment, strategy, implementation, and testing.

Monitoring

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:

- 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.
- Security personnel should monitor the information technology environment and review performance reports to identify trends, new threats, or control deficiencies. Specific activities could include reviewing security and activity logs, investigating operational anomalies, and routinely reviewing system and application access levels.
- Security personnel and system owners should monitor external sources for new technical and non-technical vulnerabilities and develop appropriate mitigation solutions to address them.

Examples include many controls discussed elsewhere in this booklet, including
- Establishing an effective process that monitors for vulnerabilities in hardware and software and establishes a process to install and test security patches,
- Maintaining up-to-date anti-virus definitions and intrusion detection attack definitions, and
- Providing effective oversight of service providers and vendors to identify and react to new security issues.

- 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.

Updating

Financial institutions should evaluate the information gathered to determine the extent of any required adjustments to the various components of their security program. The institution will need to consider the scope, impact, and urgency of any new or changing threat or vulnerability. Depending on the nature of changing environment, the institution will need to reassess the risk and make changes to its security process (e.g., the security strategy, the controls implementation, or the security monitoring requirements).

Institution management confronts routine security issues and events on a regular basis. In many cases, the issues are relatively isolated and may be addressed through an informal or targeted risk assessment embedded within an existing security control process. For example, the institution might assess the risk of a new operating system vulnerability before testing and installing the patch. More systemic events like mergers, acquisitions, new systems, or system conversions, however, warrant a more extensive security risk assessment. Regardless of the scope, the potential impact and the urgency of the risk exposure will dictate when and how controls are changed.

Endnotes

Appendix A: Examination Procedures

EXAMINATION OBJECTIVE: Assess the quantity of risk and the effectiveness of the institution's risk management processes as they relate to the security measures instituted to ensure confidentiality, integrity, and availability of information and to instill accountability for actions taken on the institution's systems. The objectives and procedures are divided into Tier 1 and Tier II:

- Tier I assesses an institution's process for identifying and managing risks.
- Tier II provides additional verification where risk warrants it.

Tier I and Tier II are intended to be a tool set examiners will use when selecting examination procedures for their particular examination. Examiners should use these procedures as necessary to support examination objectives.

Tier I Procedures

Objective 1: Determine the appropriate scope for the examination.

1. Review past reports for outstanding issues or previous problems. Consider
   - Regulatory reports of examination
   - Internal and external audit reports
   - Independent security tests
   - Regulatory, audit, and security reports from service providers
2. Review management's response to issues raised at the last examination. Consider
   - Adequacy and timing of corrective action
   - Resolution of root causes rather than just specific issues
   - Existence of any outstanding issues
3. Interview management and review examination information to identify changes to the technology infrastructure or new products and services that might increase the institution's risk from information security issues. Consider
   - Products or services delivered to either internal or external users
   - Network topology including changes to configuration or components
   - Hardware and software listings
   - Loss or addition of key personnel
   - Technology service providers and software vendor listings
   - Changes to internal business processes
   - Key management changes
   - Internal reorganizations
4. Determine the existence of new threats and vulnerabilities to the institution's information security. Consider
   - Changes in technology employed by the institution
   - Threats identified by institution staff
   - Known threats identified by information sharing and analysis organizations and other non-profit and commercial organizations.
   - Vulnerabilities raised in security testing reports

Quantity of Risk

Objective 2: Determine the complexity of the institution's information security environment.

1. Review the degree of reliance on service providers for information processing and technology support including security management. Review evidence that service providers of information processing and technology participate in an appropriate industry Information Sharing and Analysis Center (ISAC).
2. Identify unique products and services and any required third-party access requirements.
3. Determine the extent of network connectivity internally and externally, and the boundaries and functions of security domains.
4. Identify the systems that have recently undergone significant change, such as new hardware, software, configurations, and connectivity. Correlate the changed systems with the business processes they support, the extent of customer data available to those processes, and the role of those processes in funds transfers.
5. Evaluate management's ability to control security risks given the frequency of changes to the computing environment.
6. Evaluate security maintenance requirements and extent of historical security issues with installed hardware/software.
7. Identify whether external standards are used as a basis for the security program, and the extent to which management tailors the standards to the financial institutions' specific circumstances.
8. Determine the size and quality of the institution's security staff. Consider
   - Appropriate security training and certification
   - Adequacy of staffing levels and impact of any turnover
   - Extent of background investigations
   - Available time to perform security responsibilities

Quality of Risk Management

Objective 3: Determine the adequacy of the risk assessment process.

1. Review the risk assessment to determine whether the institution has characterized its system properly and assessed the risks to information assets. Consider whether the institution has:
   - Identified and ranked information assets (e.g., data, systems, physical locations) according to a rigorous and consistent methodology that considers the risks to customer non-public information as well as the risks to the institution,
   - Identified all reasonably foreseeable threats to the financial institution assets,
   - Analyzed its technical and organizational vulnerabilities, and
   - Considered the potential effect of a security breach on customers as well as the institution.
2. Determine whether the risk assessment provides adequate support for the security strategy, controls, and monitoring that the financial institution has implemented.
3. Evaluate the risk assessment process for the effectiveness of the following key practices:
   - Multidisciplinary and knowledge-based approach
   - Systematic and centrally controlled
   - Integrated process
   - Accountable activities
   - Documented
   - Knowledge enhancing
   - Regularly updated
4. Identify whether the institution effectively updates the risk assessment prior to making system changes, implementing new products or services, or confronting new external conditions that would affect the risk analysis. Identify whether, in the absence of the above factors, the risk assessment is reviewed at least once a year.

Objective 4: Evaluate the adequacy of security policies and standards relative to the risk to the

institution.

1. Review security policies and standards to ensure that they sufficiently address the following areas when considering the risks identified by the institution. If policy validation is necessary, consider performing Tier II procedures.
    - Authentication and Authorization
        - Acceptable-use policy that dictates the appropriate use of the institution's technology including hardware, software, networks, and telecommunications.
        - Administration of access rights at enrollment, when duties change, and at employee separation.
        - Appropriate authentication mechanisms including token-based systems, digital certificates, or biometric controls and related enrollment and maintenance processes as well as database security.
    - Network Access
        - Security domains
        - Perimeter protections including firewalls, malicious code prevention, outbound filtering, and security monitoring.
        - Appropriate application access controls
        - Remote access controls including wireless, VPN, modems, and Internet-based
    - Host Systems
        - Secure configuration (hardening)
        - Operating system access
        - Application access and configuration
        - Malicious code prevention
        - Logging
        - Monitoring and updating
    - User Equipment
        - Secure configuration (hardening)
        - Operating system access
        - Application access and configuration
        - Malicious code prevention
        - Logging
        - Monitoring and updating
    - Physical controls over access to hardware, software, storage media, paper records, and facilities
    - Encryption controls
    - Malicious code prevention
    - Software development and acquisition, including processes that evaluate the security features and software trustworthiness of code being developed or acquired, as well as change control and configuration management.
    - Personnel security
    - Media handling procedures and restrictions, including procedures for securing, transmitting and disposing of paper and electronic information
    - Service provider oversight
    - Business continuity
    - Insurance
2. Evaluate the policies and standards against the following key actions:
    - Implementing through ordinary means, such as system administration procedures and acceptable-use policies;
    - Enforcing with security tools and sanctions;
    - Delineating the areas of responsibility for users, administrators, and managers;
    - Communicating in a clear, understandable manner to all concerned;
    - Obtaining employee certification that they have read and understood the policy;
    - Providing flexibility to address changes in the environment; and

- Conducting annually a review and approval by the board of directors.

Objective 5: Evaluate the security-related controls embedded in vendor management.

1. Evaluate the sufficiency of security-related due diligence in service provider research and selection.
2. Evaluate the adequacy of contractual assurances regarding security responsibilities, controls, and reporting.
3. Evaluate the appropriateness of nondisclosure agreements regarding the institution's systems and data.
4. Determine that the scope, completeness, frequency, and timeliness of third-party audits and tests of the service provider's security are supported by the financial institution's risk assessment.
5. Evaluate the adequacy of incident response policies and contractual notification requirements in light of the risk of the outsourced activity.

Objective 6: Determine the adequacy of security monitoring.

1. Obtain an understanding of the institution's monitoring plans and activities, including both activity monitoring and condition monitoring.
2. Identify the organizational unit and personnel responsible for performing the functions of a security response center.
3. Evaluate the adequacy of information used by the security response center. Information should include external information on threats and vulnerabilities (ISAC and other reports) and internal information related to controls and activities.
4. Obtain and evaluate the policies governing security response center functions, including monitoring, classification, escalation, and reporting.
5. Evaluate the institution's monitoring plans for appropriateness given the risks of the institution's environment.
6. Where metrics are used, evaluate the standards used for measurement, the information measures and repeatability of measured processes, and appropriateness of the measurement scope.
7. Ensure that the institution utilizes sufficient expertise to perform its monitoring and testing.
8. For independent tests, evaluate the degree of independence between the persons testing security from the persons administering security.
9. Determine the timeliness of identification of vulnerabilities and anomalies, and evaluate the adequacy and timing of corrective action.
10. Evaluate the institution's policies and program for responding to unauthorized access to customer information, considering guidance in Supplement A to the Section 501(b) GLBA information security guidelines.
11. If the institution experienced unauthorized access to sensitive customer information, determine that it:
    - Conducted a prompt investigation to determine the likelihood the information accessed has been or will be misused;
    - Notified customers when the investigation determined misuse of sensitive customer information has occurred or is reasonably possible;
    - Delivered notification to customers, when warranted, by means the customer can reasonably be expected to receive, for example, by telephone, mail, or electronic mail; and
    - Appropriately notified its primary federal regulator.

Objective 7: Evaluate the effectiveness of enterprise-wide security administration.

1. Review board and committee minutes and reports to determine the level of senior

management support of and commitment to security.
2. Determine whether management and department heads are adequately trained and sufficiently accountable for the security of their personnel, information, and systems.
3. Review security guidance and training provided to ensure awareness among employees and contractors, including annual certification that personnel understand their responsibilities.
4. Determine whether security responsibilities are appropriately apportioned among senior management, front-line management, IT staff, information security professionals, and other staff, recognizing that some roles must be independent from others.
5. Determine whether the individual or department responsible for ensuring compliance with security policies has sufficient position and authority within the organization to implement the corrective action.
6. Evaluate the process used to monitor and enforce policy compliance (e.g., granting and revocation of user rights).
7. Evaluate the adequacy of automated tools to support secure configuration management, security monitoring, policy monitoring, enforcement, and reporting.
8. Evaluate management's ability to effectively control the pace of change to its environment, including the process used to gain assurance that changes to be made will not pose undue risk in a production environment. Consider the definition of security requirements for the changes, appropriateness of staff training, quality of testing, and post-change monitoring.
9. Evaluate coordination of incident response policies and contractual notification requirements.

Conclusions

Objective 8: Discuss corrective action and communicate findings.

1. Determine the need to proceed to Tier II procedures for additional validation to support conclusions related to any of the Tier I objectives.
2. Review your preliminary conclusions with the EIC regarding
   - Violations of law, rulings, regulations,
   - Significant issues warranting inclusion as matters requiring attention or recommendations in the Report of Examination,
   - Potential impact of your conclusions on composite or component IT ratings, and
   - Potential impact of your conclusions on the institution's risk assessment.
3. Discuss your findings with management and obtain proposed corrective action for significant deficiencies.
4. Document your conclusions in a memo to the EIC that provides report-ready comments for all relevant sections of the Report of Examination and guidance to future examiners.
5. Organize your work papers to ensure clear support for significant findings by examination objective.

Tier II Objectives and Procedures

The Tier II examination procedures for information security provide additional verification procedures to evaluate the effectiveness of, and identify potential root causes for weaknesses in, a financial institution's security program. These procedures are designed to assist in achieving examination objectives and may be used in their entirety or selectively, depending upon the scope of the examination and the need for additional verification. For instance, if additional verification is necessary for firewall practices, the examiner may find it necessary to select some of the procedures from the authentication, network security, host security, and physical security areas to create a customized examination procedure. Examiners should coordinate this coverage with other examiners to avoid duplication of effort while including the security issues found in other workprograms.

The procedures provided below should not be construed as requirements for control implementation. The selection of controls and control implementation should be guided by the risks facing the institution's information system. Thus, the controls necessary for any single institution or any given area of a given institution may differ from the specifics that can be inferred from the following procedures.

A. Authentication and Access Controls

Access Rights Administration

1. Evaluate the adequacy of policies and procedures for authentication and access controls to manage effectively the risks to the financial institution.
   - Evaluate the processes that management uses to define access rights and privileges (e.g., software and/or hardware systems access) and determine if they are based upon business need requirements.
   - Review processes that assign rights and privileges and ensure that they take into account and provide for adequate segregation of duties.
   - Determine whether access rights are the minimum necessary for business purposes. If greater access rights are permitted, determine why the condition exists and identify any mitigating issues or compensating controls.
   - Ensure that access to operating systems is based on either a need-to-use or an event-by-event basis.
2. Determine whether the user registration and enrollment process
   - Uniquely identifies the user,
   - Verifies the need to use the system according to appropriate policy,
   - Enforces a unique user ID,
   - Assigns and records the proper security attributes (e.g., authorization),
   - Enforces the assignment or selection of an authenticator that agrees with the security policy,
   - Securely distributes any initial shared secret authenticator or token, and
   - Obtains acknowledgement from the user of acceptance of the terms of use.
3. Determine whether employee's levels of online access (blocked, read-only, update, override, etc.) match current job responsibilities.
4. Determine that administrator or root privilege access is appropriately monitored, where appropriate.
   - Management may choose to further categorize types of administrator/root access based upon a risk assessment. Categorizing this type of access can be used to identify and monitor higher-risk administrator and root access requests that should be promptly reported.
5. Evaluate the effectiveness and timeliness with which changes in access control privileges are implemented and the effectiveness of supporting policies and procedures.
   - Review procedures and controls in place and determine whether access control privileges are promptly eliminated when they are no longer needed. Include former employees and temporary access for remote access and contract workers in the review.
   - Assess the procedures and controls in place to change, when appropriate, access control privileges (e.g., changes in job responsibility and promotion).
   - Determine whether access rights expire after a predetermined period of inactivity.
   - Review and assess the effectiveness of a formal review process to periodically review the access rights to assure all access rights are proper. Determine whether necessary changes made as a result of that review.
6. Determine that, where appropriate and feasible, programs do not run with greater access to other resources than necessary. Programs to consider include application programs, network administration programs (e.g., Domain Name System), and other programs.
7. Compare the access control rules establishment and assignment processes to the access

control policy for consistency.

8. Determine whether users are aware of the authorized uses of the system.
   - Do internal users receive a copy of the authorized-use policy, appropriate training, and signify understanding and agreement before usage rights are granted?
   - Is contractor usage appropriately detailed and controlled through the contract?
   - Do customers and Web site visitors either explicitly agree to usage terms or are provided a disclosure, as appropriate?

Authentication

1. Determine whether the financial institution has removed or reset default profiles and passwords from new systems and equipment.
2. Determine whether access to system administrator level is adequately controlled and monitored.
3. Evaluate whether the authentication method selected and implemented is appropriately supported by a risk assessment.
4. Evaluate the effectiveness of password and shared-secret administration for employees and customers considering the complexity of the processing environment and type of information accessed. Consider
   - Confidentiality of passwords and shared secrets (whether only known to the employee/ customer);
   - Maintenance of confidentiality through reset procedures;
   - The frequency of required changes (for applications, the user should make any changes from the initial password issued on enrollment without any other user's intervention);
   - Password composition in terms of length and type of characters (new or changed passwords should result in a password whose strength and reuse agrees with the security policy);
   - The strength of shared secret authentication mechanisms;
   - Restrictions on duplicate shared secrets among users (no restrictions should exist); and
   - The extent of authorized access (e.g., privileged access, single sign-on systems).
5. Determine whether all authenticators (e.g., passwords, shared secrets) are protected while in storage and during transmission to prevent disclosure.
   - Identify processes and areas where authentication information may be available in clear text and evaluate the effectiveness of compensating risk management controls.
   - Identify the encryption used and whether one-way hashes are employed to secure the clear text from anyone, authorized or unauthorized, who accesses the authenticator storage area.
6. Determine whether passwords are stored on any machine that is directly or easily accessible from outside the institution, and if passwords are stored in programs on machines which query customer information databases. Evaluate the appropriateness of such storage and the associated protective mechanisms.
7. Determine whether unauthorized attempts to access authentication mechanisms (e.g., password storage location) are appropriately investigated. Attacks on shared-secret mechanisms, for instance, could involve multiple log-in attempts using the same username and multiple passwords or multiple usernames and the same password.
8. Determine whether authentication error feedback (i.e., reporting failure to successfully log-in) during the authentication process provides prospective attackers clues that may allow them to hone their attack. If so, obtain and evaluate a justification for such feedback.
9. Determine whether adequate controls exist to protect against replay attacks and hijacking.
10. Determine whether token-based authentication mechanisms adequately protect against token tampering, provide for the unique identification of the token holder, and employ an adequate number of authentication factors.
11. Determine whether PKI-based authentication mechanisms
    - Securely issue and update keys,

- Securely unlock the secret key,
- Provide for expiration of keys at an appropriate time period,
- Ensure the certificate is valid before acceptance,
- Update the list of revoked certificates at an appropriate frequency,
- Employ appropriate measures to protect private and root keys, and
- Appropriately log use of the root key.

12. Determine that biometric systems
    - Have an adequately strong and reliable enrollment process,
    - Adequately protect against the presentation of forged credentials (e.g. address replay attacks), and
    - Are appropriately tuned for false accepts/false rejects.
13. Determine whether appropriate device and session authentication takes place, particularly for remote and wireless machines.
14. Review authenticator reissuance and reset procedures. Determine whether controls adequately mitigate risks from
    - Social engineering,
    - Errors in the identification of the user, and
    - Inability to re-issue on a large scale in the event of a mass compromise.

B. Network Security

1. Evaluate the adequacy and accuracy of the network architecture.
    - Obtain a schematic overview of the financial institution's network architecture.
    - Review procedures for maintaining current information, including inventory reporting of how new hardware are added and old hardware is removed.
    - Review audit and security reports that assess the accuracy of network architecture schematics and identify unreported systems.
2. Evaluate controls that are in place to install new or change existing network infrastructure and to prevent unauthorized connections to the financial institution's network.
    - Review network architecture policies and procedures to establish new, or change existing, network connections and equipment.
    - Identify controls used to prevent unauthorized deployment of network connections and equipment.
    - Review the effectiveness and timeliness of controls used to prevent and report unauthorized network connections and equipment.
3. Evaluate controls over the management of remote equipment.
4. Determine whether effective procedures and practices are in place to secure network services, utilities, and diagnostic ports, consistent with the overall risk assessment.
5. Determine whether external servers are appropriately isolated through placement in demilitarized zones (DMZs), with supporting servers on DMZs separate from external networks, public servers, and internal networks.
6. Determine whether appropriate segregation exists between the responsibility for networks and the responsibility for computer operations.
7. Determine whether network users are authenticated, and that the type and nature of the authentication (user and machine) is supported by the risk assessment. Access should only be provided where specific authorization occurs.
8. Determine that, where appropriate, authenticated users and devices are limited in their ability to access system resources and to initiate transactions.
9. Evaluate the appropriateness of technical controls mediating access between security domains. Consider
    - Firewall topology and architecture;
    - Type(s) of firewall(s) being utilized;
    - Physical placement of firewall components;
    - Monitoring of firewall traffic;

- Firewall updating;
- Responsibility for monitoring and updating firewall policy;
- Placement and monitoring of network monitoring and protection devices, including intrusion detection system (IDS) and intrusion prevention system (IPS) functionality; and
- Contingency planning

10. Determine whether firewall and routing controls are in place and updated as needs warrant.
    - Identify personnel responsible for defining and setting firewall rulesets and routing controls.
    - Review procedures for updating and changing rulesets and routing controls.
    - Confirm that the ruleset is based on the premise that all traffic that is not expressly allowed is denied, and that the firewall's capabilities for identifying and blocking traffic are effectively utilized.
    - Confirm that network mapping through the firewall is disabled.
    - Confirm that network address translation (NAT) and split DNS are used to hide internal names and addresses from external users.
    - Confirm that malicious code is effectively filtered.
    - Confirm that firewalls are backed up to external media, and not to servers on protected networks.
    - Determine that firewalls and routers are subject to appropriate and functioning host controls.
    - Determine that firewalls and routers are securely administered.
    - Confirm that routing tables are regularly reviewed for appropriateness on a schedule commensurate with risk.
11. Determine whether network-based IDSs are properly coordinated with firewalls (see "Security Monitoring" procedures).
12. Determine whether logs of security-related events and log analysis activities are sufficient to affix accountability for network activities, as well as support intrusion forensics and IDS. Additionally, determine that adequate clock synchronization takes place.
13. Determine whether logs of security-related events are appropriately secured against unauthorized access, change, and deletion for an adequate time period, and that reporting to those logs is adequately protected.
14. Determine whether appropriate filtering occurs for spoofed addresses, both within the network and at external connections, covering network ingress and egress.
15. Determine whether appropriate controls exist over the confidentiality and integrity of data transmitted over the network (e.g. encryption, parity checks, message authentication).
16. Determine whether appropriate notification is made of requirements for authorized use, through banners or other means.
17. Determine whether remote access devices and network access points for remote equipment are appropriately controlled.
    - Remote access is disabled by default, and enabled only by management authorization.
    - Management authorization is required for each user who accesses sensitive components or data remotely.
    - Authentication is of appropriate strength (e.g., two-factor for sensitive components).
    - Modems are authorized, configured, and managed to appropriately mitigate risks.
    - Appropriate logging and monitoring takes place.
    - Remote access devices are appropriately secured and controlled by the institution.
18. Determine whether an appropriate archive of boot disks, distribution media, and security patches exists.
19. Evaluate the appropriateness of techniques that detect and prevent the spread of malicious code across the network.

C. Host Security

1. Determine whether hosts are hardened through the removal of unnecessary software and services, consistent with the needs identified in the risk assessment, that configuration takes advantage of available object, device, and file access controls, and that necessary software updates are applied.
2. Determine whether the configuration minimizes the functionality of programs, scripts, and plug-ins to what is necessary and justifiable.
3. Determine whether adequate processes exist to apply host security updates, such as patches and anti-virus signatures, and that such updating takes place.
4. Determine whether new hosts are prepared according to documented procedures for secure configuration or replication, and that vulnerability testing takes place prior to deployment.
5. Determine whether remotely configurable hosts are configured for secure remote administration.
6. Determine whether an appropriate process exists to authorize access to host systems and that authentication and authorization controls on the host appropriately limit access to and control the access of authorized individuals.
7. Determine whether access to utilities on the host are appropriately restricted and monitored.
8. Determine whether the host-based IDSs identified as necessary in the risk assessment are properly installed and configured, that alerts go to appropriate individuals using an out-of-band communications mechanism, and that alerts are followed up. (Coordinate with the procedures listed in "Security Monitoring.")
9. Determine whether logs are sufficient to affix accountability for host activities and to support intrusion forensics and IDS and are appropriately secured for a sufficient time period.
10. Determine whether vulnerability testing takes place after each configuration change.
11. Determine whether appropriate notification is made of authorized use, through banners or other means.
12. Determine whether authoritative copies of host configuration and public server content are maintained off line.
13. Determine whether an appropriate archive of boot disks, distribution media, and security patches exists.
14. Determine whether adequate policies and procedure govern the destruction of sensitive data on machines that are taken out of service.

D. User Equipment Security (e.g. workstation, laptop, handheld)

1. Determine whether new user equipment is prepared according to documented procedures for secure configuration or replication and that vulnerability testing takes place prior to deployment.
2. Determine whether user equipment is configured either for secure remote administration or for no remote administration.
3. Determine whether adequate inspection for, and removal of, unauthorized hardware and software takes place.
4. Determine whether adequate policies and procedures exist to address the loss of equipment, including laptops and other mobile devices. Such plans should encompass the potential loss of customer data and authentication devices.
5. Determine whether adequate policies and procedures govern the destruction of sensitive data on machines that are taken out of service and that those policies and procedures are consistently followed by appropriately trained personnel.
6. Determine whether appropriate user equipment is deactivated after a period of inactivity through screen saver passwords, server time-outs, powering down, or other means.
7. Determine whether systems are appropriately protected against malicious software such as Trojan horses, viruses, and worms.

E. Physical Security

1. Determine whether physical security for information technology assets is coordinated with other security functions.
2. Determine whether sensitive data in both electronic and paper form is adequately controlled physically through creation, processing, storage, maintenance, and disposal.
3. Determine whether
   - Authorization for physical access to critical or sensitive information-processing facilities is granted according to an appropriate process;
   - Authorizations are enforceable by appropriate preventive, detective, and corrective controls; and
   - Authorizations can be revoked in a practical and timely manner.
4. Determine whether information processing and communications devices and transmissions are appropriately protected against physical attacks perpetrated by individuals or groups, as well as against environmental damage and improper maintenance. Consider the use of halon gas, computer encasing, smoke alarms, raised flooring, heat sensors, notification sensors, and other protective and detective devices.

F. Personnel Security

1. Determine whether the institution performs appropriate background checks on its personnel during the hiring process and thereafter, according to the employee's authority over the institution's systems and information.
2. Determine whether the institution includes in its terms and conditions of employment the employee's responsibilities for information security.
3. Determine whether the institution requires personnel with authority to access customer information and confidential institution information to sign and abide by confidentiality agreements.
4. Determine whether the institution provides to its employees appropriate security training covering the institution's policies and procedures, on an appropriate frequency and that institution employees certify periodically as to their understanding and awareness of the policy and procedures.
5. Determine whether employees have an available and reliable mechanism to promptly report security incidents, weaknesses, and software malfunctions.
6. Determine whether an appropriate disciplinary process for security violations exists and is functioning.

G. Application Security

1. Determine whether software storage, including program source, object libraries, and load modules, are appropriately secured against unauthorized access.
2. Determine whether user input is validated appropriately (e.g. character set, length, etc).
3. Determine whether appropriate message authentication takes place.
4. Determine whether access to sensitive information and processes require appropriate authentication and verification of authorized use before access is granted.
5. Determine whether re-establishment of any session after interruption requires normal user identification, authentication, and authorization.
6. Determine whether appropriate warning banners are displayed when applications are accessed.
7. Determine whether appropriate logs are maintained and available to support incident detection and response efforts.

H. Software Development and Acquisition

1. Inquire about how security control requirements are determined for software, whether internally developed or acquired from a vendor.

2. Determine whether management explicitly follows a recognized security standard development process, or adheres to widely recognized industry standards.
3. Determine whether the group or individual establishing security control requirements has appropriate credentials, background, and/or training.
4. Evaluate whether the software acquired incorporates appropriate security controls, audit trails, and activity logs and that appropriate and timely audit trail and log reviews and alerts can take place.
5. Evaluate whether the software contains appropriate authentication and encryption.
6. Evaluate the adequacy of the change control process.
7. Evaluate the appropriateness of software libraries and their access controls.
8. Inquire about the method used to test the newly developed or acquired software for vulnerabilities.
    - For manual source code reviews, inquire about standards used, the capabilities of the reviewers, and the results of the reviews.
    - If source code reviews are not performed, inquire about alternate actions taken to test the software for covert channels, backdoors, and other security issues.
    - Whether or not source code reviews are performed, evaluate the institution's assertions regarding the trustworthiness of the application and the appropriateness of the network and host level controls mitigating application-level risk.
9. Evaluate the process used to ascertain software trustworthiness. Include in the evaluation management's consideration of the:
    -
        - Development process
            - Establishment of security requirements
            - Establishment of acceptance criterio
            - Use of secure coding standards
            - Compliance with security requirements
            - Background checks on employees
            - Code development and testing processes
            - Signed non-disclosure agreements
            - Restrictions on developer access to production source code
            - Physical security over developer work areas
        - Source code review
            - Automated reviews
            - Manual reviews
        - Vendor or developer history and reputation
            - Vulnerability history
            - Timeliness, thoroughness, and candidness of the response to security issues
            - Quality and functionality of security patches
10. Evaluate the appropriateness of management's response to assessments of software trustworthiness:
    - Host and network control evaluation
    - Additional host and network controls

I. Business Continuity-Security

1. Determine whether adequate physical security and access controls exist over data back-ups and program libraries throughout their life cycle, including when they are created, transmitted/taken to storage, stored, retrieved and loaded, and destroyed.
    - Review the risk assessment to identify key control points in a data set's life cycle.
    - Verify controls are in place consistent with the level of risk presented.
2. Determine whether substitute processing facilities and systems undergo similar testing as production facilities and systems.
3. Determine whether appropriate access controls and physical controls have been considered

and planned for the replicated production system and networks when processing is transferred to a substitute facility.

4. Determine whether the security monitoring and intrusion response plan considers the resource availability and facility and systems changes that may exist when substitute facilities are placed in use.
5. Evaluate the procedure for granting temporary access to personnel during the implementation of contingency plans.
    - Evaluate the extent to which back-up personnel have been assigned different tasks when contingency planning scenarios are in effect and the need for different levels of systems, operational, data and facilities access.
    - Review the assignment of authentication and authorization credentials to see if they are based upon primary job responsibilities or if they also include contingency planning responsibilities. (If an employee is permanently assigned access credentials to fill in for another employee who is on vacation or out the office, this assignment would be a primary job responsibility.)

J. Service Provider Oversight-Security

1. Determine whether contracts contain security requirements that at least meet the objectives of the 501(b) guidelines and contain nondisclosure language regarding specific requirements.
2. Determine whether the institution has assessed the service provider's ability to meet contractual security requirements.
3. Determine whether appropriate controls exist over the substitution of personnel on the institution's projects and services.
4. Determine whether appropriate security testing is required and performed on any code, system, or service delivered under the contract.
5. Determine whether appropriate reporting of security incidents is required under the contract.
6. Determine whether institution oversight of third-party provider security controls is adequate.
7. Determine whether any third party provider access to the institution's system is controlled according to "Authentication and Access Controls" and "Network Security" procedures.
8. Determine whether the contract requires secure remote communications, as appropriate.
9. Determine whether the institution appropriately assessed the third party provider's procedures for hiring and monitoring personnel who have access to the institution's systems and data.
10. Determine whether the third party service provider participates in an appropriate industry ISAC.

K. Encryption

1. Review the information security risk assessment and identify those items and areas classified as requiring encryption.
2. Evaluate the appropriateness of the criteria used to select the type of encryption/ cryptographic algorithms.
    - Consider if cryptographic algorithms are both publicly known and widely accepted (e.g. RSA, SHA, Triple DES, Blowfish, Twofish, etc.) or banking industry standard algorithms.
    - Note the basis for choosing key sizes (e.g., 40-bit, 128-bit) and key space.
    - Identify management's understanding of cryptography and expectations of how it will be used to protect data.
3. Determine whether cryptographic key controls are adequate.
    - Identify where cryptographic keys are stored.

- Review security where keys are stored and when they are used (e.g., in a hardware module).
- Review cryptographic key distribution mechanisms to secure the keys against unauthorized disclosure, theft, and diversion.
- Verify that two persons are required for a cryptographic key to be used, when appropriate.
- Review audit and security reports that review the adequacy of cryptographic key controls.

4. Determine whether adequate provision is made for different cryptographic keys for different uses and data.
5. Determine whether cryptographic keys expire and are replaced at appropriate time intervals.
6. Determine whether appropriate provisions are made for the recovery of data should a key be unusable.
7. Determine whether cryptographic keys are destroyed in a secure manner when they are no longer required.

L. Data Security

1. Obtain an understanding of the data security strategy.
   - Identify the financial institution's approach to protecting data (e.g., protect all data similarly, protect data based upon risk of loss).
   - Obtain and review the risk assessment covering financial institution data. Determine whether the risk assessment classifies data sensitivity in a reasonable manner and consistent with the financial institution's strategic and business objectives.
   - Consider whether policies and procedures address the protections for data that is sent outside the institution.
   - Identify processes to periodically review data sensitivity and update corresponding risk assessments.
2. Verify that data is protected consistent with the financial institution's risk assessment.
   - Identify controls used to protect data and determine if the data is protected throughout its life cycle (i.e., creation, storage, maintenance, transmission, and disposal) in a manner consistent with the risk assessment.
   - Consider data security controls in effect at key stages such as data creation/acquisition, storage, transmission, maintenance, and destruction.
   - Review audit and security review reports that summarize if data is protected consistent with the risk assessment.
3. Determine whether individual and group access to data is based on business needs.
4. Determine whether, where appropriate, the system securely links the receipt of information with the originator of the information and other identifying information, such as date, time, address, and other relevant factors.

M. Security Monitoring

1. Identify the monitoring performed to identify non-compliance with institution security policies and potential intrusions.
   - Review the schematic of the information technology systems for common security monitoring devices.
   - Review security procedures for report monitoring to identify unauthorized or unusual activities.
   - Review management's self-assessment and independent testing activities and plans.
2. Determine whether users are appropriately notified regarding security monitoring.
3. Determine whether the activity monitoring sensors identified as necessary in the risk assessment process are properly installed and configured at appropriate locations.

4. Determine whether an appropriate firewall ruleset and routing controls are in place and updated as needs warrant.
    - Identify personnel responsible for defining and setting firewall rulesets and routing controls.
    - Review procedures for updating and changing rulesets and routing controls.
    - Determine that appropriate filtering occurs for spoofed addresses, both within the network and at external connections, covering network entry and exit.
5. Determine whether logs of security-related events are sufficient to support security incident detection and response activities, and that logs of application, host, and network activity can be readily correlated.
6. Determine whether logs of security-related events are appropriately secured against unauthorized access, change, and deletion for an adequate time period, and that reporting to those logs is adequately protected.
7. Determine whether logs are appropriately centralized and normalized, and that controls are in place and functioning to prevent time gaps in logging.
8. Determine whether an appropriate process exists to authorize employee access to security monitoring and event management systems and that authentication and authorization controls appropriately limit access to and control the access of authorized individuals.
9. Determine whether appropriate detection capabilities exist related to
    - Network related anomalies, including
        - Blocked outbound traffic
        - Unusual communications, including communicating hosts, times of day, protocols, and other header-related anomalies
        - Unusual or malicious packet payloads
    - Host-related anomalies, including
        - System resource usage and anomalies
        - User related anomalies
        - Operating and tool configuration anomalies
        - File and data integrity problems
        - Anti-virus, anti-spyware, and other malware identification alerts
        - Unauthorized access
        - Privileged access
10. Evaluate the institution's self-assessment plan and activities, including
    - Policies and procedures conformance
    - Service provider oversight
    - Vulnerability scanning
    - Configuration verification
    - Information storage
    - Risk assessment and monitoring plan review
    - Test reviews
11. Evaluate the use of metrics to measure
    -
        - Security policy implementation
        - Security service delivery effectiveness and efficiency
        - Security event impact on business process
12. Evaluate independent tests, including penetration tests, audits, and assessments. Consider:
    - Personnel
    - Scope
    - Controls over data integrity, confidentiality, and availability
    - Confidentiality of test plans and data
    - Frequency
13. Determine that the functions of a security response center are appropriately governed by implemented policies addressing
    - Monitoring

- Classification
- Escalation
- Reporting
- Intrusion declaration

14. Determine whether an intrusion response team
    - Contains appropriate membership;
    - Is available at all times;
    - Has appropriate training to investigate and report findings;
    - Has access to back-up data and systems, an inventory of all approved hardware and software, and monitored access to systems (as appropriate);
    - Has appropriate authority and timely access to decision makers for actions that require higher approvals; and
    - Have procedures for submitting appropriate incidents to the industry ISAC.
15. 1Evaluate the appropriateness of the security policy in addressing the review of compromised systems. Consider
    - Documentation of the roles, responsibilities and authority of employees and contractors, and
    - Conditions for the examination and analysis of data, systems, and networks.
16. Determine whether the information disclosure policy indicates what information is shared with others, in what circumstances, and identifies the individual(s) who have the authority to initiate disclosure beyond the stated policy.
17. Determine whether the information disclosure policy addresses the appropriate regulatory reporting requirements.
18. Determine whether the security policy provides for a provable chain of custody for the preservation of potential evidence through such mechanisms as a detailed action and decision log indicating who made each entry.
19. Determine whether the policy requires all compromised systems to be restored before reactivation, through either rebuilding with verified good media or verification of software cryptographic checksums.
20. Determine whether all participants in security monitoring and intrusion response are trained adequately in the detection and response policies, their roles, and the procedures they should take to implement the policies.\
21. Determine whether response policies and training appropriately address unauthorized disclosures of customer information, including
    - Identifying the customer information and customers effected;
    - Protecting those customers through monitoring, closing, or freezing accounts;
    - Notifying customers when warranted; and
    - Appropriately notifying its primary federal regulator
22. Determine whether an effective process exists to respond in an appropriate and timely manner to newly discovered vulnerabilities. Consider
    - Assignment of responsibility
    - Prioritization of work to be performed
    - Appropriate funding
    - Monitoring, and
    - Follow-up activities

Appendix B: Glossary

ACL - Access control list.

Applet - A small program that typically is transmitted with a Web page.

AUP - An acceptable use policy. It documents permitted system uses and activities for a specific user and the consequences of noncompliance.

Authentication - The process of verifying the identity of an individual user, machine, software component, or any other entity.

Authorization - The process of giving access to parts of a system, typically based on the business needs and the role of the individual within the business.

Cookie - A message given by a Web server to a Web browser, stored by the Web browser, and returned to the Web server when requested.

Dictionary Attack - Discovery of authenticators by encrypting likely authenticators and comparing the actual encrypted authenticator with the newly encrypted possible authenticators.

Encryption - The conversion of information into a code or cipher.

Exploit - A technique or code that uses a vulnerability to provide system access to the attacker.

FS/ISAC - Financial Services Information Sharing and Analysis Center.

Full-Duplex - A communications channel that carries data in both directions.

Hardening - Decreasing the capability of a device to the minimum required for its intended purpose.

Hash - A fixed length cryptographic output of variables, such as a message, being operated on by a formula or cryptographic algorithm.

Hijacking - The use of an authenticated user's communication session to communicate with system components.

Host - A computer that is accessed by a user from a remote location.

I/O - Input/Output.

IDS - Intrusion Detection System.

IPS - Intrusion Prevention System.

IPv6 - Version 6 of the Internet Protocol.

ISAC - Information Sharing and Analysis Center.

ISO - International Organization for Standards.

Man-In-The-Middle Attack - A man-in-the-middle attack places the attacker's computer in the communication line between the server and the client. The attacker's machine can monitor and change communications.

Media - Physical objects that store data, such as paper, hard disk drives, tapes, and compact disks (CDs).

Non-Repudiation - Ensuring that a transferred message has been sent and received by the parties claiming to have sent and received the message. Non-repudiation is a way to guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message.

P2P - Peer-to-peer communication, the communications that travel from one user's computer to another user's computer without being stored for later access on a server. E-mail is not a P2P communication since it travels from the sender to a server, and is retrieved by the recipient from the server. On-line chat, however, is a P2P communication since messages travel directly from one user to another.

Patch - Software code that replaces or updates other code. Frequently patches are used to correct security flaws.

Port - Either an endpoint to a logical connection or a physical connection to a computer.

Protocol - A format for transmitting data between devices.

Replay Attack - The interception of communications, such as an authentication communication, and subsequently impersonation of the sender by retransmitting the intercepted communication.

Routing - The process of moving information from its source to the destination.

Security Event - An event that compromises the confidentiality, integrity, availability, or accountability of an information system.

Server - A computer or other device that manages a network service. An example is a print server, a device that manages network printing.

Sniffing - The passive interception of data transmissions.

Social Engineering - Obtaining information from individuals by trickery.

Spoofing - A form of masquerading where a trusted IP address is used instead of the true IP address as a means of gaining access to a computer system.

Stateful Inspection - A firewall inspection technique that examines the claimed purpose of a communication for validity. For example, a communication claiming to respond to a request is compared to a table of outstanding requests.

System Resources - Capabilities that can be accessed by a user or program either on the user's machine or across the network. Capabilities can be services, such as file or print services, or devices, such as routers.

Trojan Horse - Malicious code that is hidden in software that has an apparently beneficial or

harmless use.

Utility - A program used to configure or maintain systems, or to make changes to stored or transmitted data.

Virus - Malicious code that replicates itself within a computer.

VLAN - Virtual local area network.

Vulnerability - A flaw that allows a person to operate a computer system with authorization in excess of that which the system owner specifically granted to him or her.

Warehouse Attack - The compromise of systems that store authenticators.

Worm - Malicious code that infects computers across a network without user intervention.

Appendix C: Laws, Regulations, and Guidance

Laws

- 12 USC 1867(c): Bank Service Company Act ()
- 12 USC 1882: Bank Protection Act ()
- 15 USC 1681w: Fair and Accurate Credit Transactions Act ()
- 15 USC 6801 and 6805(b): Gramm-Leach-Bliley Act ()
- 18 USC 1030: Fraud and Related Activity in Connection with Computers ()
- USA Patriot Act ()

Federal Reserve Board

- 12 CFR 208.61: Minimum Security Devices and Procedures (N/A)
- 12 CFR 208.62: Reports of Suspicious Activities (N/A)
- 12 CFR 208.63: Procedures for Monitoring Bank Secrecy Act Compliance (N/A)
- 12 CFR 208, Appendix D-1: Interagency Guidelines Establishing Standards for Safety and Soundness (N/A)
- 12 CFR 208, Appendix D-2: Interagency Guidelines Establishing Standards for Safeguarding Customer Information (N/A)
- 12 CFR 211.5 (1): Interagency Guidelines Establishing Standards for Safeguarding Customer Information (Edge or agreement corporation) (N/A)
- 12 CFR 211.24 (i): Interagency Guidelines Establishing Standards for Safeguarding Customer Information (N/A)
- 12 CFR 225 Appendix F: Interagency Guidelines Establishing Standards for Safeguarding Customer Information (N/A)
- SR Letter 05-23 Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice (December 1, 2005)
- SR Letter 05-19 Interagency Guidance on Authentication in an Internet Banking Environment (October 13, 2005)
- SR Letter 04-17 FFIEC Guidance on the use of Free and Open Source Software (December 6, 2004)
- SR Letter 04-14 FFIEC Brochure with Information on Internet "Phishing" (October 19, 2004)
- SR Letter 02-18 Section 312 of the USA Patriot Act--Due Diligence for Correspondent and Private Banking Accounts (July 23, 2002)
- SR Letter 02-6 Information Sharing Pursuant to Section 314(b) of the USA Patriot Act (March 14, 2002)
- SR Letter 01-15 Safeguarding Customer Information (May 31, 2001)
- SR Letter 01-11 Identity Theft and Pretext Calling (April 26, 2001)
- SR Letter 00-17 Guidance on the Risk Management of Outsourced Technology Services (November 30, 2000)
- SR Letter 00-04 Outsourcing of Information and Transaction Processing (February 29, 2000)
- SR Letter 99-08 Uniform Rating System for Information Technology (March 31, 1999)
- SR Letter 97-32 Sound Practices Guidance for Information Security for Networks (December 4, 1997)

Federal Deposit Insurance Corporation

- 12 CFR 326, subpart A: Minimum Security Procedures (N/A)
- 12 CFR 326, subpart B: Procedures for Monitoring Bank Secrecy Act Compliance (N/A)
- 12 CFR 332: Privacy of Consumer Financial Information (N/A)
- 12 CFR 353: Suspicious Activity Reports (N/A)
- 12 CFR 364, appendix A: Interagency Guidelines Establishing Standards for Safety and Soundness (N/A)
- 12 CFR 364, appendix B: Interagency Guidelines Establishing Standards for Safeguarding Customer Information (N/A)
- FIL-103-2005: FFIEC Guidance Authentication in an Internet Banking Environment (October 12, 2005)
- FIL-66-2005: Spyware - Guidance on Mitigating Risks From Spyware (July 22, 2005)
- FIL-64-2005: "Pharming" - Guidance on How Financial Institutions can Protect against Pharming Attacks (July 18, 2005)
- FIL-59-2005: Identity Theft Study Supplement on "Account Hijacking Identity Theft" (July 5, 2005)
- FIL-46-2005: Pre-Employment Background Screening: Guidance on Developing an Effective Pre-Employment Background Screening Process (June 1, 2005)
- FIL-27-2005: Final Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice (April 1, 2005)
- FIL-7-2005: Fair and Accurate Credit Transactions Act of 2003 Guidelines Requiring the Proper Disposal of Customer Information (February 2, 2005)
- FIL-132-2004: Identity Theft Study on "Account Hijacking" Identity Theft and Suggestions for Reducing Online Fraud (December 14, 2004)
- FIL-121-2004: Computer Software Due Diligence - Guidance on Developing an Effective Software Evaluation Program to Assure Quality and Regulatory Compliance (November 16, 2004)
- FIL-114-2004: Risk Management of Free and Open Source Software FFIEC Guidance (October 21, 2004)
- FIL-103-2004: Interagency Informational Brochure on Internet "Phishing" Scams (September 13, 2004)
- FIL-84-2004: Guidance on Instant Messaging (July 21, 2004)
- FIL-62-2004: Guidance on Developing and Effective Computer Virus Protection Program (June 7, 2004)
- FIL-27-2004: Guidance on Safeguarding Customers Against E-Mail and Internet Related Fraud Schemes (March 12, 2004)
- FIL-63-2003: Guidance on Identity Theft Response Programs, FIL-63-2003 (August 13, 2003)
- FIL-43-2003: Guidance on Developing an Effective Software Patch Management Program (May 29, 2003)
- FIL-8-2002: Wireless Networks And Customer Access (February 1, 2002)
- FIL-69-2001: Authentication In An Electronic Banking Environment (August 24, 2001)
- FIL-68-2001: 501(b) Examination Guidance (August 24, 2001)
- FIL-39-2001: Guidance on Identity Theft and Pretext Calling (May 9, 2001)
- FIL-22-2001: Security Standards for Customer Information (March 14, 2001)
- FIL-77-2000: Bank Technology Bulletin: Protecting Internet Domain Names (November 9, 2000)
- FIL-67-2000: Security Monitoring of Computer Networks (October 3, 2000)
- Risk Assessment Tools and Practices, FIL-68-99 (July 1999)
- FIL-98-98: Pretext Phone Calling (September 2, 1998)
- FIL-131-97: Security Risks Associated with the Internet (December 18, 1997)
- FIL-124-97: Suspicious Activity Reporting (December 5, 1997)

- FIL-48-2000: Suspicious Activity Reports (July 14, 2000)
- FIL-82-96: Risks Involving Client/Server Computer Systems (October 8, 1996)

National Credit Union Administration

- 12 CFR 721: Federal Credit Union Incidental Powers Activities (N/A)
- 12 CFR 748: Security Program, Report of Crime and Catastrophic Act and Bank Secrecy Act Compliance and Appendix (N/A)
- 12 CFR 716: Privacy of Consumer Financial Information, and Appendix (N/A)
- 12 CFR 741: Requirements for Insurance (N/A)
- NCUA Letter to Credit Unions 05-CU-20: Phishing Guidance for Credit Unions and Their Members (December 2005)
- NCUA Letter to Credit Unions 05-CU-18: Guidance on Authentication in Internet Banking Environment (November 2005)
- NCUA Letter to Credit Unions 04-CU-12: Phishing Guidance for Credit Union Members (September 2004)
- NCUA Letter to Credit Unions 04-CU-06: E-Mail and Internet Related Fraudulent Schemes Guidance (April 2004)
- NCUA Letter to Credit Unions 04-CU-05: Fraudulent E-Mail Schemes (April 2004)
- NCUA Letter to Credit Unions 03-CU-14: Computer Software Patch Management (September 2003)
- NCUA Letter to Credit Unions 03-CU-12: Fraudulent Newspaper Advertisements, and Websites by Entities Claiming to be Credit Unions (August 2003)
- NCUA Letter to Credit Unions 03-CU-08: Weblinking: Identifying Risks & Risk Management Techniques (April 2003)
- NCUA Letter to Credit Unions 03-CU-03: Wireless Technology (February 2003)
- NCUA Letter to Federal Credit Unions 02-FCU-11: Tips to Safely Conduct Financial Transactions Over the Internet (July 2002)
- NCUA Letter to Credit Unions 02-CU-13: Vendor Information Systems & Technology Reviews - Summary Results (July 2002)
- NCUA Letter to Credit Unions 02-CU-08: Account Aggregation Services (April 2002)
- NCUA Letter to Federal Credit Unions 02-FCU-04: Weblinking Relationships (March 2002)
- NCUA Letter to Credit Unions 01-CU-21: Disaster Recovery and Business Resumption Contingency Plans (December 2001)
- NCUA Letter to Credit Unions 01-CU-20: Due Diligence Over Third Party Service Providers (November 2001)
- NCUA Letter to Credit Unions 01-CU-12: E-Commerce Insurance Considerations (October 2001)
- NCUA Letter to Credit Unions 01-CU-09: Identity Theft and Pretext Calling (September 2001)
- NCUA Letter to Credit Unions 01-CU-11: Electronic Data Security Overview (August 2001)
- NCUA Letter to Credit Unions 01-CU-10: Authentication in an Electronic Banking Environment (August 2001)
- NCUA Letter to Credit Unions 01-CU-04: Integrating Financial Services and Emerging Technology, NCUA Letter to Credit Unions 01-CU-04 (March 2001)
- NCUA Regulatory Alert 01-RA-03: Electronic Signatures in Global and National Commerce Act (March 2001)
- NCUA Letter to Credit Unions 01-CU-02: Privacy of Consumer Financial Information (February 2001)
- NCUA Letter to Credit Unions 00-CU-11: Risk Management of Outsourced Technology Services (December 2000)
- NCUA Letter to Credit Unions 00-CU-11: NCUA's Information Systems & Technology Examination Program (October 2000)

- NCUA Letter to Credit Unions 00-CU-04: Suspicious Activity Reporting (July 2000)
- NCUA Letter to Credit Unions 00-CU02: Identity Theft Prevention, NCUA Letter to Credit Unions 00-CU-02 (May 2000)
- NCUA Regulatory Alert 99-RA-3: Pretext Phone Calling by Account Information Brokers (February 1999)
- NCUA Regulatory Alert 98-RA-4: Interagency Guidance on Electronic Financial Services and Consumer Compliance (July 1998)
- NCUA Letter to Credit Unions 97-CU-5: Interagency Statement on Retail On-line PC Banking (April 1997)
- Automated Response System Controls (January 1997)
- NCUA Letter to Credit Unions 109: Information Processing Issues (September 1989)

Office of the Comptroller of the Currency

- 12 CFR, 21, Subpart A: Minimum Security Devices and Procedures (N/A)
- 12 CFR, 21, Subpart B: Reports of Suspicious Activities (N/A)
- 12 CFR, 21, Subpart C: Procedures for Monitoring Bank Secrecy Act Compliance (N/A)
- 12 CFR, 30, Appendix A: Interagency Guidelines Establishing Standards for Safety and Soundness (N/A)
- 12 CFR, 30, Appendix B: Interagency Guidelines Establishing Information Security (N/A)
- OCC Bulletin 2011-26: Authentication in an Internet Environment - Supplement (June 28, 2011)
- OCC Bulletin 2005-35; Authentication in an Internet Banking Environment (October 12, 2005)
- OCC Bulletin 2005-24: Threats from Fraudulent Bank Web Sites (July 1, 2005)
- OCC Bulletin 2005-13: Response Programs for Unauthorized Access to Customer Information and Customer Notice: Final Guidance (April 14, 2005)
- OCC Bulletin 2005-1: Proper Disposal of Consumer Information (January 12, 2005)
- OCC Bulletin 2003-27: Suspicious Activity Report (June 24, 2003)
- OCC Advisory 2003-10: Risk Management of Wireless Networks (December 9, 2003)
- OCC Alert 2003-11: Customer Identity Theft: E-Mail-Related Fraud Threats (September 12, 2003)
- OCC Bulletin 2001-47: Third Party Relationships (November 1, 2001)
- OCC Bulletin 2001-35: Examination Procedures for Guidelines to Safeguard Customer Information (July 18, 2001)
- OCC Alert 2001-04: Network Security Vulnerabilities (April 24, 2001)
- OCC Bulletin 2001-12: Bank Provided Account Aggregation Services (February 28, 2001)
- OCC Bulletin 99-20: Certificate Authority Guidance (May , 1999)
- OCC Bulletin 2001-8: Guidelines Establishing Standards for Safeguarding Customer Information (February 15, 2001)
- OCC Alert 2000-9: Protecting Internet Addresses of National Banks (July 19, 2000)
- OCC Bulletin 2000-19: Suspicious Activity Report (June19, 2000)
- OCC Bulletin 2000-14: Infrastructure Threats-Intrusion Risks (May 15, 2000)
- OCC Alert 2000-1: Internet Security: Distributed Denial of Service Attacks (February 11, 2000)
- OCC Advisory Letter 2000-12: Risk Management of Outsourcing Technology Services (November 28, 2000)
- OCC Bulletin 98-3: Technology Risk Management (February 4, 1998)
- OCC Bulletin 98:38 Technology Risk Management: PC Banking (August 24, 1998)

Office of Thrift Supervision

- 12 CFR Part 555: Electronic Operations (N/A)

- 12 CFR 563.177: Procedures for Monitoring Bank Secrecy Act Compliance (N/A)
- 12 CFR 563.180: Suspicious Activity Reports and Other Reports and Statements (N/A)
- 12 CFR 568: Security Procedures Under the Bank Protection Act (N/A)
- 12 CFR 570 Appendix A: Interagency Guidelines Establishing Standards for Safety and Soundness (N/A)
- 12 CFR 570 Appendix B: Interagency Guidelines Establishing Information Security Standards (N/A)
- 12 CFR 573: Privacy of Consumer Financial Information (N/A)
- CEO Ltr 97: Policy Statement on Privacy and Accuracy of Customer Information and Interagency Pretext Phone Calling Memorandum (November 3, 1998)
- CEO Ltr 109: Transactional Web Sites (June 10, 1999)
- CEO Ltr 125: Privacy Rule (Transmits final rule for Privacy of Consumer Financial Information) (June 1, 2000)
- CEO Ltr 139: Identity Theft and Pretext Calling (May 4, 2001)
- CEO Ltr 155: Interagency Guidance: Privacy of Consumer Financial Information (February 11, 2002)
- CEO Ltr 193: 'Phishing' and E-Mail Scams (March 8, 2004)
- CEO Ltr 214: Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice (March 30, 2005)
- CEO Ltr 228: Interagency Guidance on Authentication in an Internet Banking Environment (October 12, 2005)
- CEO Ltr 231: Compliance Guide- Interagency Guidelines Establishing Information Security Standards (December 14, 2005)
- CEO Ltr 237: Interagency Advisory on Influenza Pandemic Preparedness (March 15, 2006)
- Thrift Activities Handbook, Section 341: Technology Risk Controls (January 2002)

External Resources

- Control Objectives for Information Technology Website at www.isaca.org (The Information Systems Audit and Control Association & Foundation) (N/A)
- Code of Practice for Information Security Management (ISO /IEC 17799) (available at The International Organization for Standards (ISO) Information Technology Website, www.iso.org/iso/en/CatalogueListPage.CatalogueList) (September 2001)
- Information Security -- Security Techniques-Evaluation Criteria for IT Security (ISO /IEC 15408) (available at The International Organization for Standards (ISO) Information Technology Website, www.iso.org/iso/en/CatalogueListPage.CatalogueList) (December 1999)
- Guidelines on Firewalls and Firewall Policy, Special Publication 800-41 (January 2002)
- Risk Management Guide for Information Technology Systems, Special Publication 800-30 (October 2001)
- The National Institute of Standards and Technology (NIST) Website at www.nist.gov (N/A)