Federal Financial Institutions Examination Council

FFIEC

Information Security

IS

December 2002

IT Examination Handbook

TABLE OF CONTENTS

INTRODUCTION 1
Overview 1
Security Objectives 2
Regulatory Guidance, Resources, and Standards 3

SECURITY PROCESS 4
Overview 4
Roles and Responsibilities 5

INFORMATION SECURITY RISK ASSESSMENT 7
Overview 7
Key Steps 8
Information Gathering 8
Analyze Information 9
Prioritize Responses 11
Key Risk Assessment Practices 11

INFORMATION SECURITY STRATEGY 13

SECURITY CONTROLS IMPLEMENTATION 15
Logical and Administrative Access Control 15
Access Rights Administration 15
Authentication 18
Network Access 27
Operating System Access 39
Application Access 41
Remote Access 43
Physical Security 44
Data Center Security 45
Cabinet and Vault Security 46
Physical Security in Distributed IS Environments 46
Encryption 48
How Encryption Works 49
Encryption Key Management 50
Encryption Types 51

Examples of Encryption Uses 52
Malicious Code 53
Controls to Protect Against Malicious Code 54
Systems Development, Acquisition, and Maintenance 55
Software Development and Acquisition 56
Host and User Equipment Acquisition and Maintenance 58
Personnel Security 60
Background Checks and Screening 61
Agreements: Confidentiality, Non-disclosure, and Authorized Use 61
Job descriptions 62
Training 62
Electronic and Paper-Based Media Handling 62
Handling and Storage 63
Disposal 63
Transit 64
Logging and Data Collection 64
Service Provider Oversight 66
SAS 70 Reports 67
Intrusion Detection and Response 68
Intrusion Detection 68
Intrusion Response 73
Business Continuity Considerations 75
Insurance 75

SECURITY TESTING 78
Testing Concepts and Application 78
Independent Diagnostic Tests 80
Key Factors 80
Outsourced Systems 81

MONITORING AND UPDATING 82
Monitoring 82
Updating 83

APPENDIX A: EXAMINATION PROCEDURES A-1

APPENDIX B: GLOSSARY B-1

APPENDIX C: LAWS, REGULATIONS, AND GUIDANCE C-1

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. 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 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. Individual financial institutions and their service providers must maintain effective security programs adequate for their operational complexity. These security programs must have strong board and senior management level support, integration of security responsibilities 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 determining 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.

Member agencies of the Federal Financial Institutions Examination Council (FFIEC) defined such a process-based approach to security in the "Guidelines Establishing Standards to Safeguard Customer Information" to implement section 501(b) of the Gramm–Leach–Bliley Act of 1999 (GLBA)[1]. The guidelines afford the FFIEC 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

[1] See Appendix C for a listing of laws, regulations, and agency guidance.

aspects of the financial institution's operations, and serves as a supplement to agency GLBA 501(b) expectations.

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.

This booklet is one of a series of updates to the *1996 FFIEC Information Systems Examination Handbook*. It updates and rescinds the security-related guidance in that handbook, including Chapters 12-14.

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. [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 and/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, intrusion detection, 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

[2] Underlying Models for IT Security, NIST, draft 0.2, May 15, 2001, p. 4.

provide the intended functionality while preventing undesired actions.

Appropriate security controls are necessary for financial institutions to challenge potential customer or user claims that they did not initiate a transaction. Financial institutions can accomplish this by achieving both integrity and accountability 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[3].

REGULATORY GUIDANCE, RESOURCES, AND STANDARDS

Financial institutions developing or reviewing their information security controls, policies, procedures, or processes have a variety of sources to draw upon. First, federal laws and regulations address security, and regulators have issued numerous security related guidance documents.[4] 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 at www.iso.ch with specific standards such as
  - The code of practice for information security management (ISO/IEC 17799) and
  - Information Security -- 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.

[3] The federal E-Sign Act, 15 USC 7001, et. Seq., does not resolve this issue.

[4] See Appendix B for a listing of laws, regulations, and agency guidance.

SECURITY PROCESS

Action Summary

- Financial institutions should implement an ongoing security process, and assign 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 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 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 assurance that management and staff understand their responsibilities and have the knowledge, skills, and motivation necessary to fulfill their duties.
- *Security Testing*—The use of various methodologies to gain assurance that risks are appropriately assessed and mitigated. These testing methodologies should verify that significant controls are effective and performing as intended.
- *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.

ROLES AND RESPONSIBILITIES

Information security is the responsibility of everyone at the institution, as well as the institution's service providers and contractors. The board, management, and employees all have different roles in developing and implementing an effective security process.

The board of directors is responsible for overseeing the development, implementation, and maintenance of the institution's information security program. Oversight requires the board to provide management with guidance and receive reports on the effectiveness of management's response. The board should approve written information security policies and the information security program at least annually. The board should provide management with its expectations and requirements for

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

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 designate one or more individuals as information security officers. Security officers should be responsible and accountable for security administration. At a minimum, they should directly manage or oversee risk assessment, development of policies, standards, and procedures, testing, and security reporting processes. Security officers should have the authority to respond to a security event[5] 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 throughout the institution from the IT department to various lines of business depending on the institution's size, complexity, culture, nature of operations, and other factors. The

[5] A security event occurs when the confidentiality, integrity, availability, or accountability of an information system is compromised.

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, and
- Coordinate information security with physical security.

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.

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, employee certifications of compliance, self-assessments, audits, and monitoring.

Management also should consider the roles and responsibilities of external parties. Technology service providers (TSPs), contractors, customers, and others who have access to the institution's systems and data should have their security responsibilities clearly delineated and documented in contracts.

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 its assets; and
- Prioritizes the risks present due to threats and vulnerabilities to determine the appropriate level of training, controls, and testing necessary for effective mitigation.

OVERVIEW

The quality of security controls can significantly influence all categories of risk.[6] Traditionally, examiners and bankers recognize 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 in the future. Effective application access controls can reduce credit and market risk by imposing risk limits on loan officers or traders. 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 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 im-

[6] 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.

portant 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. 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 necessary 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 should also consider the risk to their customers' information. For example, section 501(b) of the GLBA requires 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.

INFORMATION GATHERING

Identifying and understanding risk requires the analysis of a wide range of information relevant to the particular institution's risk environment. Once gathered, the information can be catalogued to facilitate later analysis. Information gathering generally includes the following actions:

- Obtaining listings of information system assets (e.g., data, software, and hardware). Inventories on a device-by-device basis can be helpful in risk assessment as well as risk mitigation. Inventories should consider whether data resides in house or at a TSP.
- Determining threats to those assets, resulting from people with malicious intent,[7] employees and others who accidentally cause damage, and environmental problems that are outside the control of the organization (e.g., natural disasters, failures of interdependent infrastructures such as power, telecommunications, etc.).

[7] Examples include low-skilled attackers who use programs created by others in order to intrude on the institution's systems, and experts employed by organized crime and nation-states. The greatest volume of attacks are associated with low-skilled attackers that use attack programs created by others.

- Identifying organizational vulnerabilities (e.g., weak senior management support, ineffective training, inadequate expertise or resource allocation, and inadequate policies, standards, or procedures).
- Identifying technical vulnerabilities (e.g., vulnerabilities in hardware and software, configurations of hosts, networks, workstations, and remote access).
- Documenting current controls and security processes, including both information technology and physical security.
- Identifying security requirements and considerations (e.g., GLBA).
- Maintaining the risk assessment process requires institutions to review and update their risk assessment at least once a year, or more frequently in response to material changes in any of the six actions above.

ANALYZE INFORMATION

The information gathered is used to characterize the system, to identify and measure threats to the system and the data it contains and transmits, and to estimate the likelihood that a threat will take action against the system or data.

System characterization articulates the understanding of the system, including the boundaries of the system being assessed, the system's hardware and software, and the information that is stored, processed, and transmitted. Since operational systems may have changed since they were last documented, a current review of the system should be performed. Developmental systems, on the other hand, should be analyzed to determine their key security rules and attributes.[8] Those rules and attributes should be documented as part of the systems development lifecycle process. System characterization also requires the cross-referencing of vulnerabilities to current controls to identify those that mitigate specific threats, and to assist in highlighting the control areas that should be improved.

A key part of system characterization is the ranking of data and system components according to their sensitivity and importance to the institution's operations. Additionally, consistent with the GLBA, the ranking should consider the potential harm to customers of unauthorized access and disclosure of customer non-public personal information. Ranking allows for a reasoned and measured analysis of the relative outcome of various attacks, and the limiting of the analysis to sensitive information or information and systems that may materially affect the institution's condition and operations.

Threats are identified and measured through the creation and analysis of threat scenarios. Threat scenarios should be comprehensive in their scope (e.g., they should consider reasonably foreseeable threats and possible attacks against information and systems that may affect the institution's condition and operations or may cause data disclosures that could

[8] NIST Special Publication 800-30, Risk Management Guide

result in substantial harm or inconvenience to customers). They should consider the potential effect and likelihood for failure within the control environment due to non-malicious or malicious events. They should also be coordinated with business continuity planning to include attacks performed when those plans are implemented. Non-malicious scenarios typically involve accidents related to inadequate access controls and natural disasters. Malicious scenarios, either general or specific, typically involve a motivated attacker (i.e., *threat*) exploiting a *vulnerability* to gain access to an *asset* to create an *outcome* that has an *impact*.

An example of a general malicious threat scenario is an unskilled attacker using a program script to exploit a vulnerable Internet-accessible Web server to extract customer information from the institution's database. Assuming the attacker's motivation is to seek recognition from others, the attacker publishes the information, causing the financial institution to suffer damage to its reputation. Ultimately, customers are likely to be victims of identity theft.

Since specific scenarios can become too numerous for financial institutions to address individually, various techniques are used to generalize and extend the scenarios. For instance, one technique starts with a specific scenario and looks at additional damage that could occur if the attacker had different knowledge or motivation. This technique allows the reviewers to see the full extent of risk that exists from a given vulnerability. Another technique aggregates scenarios by high-value system components.

Scenarios should consider attacks against the logical security, physical security, and combinations of logical and physical attacks. In addition, scenarios could consider social engineering, which involves manipulation of human trust by an attacker to obtain access to computer systems. It is often easier for an attacker to obtain access through manipulation of one or more employees than to perform a logical or physical intrusion.

The risk from any given scenario is a function of the probability of the event occurring and the impact on the institution. The probability and impact are directly influenced by the financial institution's business profile, the effectiveness of the financial institution's controls, and the relative strength of controls when compared to other industry targets[9].

The probability of an event occurring is reflected in one of two ways. If reliable and timely probability data is available, institutions can use it. Since probability data is often limited, institutions can assign a qualitative probability, such as frequent, occasional, remote, and improbable.

Frequently, TSPs perform some or all of the institution's information processing and storage. Reliance on a third party for hosting systems or processing does not remove the institution's responsibility for securing the information. It does change how the financial institution will fulfill its role. Accordingly, risk assessments should evaluate the sensitiv-

[9] An attack on the financial institution industry in general may be targeted at the organizations with the weakest controls. Alternatively, an attack scenario postulating an attack on a particular institution would not consider the strength of another institution's controls.

ity of information accessible to or processed by TSPs, the importance of the processing conducted by TSPs, communications between the TSP's systems and the institution, contractually required controls, and the testing of those controls. Additional vendor management guidance is contained in the FFIEC's statement on "Risk Management of Outsourced Technology Services," dated November 28, 2000.

PRIORITIZE RESPONSES

This phase ranks the risk (outcomes and probabilities) presented by various scenarios produced in the analysis phase to prioritize management's response. Management may decide that since some risks do not meet the threshold set in their security requirement, they will accept those risks and not proceed with a mitigation strategy. Other risks may require immediate corrective action. Still others may require mitigation, either fully or partially, over time. Risks that warrant action are addressed in the information security strategy.

In some borderline instances, or if planned controls cannot fully mitigate the risk, management may need to review the risk assessment and risk ranking with the board of directors or a delegated committee. The board should then document its acceptance of the risk or authorize other risk mitigation measures.

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 followed by the institution requires the involvement of a broad range of users, with a 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, that organization will likely be the business unit. The information security officer(s) 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. Documentation of the analysis and results provides a useful starting point for subsequent assessments, potentially reducing the effort required in those assessments. Documentation of risks accepted and risk mitigation decisions is fundamental to achieving 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 are 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

- Cost comparisons of different strategic approaches appropriate to the institution's environment and complexity,
- Layered controls that establish multiple control points between threats and organization assets, and
- Policies that guide officers and employees in implementing the security program.

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 perceived 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 and architecture; (3) resource dedication; (4) training; and (5) testing.

For example, an institution's management may be assessing the proper strategic approach to intrusion detection for an Internet environment. Two potential approaches were identified for evaluation. The first approach uses a combination of network and host intrusion detection 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 dam-

age, 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.

Strategies should consider the layering of controls. Excessive reliance on a single control could create a false sense of confidence. For example, a financial institution that depends solely on a firewall can still be subject to numerous attack methodologies that exploit authorized network traffic. Financial institutions should design multiple layers of security controls and testing to establish several lines of defense between the attacker and the asset being attacked.[10] To successfully attack the data, each layer must be penetrated. With each penetration, the probability of detecting the attacker increases.

Policies are the primary embodiment of strategy, guiding decisions made by users, administrators, and managers, and informing those individuals of their security responsibilities. Policies also specify the mechanisms through which responsibilities can be met, and provide guidance in acquiring, configuring, and auditing information systems. Key actions that contribute to the success of a security policy are

- Implementing through ordinary means, such as system administration procedures and acceptable-use policies;
- Enforcing policy through 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.

[10] 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.

SECURITY CONTROLS IMPLEMENTATION

LOGICAL AND ADMINISTRATIVE ACCESS CONTROL

The goal of logical and administrative access control is to restrict access to system resources. Access should be provided only to authorized individuals whose identity is established, and their activities should be limited to the minimum required for business purposes. Authorized individuals (users) may be employees, TSP employees, vendors, contractors, customers, or visitors.

An effective control mechanism includes numerous controls to safeguard and limit access to key information system assets. This section addresses logical and administrative controls, including access rights administration and authentication through network, operating system, application, and remote access. 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 the following controls:

- Assign users and system resources only the access required to perform their required functions,
- Update access rights based on personnel or system changes,
- Periodically review users' access rights at an appropriate frequency based on the risk to the application or system, and
- Design appropriate acceptable-use policies and require users to sign them.

System devices, programs, and data are system resources. Each system resource may need to be accessed by other system resources and individuals 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 or system resource 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 to 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,[11] 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. Institutions should take particular care to remove promptly the access rights for users who have remote access privileges, and those who administer 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.[12]

Access rights to new software and hardware present a unique problem. Typically, hardware and software are installed 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;

[11] See ISO 17799, 9.2.4

[12] ISO 17799, 9.2.4 requires reviews at six month intervals.

- 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 the protection 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, 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 au-

thentication and is generally stronger than any single 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 is not identification as that term is used in the USA PATRIOT Act (31 U.S.C. 5318(l)). Authentication does not provide assurance that the initial identification of a system user is proper. Authentication only provides assurance that the user of the system is the same user that was initially identified. 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 login, after which the system prompts 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 can also be dynamic. Dynamic passwords typically use seeds, 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.

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

- 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, heuristic[13] 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 those attacks are account lockout mechanisms, which commonly lock out access to the account after a risk-based number of failed login attempts[14].

- 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 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[15], character set, prohibition against using well-known user identifiers, and length of time before the password must be changed. Users with greater authorization or privi-

[13] Behavior-based

[14] Existing industry practice is no more than five access attempts for customer retail account access.

[15] Industry practice is moving to six characters.

leges, 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 inactivity[16] and heuristic intrusion detection.

- Attacks can take advantage of automatic login features, allowing the attacker to assume an authorized user's identity merely by using a workstation.

  Controls include prohibiting and disabling automatic login features, and heuristic intrusion detection.

- User's 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.

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 every X 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

[16] Existing industry practice is no more than 20-30 minutes, but may be substantially less depending on the application.

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 of the token, ease in guessing any password-generating algorithm within the token, ease of successfully forging any authentication credential that unlocks the token, and reverse engineering, or cloning, of the token. Each of these weaknesses can be addressed through additional control mechanisms. Token theft generally is protected against by policies that require prompt reporting and cancellation of the token's ability to allow access to the system. 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.

Token systems can also incorporate public key infrastructure, and biometrics.

Public Key Infrastructure

Public key infrastructure (PKI), if properly implemented and maintained, may 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 a *digital 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.[17] 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 closure of user accounts;

[17] Private keys are necessary to defeat the system, and those keys are stored in a distributed fashion on each user's access device.

- 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 a user 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.

Single Sign-On

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 login 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,* 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 force[18] 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 pass-

[18] An attack that tries all possible combinations of the allowed character set.

word reset, or 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, 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.

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; and
- Implement appropriate technological controls to meet those access requirements consistently.

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 transaction, reputation, and compliance risk from threats including the theft of customer information, data alteration, system misuse, or denial-of-service attacks.

Network Configuration

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.

A typical 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. The differences may be far broader than network controls, encompassing personnel, host, and other issues.

Typical network controls that distinguish security domains include access control software permissions, dedicated lines, filtering routers, firewalls, remote-access servers, and virtual private networks. This booklet will discuss additional access controls within the applications and operating systems residing on the network in other sections. Before selecting the appropriate controls, financial institutions should map and configure the network to identify and control all access control points. Network configuration considerations could include the following actions:

- Identifying the various applications and user-groups 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 "demilitarized zone" (DMZ).

Protocols and Ports

Network communications rely on software protocols to ensure the proper flow of information. A protocol is a set of rules that allows communication between two points in a telecommunications connection. Different types of networks use different protocols. The Internet and most intranets and extranets, however, are based on the TCP/IP layered model of protocols. That model has four layers, and different protocols within each layer. The layers, from bottom to top, are the network access layer, the Internet layer, the host-to-host layer, and the application layer. Vulnerabilities and corresponding attack strategies exist at each layer. This becomes an important consideration in evaluating the necessary controls. Hardware and software can use the protocols to restrict network access. Likewise, attackers can use weaknesses in the protocols to attack networks.

The primary TCP/IP protocols are the Internet protocol (IP) and the transmission control protocol (TCP). IP is used to route messages between devices on a network, and operates at the Internet layer. TCP operates at the host-to-host layer, and provides a connection-oriented, full-duplex, virtual circuit between hosts. Different protocols support different services for the network. The different services often introduce additional vulnerabilities. For example, a third protocol, the user datagram protocol (UDP) is also used at the host-to-host layer. Unlike TCP, UDP is not connection-oriented, which makes it faster and a better protocol for supporting broadcast and streaming services. Since UDP is not connection-oriented, however, firewalls often do not effectively filter it. To provide additional safeguards, it is often blocked entirely from inbound traffic or additional controls are added to verify and authenticate inbound UDP packets as coming from a trusted host.

Other common protocols in a TCP/IP network include the following types.

- Address resolution protocol (ARP)—Obtains the hardware address of connected devices and matches that address with the IP address for that device. The hardware address is the Ethernet card's address, technically referred to as the "media access control" (MAC) address. Ethernet systems route messages by the MAC address, requiring a router to obtain both the IP address and the MAC address of connected devices. Reverse ARP (RARP) also exists as a protocol.
- Internet control message protocol (ICMP)—Used to send messages about network health between devices, provides alternate routing information if trouble is detected, and helps to identify problems with a routing.
- File transfer protocol (FTP)—Used to browse directories and transfer files. Although access can be authenticated or anonymous, FTP does not support encrypted authentication. Conducting FTP within encrypted channels, such as a Virtual Private Network (VPN), secure shell (SSH) or secure sockets layer (SSL) sessions can improve security.
- Trivial file transfer protocol (TFTP)—A file transfer protocol with no file-browsing ability, and no support for authentication.
- Simple mail-transfer protocol (SMTP)—Commonly used in e-mail systems to send mail.
- Post office protocol (POP)—Commonly used to receive e-mail.
- Hypertext transport protocol (HTTP)—Used for Web browsing.
- Secure shell (SSH) —Encrypts communications sessions, typically used for remote administration of servers.
- Secure sockets layer (SSL) —Typically used to encrypt Web-browsing sessions, sometimes used to secure e-mail transfers and FTP sessions.

Applications are built in conformance with the protocols to provide services from hosts to clients. Because clients must have a standard way of accessing the services, the services are assigned to standard host ports. Ports are logical not physical locations that are either assigned or available for specific network services. Under TCP/IP, 65536 ports are available, and the first 1024 ports are commercially accepted as being assigned to certain services. For instance, Web servers listen for requests on port 80, and secure socket layer Web servers listen on port 443. A complete list of the commercially accepted port assignments is available at www.iana.org. Ports above 1024 are known as high ports, and are user-assignable. However, users and administrators have the freedom to assign any port to any service, and to use one port for more than one service. Additionally, the service listening on one port may only proxy a connection for a separate service. For example, a Trojan horse keystroke-monitoring program can use the Web browser to send captured keystroke information to port 80 of an attacker's machine. In that case, monitoring

of the packet headers from the compromised machine would only show a Web request to port 80 of a certain IP address.

TCP/IP Packets

TCP/IP is a packet-based communications system. A packet consists of a header and a data payload. A header is analogous to a mail envelope, containing the information necessary for delivery of the envelope, and the return address. The data payload is the content of the envelope.

The IP packet header contains the address of the sender (source address) and the intended recipient (destination address) and other information useful in handling the packet. Under IP, the addresses are unique numbers known as IP addresses. Each machine on an IP network is identified by a unique IP address. The vast majority of IP addresses are publicly accessible. Some IP addresses, however, are reserved for use in internal networks. Those addresses are 10.0.0.0 - 10.255.255.255, 172.16.0.0 - 172.31.255.255, and 192.168.0.0 - 192.168.255.255. Since those internal addresses are not accessible from outside the internal network, a gateway device is used to translate the external IP address to the internal address. The device that translates external and internal IP addresses is called a network address translation (NAT) device. Other IP packet header fields include the protocol field (e.g., 1=ICMP, 6=TCP, 7=UDP), flags that indicate whether routers are allowed to fragment the packet, and other information.

If the IP packet indicates the protocol is TCP, a TCP header will immediately follow the IP header. The TCP header contains the source and destination ports, the sequence number, and other information. The sequence number is used to order packets upon receipt and to verify that all packets in the transmission were received.

Information in headers can be spoofed, or specially constructed to contain misleading information. For instance, the source address can be altered to reflect an IP address different from the true source address, and the protocol field can indicate a different protocol than actually carried. In the former case, an attacker can hide their attacking IP, and cause the financial institution to believe the attack came from a different IP and take action against that erroneous IP. In the latter case, the attacker can craft an attack to pass through a firewall and attack with an otherwise disallowed protocol.

Routing

Packets are moved through networks using routers, switches, and hubs. The unique IP address is commonly used in routing. Since users typically use text names instead of IP addresses for their addressing, the user's software must obtain the numeric IP address before sending the message. The IP addresses are obtained from the Domain Naming System (DNS), a distributed database of text names (e.g., anybank.com) and their associated IP addresses. For example, financial institution customers might enter the URL of the Web site in their Web browser. The user's browser queries the domain name server for the IP associated with anybank.com. Once the IP is obtained, the message is sent. Al-

though the example depicts an external address, DNS can also function on internal addresses.

A router directs where data packets will go based on a table that links the destination IP address with the IP address of the next machine that should receive the packet. Packets are forwarded from router to router in that manner until they arrive at their destination.[19] Since the router reads the packet header and uses a table for routing, logic can be included that provides an initial means of access control by filtering the IP address and port information contained in the message header. Simply put, the router can refuse to forward, or forward to a quarantine or other restricted area, any packets that contain IP addresses or ports that the institution deems undesirable. Security policies should define the filtering required by the router, including the type of access permitted between sensitive source and destination IP addresses. Network administrators implement these policies by configuring an access configuration table, which creates a filtering router or a basic firewall.

A switch directs the path a message will take within the network. Switching works faster than IP routing because the switch only looks at the network address for each message and directs the message to the appropriate computer. Unlike routers, switches do not support packet filtering. Switches, however, are designed to send messages only to the device for which they were intended. The security benefits from that design can be defeated and traffic through a switch can be sniffed.

Routers and switches are sometimes difficult to locate. Users may install their own devices and create their own unauthorized subnets. Any unrecognized or unauthorized network devices pose security risks. Financial institutions should periodically audit network equipment to ensure that only authorized and maintained equipment resides on their network.

DNS hosts, routers and switches are computers with their own operating system. If successfully attacked, they can allow traffic to be monitored or redirected. Financial institutions must restrict, log, and monitor administrative access to these devices. Remote administration typically warrants an encrypted session, strong authentication, and a secure client. The devices should also be appropriately patched and hardened (see "Systems Development, Acquisition and Maintenance").

Packets are sent and received by devices using a network interface card (NIC) for each network to which they connect. Internal computers would typically have one NIC card for the corporate network or a subnet. Firewalls, proxy servers, and gateway servers are typically dual-homed with two NIC cards that allow them to communicate securely both internally and externally while limiting access to the internal network.

[19] One exception is source-routed packets. Under source routing, the packet contains the information that dictates which routing to take to the destination. Source routing is sometimes useful in network diagnostics; however, since source routing can be helpful to an attacker in bypassing defenses, most networks should have source routing disabled.

Firewalls

A firewall[20] 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 a choke point for traffic between security domains, they are ideally situated to inspect and block traffic and coordinate activities with network IDS systems (see "Intrusion Detection and Response").

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.

Packet Filter Firewalls

Basic packet filtering was described in the router section and does not include stateful inspection. 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. Dynamic packet filtering incorporates stateful inspection[21] 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 employ application-specific vulnerabilities and functions because the packet filter cannot 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 problems in the TCP/IP specification.
- The firewalls are easy to misconfigure, which allows traffic to pass that should be blocked.

[20] For additional firewall explanations, see NIST Special Publication 800-41, "Guidelines on Firewalls and Firewall Policy."

[21] A technique that essentially verifies that inbound traffic is in response to requests initiated from inside the firewall.

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 important. 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”).

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:

- 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. The illustration below demonstrates how additional layers and security controls such as intrusion detection systems can strengthen the firewall architecture and bolster network security.

Financial institutions have a variety of firewall options from which to choose depending on the extent of Internet access and the complexity of their network. Considerations include 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.

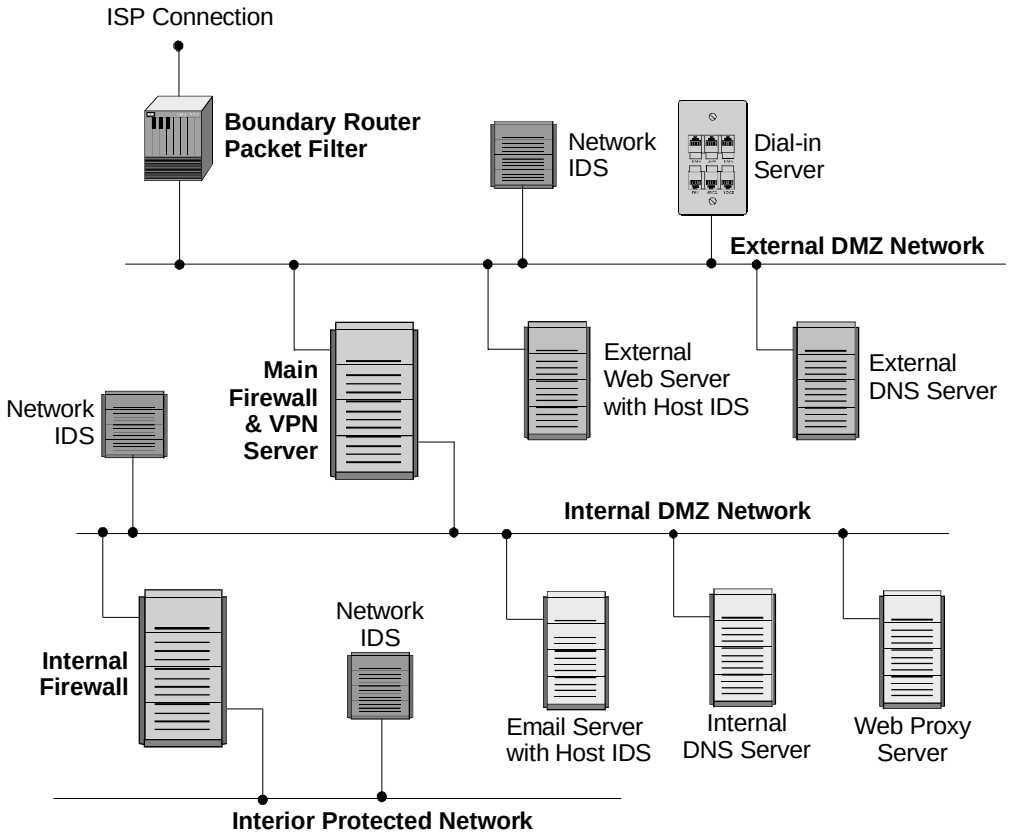

Figure 1: A Typical Firewall Environment
Source: NIST

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 intrusion detection and 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 and manage 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 machines and communications used for remote administration.

Financial institutions can reduce their vulnerability to these attacks somewhat through network configuration and design, sound implementation of its firewall architecture that includes multiple filter points, active firewall monitoring and management, and integrated intrusion detection. In most 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 traffic;
- Using a ruleset that disallows all traffic that is not specifically allowed;
- Using NAT and split DNS (domain name service) 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 intrusion detection devices to monitor actions on the firewall and to monitor communications allowed through the firewall (see "Intrusion Detection and Response");
- Administering the firewall using encrypted communications and strong authentication, only accessing the firewall from secure devices, and monitoring all administrative access;
- Limiting administrative access to few individuals; and
- Making changes only through well-administered change control procedures.

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 OS/400 and 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 must restrict privileged access to sensitive operating systems. While many operating systems have integrated access control software, third-party security software is available for most operating systems. 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; and
- 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 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 database 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. That 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 could also 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 "Logging and Data Collection").
- Easing the administrative burden of managing access rights by utilizing software that supports group profiles. Some financial institutions manage access rights individually and it 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 at the operating system level if no business need exists,
- Tightly controlling access through management approvals and subsequent audits,
- Implementing robust controls over configuration to disallow potential malicious use,
- Logging and monitoring remote access,
- Securing remote access devices, and
- Using strong authentication and encryption to secure communications.

Many financial institutions use modems, remote-access servers (RAS), and VPNs to provide remote access into their systems or to allow remote access out of their systems. Remote access can support mobile users through wireless, Internet, or dial-in capabilities. In some cases, modem 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 remotely attack the systems either individually or in groups. 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.
- Disable remote access at the operating system level if a business need for such access does not exist.
- Require management approval for remote access.
- Require an operator to leave the modems unplugged or disabled by default, to enable modems only for specific, 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.
- Log and monitor the date, time, user, user location, duration, and purpose for all remote access.
- Require a two-factor authentication process for all remote access (e.g., PIN-based token card with a one-time random password generator).
- Implement controls consistent with the sensitivity of remote use (e.g., remote system administration requires strict controls and oversight including encrypting the authentication and log-in process).
- Appropriately patch and maintain all remote access software.
- Use trusted, secure access devices.
- Use remote-access servers (RAS) to centralize modem and Internet access, to provide a consistent authentication process, and to subject the inbound and outbound network traffic to firewalls.

PHYSICAL SECURITY

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 in those 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
- Wireless emissions
- 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 only useful 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 somewhat through devices such as halon gas, smoke alarms, raised flooring, heat sensors, and the like.

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 access 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 IS 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 IS hardware and software should de-

pend 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, 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 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 environmental 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 IS, 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 IS 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.

Capturing radio frequency emissions also can compromise network security. 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 is used both as a prevention and detection control. 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. The products used and administrative controls should contain robust and effective controls to ensure reliability.

Encryption can impose significant overhead on networks and computing devices. A loss of encryption keys or other failures in the encryption process can deny the institution access to the encrypted data.

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. Generally speaking, authenticators are always 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 address[22]

- 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.

[22] Source: ISO 17799, 10.3.5.2

- 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 individ-

ual 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 PKI, or 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 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.

Virtual Private Networks (VPNs) are used to provide employees, contractors, and customers remote access over the Internet to institution systems. VPN security is provided by authentication and authorization for the connection and the user, as well as encryption of the traffic between the institution and the user. While VPNs can exist between client systems, and between servers, the typical installation terminates the VPN connection at the institution firewall. VPNs can use many different protocols for their communications. Among the popular protocols are PPTP (point-to-point tunneling protocol), L2F, L2TP, and IPSec. VPNs can also use different authentication methods, and different components on the host systems. Implementations between vendors, and between products,

may differ. Currently, the problems with VPN implementations generally involve interfacing a VPN with different aspects of the host systems, and reliance on passwords for authentication.

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.

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

Disk encryption is typically used to protect data in storage.

MALICIOUS CODE

Action Summary

Financial institutions should protect against the risk of malicious code by

- Using anti-virus products on clients and servers;
- Using an appropriate blocking strategy on the network perimeter;
- Filtering input to applications; and
- Creating, implementing, and training staff in appropriate computing policies and practices.

Malicious code is any program that acts in unexpected and potentially damaging ways. Common types of malicious code are viruses, worms, and Trojan horses. The functions of each were once mutually exclusive; however, developers combined functions to create more powerful malicious code. Currently malicious code can replicate itself within a computer and transmit itself between computers. Malicious code also can change, delete, or insert data, transmit data outside the institution, and insert backdoors into institution systems. Malicious code can attack institutions at either the server or the client level. It can also 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.

Prevention and detection of malicious code typically involves anti-virus and other detection products at gateways, mail servers, and workstations. Those products generally scan messages for known signatures of a variety of malicious code, or potentially dangerous behavioral characteristics. Differences between products exist in detection capabilities and the range of malicious code included in their signatures. Detection products should not be relied upon to detect all malicious code. Additionally, anti-virus and other products that rely on signatures generally are ineffective when the malicious code is encrypted. For example, VPNs, IPSec, and encrypted e-mail will all shield malicious code from detection.

Signature-based anti-virus products scan for unique components of certain known malicious code. Since new malicious code is created daily, the signatures need to be updated continually. Different vendors of anti-virus products update their signatures on different frequencies. When an update appears, installing the update on all of an institution's computers may involve automatically pushing the update to the computers, or requesting users to manually obtain the update.

Heuristic anti-virus products generally execute code in a protected area of the host to analyze and detect any hostile intent. Heuristic products are meant to defend against previously unknown or disguised malicious code.

Malicious code may be blocked at the firewall or gateway. For example, a general strategy might be to block all executable e-mail attachments, as well as any Active-X or Java applets. A more refined strategy might block based on certain characteristics of known code.

Protection of servers involves examining input from users and only accepting that input which is expected. This activity is called filtering. If filtering is not employed, a Web site visitor, for instance, could employ an attack that inserts code into a response form, causing the server to perform certain actions. Those actions could include changing or deleting data and initiating fund transfers.

Protection from malicious code also involves limiting the capabilities of the servers and Web applications to only include functions necessary to support operations. See "Systems Development, Acquisition, and Maintenance."

Anti-virus tools and code blocking are not comprehensive solutions. New malicious code could have different signatures, and bypass other controls. Protection against newly developed malicious code typically comes in the form of policies, procedures, and user awareness and training. For example, policies could prohibit the installation of software by unauthorized employees, and regular reviews for unauthorized software could take place. System users could be trained not to open unexpected messages, not to open any executables, and not to allow or accept file transfers in P2P communications. Additional protection may come from disconnecting and isolating networks from each other or from the Internet in the face of a fast-moving malicious code attack.

An additional detection control involves network and host intrusion detection devices. Network intrusion detection devices can be tuned to alert when known malicious code attacks occur. Host intrusion detection can be tuned to alert when they recognize abnormal system behavior, the presence of unexpected files, and changes to other files.

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

- Defining security requirements before developing or acquiring new systems;
- Incorporating widely recognized standards in developing security requirements;
- Incorporating appropriate security controls, audit trails, and logs for data entry and data processing;
- Implementing an effective change control process;
- Hardening systems before deployment;
- Establishing an effective patch process for new security vulnerabilities; and
- Overseeing vendors to protect the integrity and confidentiality of application source code.

Financial institution system development, acquisition, and maintenance functions should incorporate agreed upon security controls into software prior to development and implementation. Management should integrate consideration of security controls into each

phase of the system development process. For the purposes of this section, system development could include the internal development of customized systems, the creation of database systems, or the acquisition of third-party developed software. System development could include long-term projects related to large mainframe-based software projects with legacy source code or rapid Web-based software projects using fourth-generation-programming. In all cases, institutions need to prioritize security controls appropriately.

SOFTWARE DEVELOPMENT AND ACQUISITION

Security 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.[23] Management may also refer to published, widely recognized industry standards as a baseline for establishing their security requirements. 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. When evaluating purchased software, financial institutions should consider the availability of products that have either been independently evaluated or received security accreditation through financial institution or information technology-related industry groups.

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

[23] See http://www.commoncriteria.org

utilities); and job control checks to ensure programs run in correct sequence (see the booklet "Computer Operations" 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.

Development and Support

Development and support activities should ensure that new software and software changes do not compromise security. Financial institutions should have an effective application and system change control process for developing, implementing, and testing changes to internally developed software and purchased software. Weak change control procedures can corrupt applications and introduce new security vulnerabilities. Change 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 impacted 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.

When creating and maintaining software, separate software libraries should be used to assist in enforcing access controls and segregation of duties. Typically, separate libraries exist for development, test, and production.

Source Code Review and Testing

Application and operating system source code can have numerous vulnerabilities due to programming errors or misconfiguration. Where possible, financial institutions should use software that has been subjected to independent security reviews of the source code especially for Internet facing systems. 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 often provide unauthorized access to systems or data that circumvents built-in access controls and logging. The source code reviews should be repeated after the creation of potentially significant changes.

Outsourced Development

Many financial institutions outsource software development to third parties. Numerous vendor management issues exist when outsourcing software development. The vendor management program established by management should address the following:

- Verifying credentials and contracting only with reputable providers;
- Evaluating the provider's secure development environment, including background checks on its employees and code development and testing processes;
- Obtaining fidelity coverage;
- Requiring signed nondisclosure agreements to protect the financial institution's rights to source code and customer data as appropriate;
- Establishing security requirements, acceptance criterion, and test plans;
- Reviewing and testing source code for security vulnerabilities, including covert channels or backdoors that might obscure unauthorized access into the system;
- Restricting any vendor access to production source code and systems and monitoring their access to development systems; and
- Performing security tests to verify that the security requirements are met before implementing the software in production.

HOST AND USER EQUIPMENT ACQUISITION AND MAINTENANCE

Hardening Systems

Many 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 it is 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, the 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.

System Patches

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.

Patches make direct changes to the software and configuration of each system to which they are applied. They may degrade system performance. Also, patches may introduce new vulnerabilities, or reintroduce old vulnerabilities. The following considerations 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;
- 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 the master configurations used to build new systems;
- Create and document an audit trail of all changes; and
- Seek additional expertise as necessary to maintain a secure computing environment.

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.

Security personnel allow legitimate users to have system access necessary to perform their duties. 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,
- Crashing 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 verify job application information on all new employees. The sensitivity of a particular job or access level may warrant additional criminal background and credit checks. Institutions should verify that contractors are subject to similar screening procedures. Typically, the minimum verification considerations include

- Character references;
- 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[24]. 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.

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

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 should strengthen compliance with the security policy. 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 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.

ELECTRONIC AND PAPER-BASED MEDIA HANDLING

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 media in transit or transmission to third parties.

Sensitive information is frequently contained on media such as paper documents, output reports, back-up tapes, disks, cassettes, optical storage, test data, and system documentation. Protection of that data requires protection of the media. The theft, destruction, or

other loss of the media could result in the exposure of corporate secrets, breaches in customer confidentiality, alteration of data, and the disruption of business activities. The policies and procedures necessary to protect media may need revision as new data storage technologies are contemplated for use and new methods of attack are developed.

The sensitivity of the data (as reflected in the data classification) dictates the extent of procedures and controls required. Many institutions find it easier to store and dispose of all media consistently without having to segregate out the most sensitive information. This approach also can help reduce the likelihood that someone could infer sensitive information by aggregating a large amount of less sensitive information. Management must address three components to secure media properly: handling and storage, disposal, and transit.

HANDLING AND STORAGE

IT management should ensure secure storage of media from unauthorized access. Controls could include physical and environmental controls including fire and flood protection, limited access (e.g., physical locks, keypad, passwords, biometrics), labeling, and logged access. Management should establish access controls to limit access to media, while ensuring all employees have authorization to access the minimum level of data required to perform their responsibilities. More sensitive media like 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 media, including the printouts of sensitive information. Periodically, the security staff, audit staff, and data owners should review authorization levels and distribution lists to ensure they remain appropriate and current.

DISPOSAL

Financial institutions need appropriate disposal procedures for both electronic and paper-based media. Policies should prohibit employees from discarding sensitive media 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 unreconstructable before disposal. Institutions that contract with third parties should use care in selecting vendors to ensure adequate employee background checks, controls, and experience.

Computer-based media presents unique disposal problems. 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. Addi-

tionally, data can sometimes be destroyed after overwriting[25]. 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.

TRANSIT

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

- 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 of sensitive information,
- 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.

LOGGING AND DATA COLLECTION

Action Summary

Financial institutions should

- Identify the system components that warrant logging,
- Determine the level of data logged for each component, and
- Establish policies for securely handling and analyzing log files.

Financial institutions should take reasonable steps to ensure that sufficient data is collected from secure log files to identify and respond to security incidents and to monitor and enforce policy compliance. Appropriate logging controls ensure that security per-

[25] 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.

sonnel can review and analyze log data to identify unauthorized access attempts and security violations, provide support for personnel actions, and aid in reconstructing compromised systems.

An institution's ongoing security risk assessment process should evaluate the adequacy of the system logging and the type of information collected. Security policies should address the proper handling and analysis of log files. Institutions have to make risk-based decisions on where and when to log activity. The following data are typically logged to some extent including

- Inbound and outbound Internet traffic,
- Internal network traffic,
- Firewall events,
- Intrusion detection system events,
- Network and host performance,
- Operating system access (especially high-level administrative or root access),
- Application access (especially users and objects with write-and-execute privileges), and
- Remote access.

When evaluating whether and what data to log, institutions should consider the importance of the related system or information, the importance of monitoring the access controls, the value of logged data in restoring a compromised system, and the means to effectively analyze the data. Generally, logs should capture source identification information; session ID; terminal ID; and the date, time, and the nature of the access attempt, service request, or process. Many hardware and software products come with logging disabled and may have inadequate log analysis and reporting capabilities. Institutions may have to enable the logging capabilities and then verify that logging remains enabled after rebooting. In some cases, additional software will provide the only means to analyze the log files effectively.

Many products such as firewall and intrusion detection software can simplify the security monitoring by automating the analysis of the logs and alerting the appropriate personnel of suspicious activity. 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. 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 backup 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,
- Utilizing centralized logging, such as the UNIX "SYSLOG" utility, and
- Setting logging parameters to disallow any modification to previously written data.

The financial institution should have an effective means of tracing a security event through their system. Synchronized time stamps on network devices may be necessary to gather consistent logs and a consistent audit trail. Additionally, logs should be available, when needed, for incident detection, analysis and response.

When using logs to support personnel actions, management should consult with counsel about whether the logs are sufficiently reliable to support the action.

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;
- Third-party 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 Section 501(b) of the GLBA to ensure service providers have implemented adequate security controls to safeguard customer information. Supporting interagency 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 determine the following security considerations when selecting or monitoring 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 provisions for 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.

SAS 70 REPORTS

Frequently TSPs or user groups will contract with an accounting firm to report on security using Statement on Auditing Standards 70 (SAS 70), 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 point in 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 evaluate the scope and findings of any SAS 70 report. The report may be based on different security requirements than those established by the institution. It may not provide a thorough test of security controls unless requested by the TSP or augmented with additional coverage. Additionally, the report may not address the effectiveness of the security process in continually mitigating changing risks.

Therefore, financial institutions may require additional reports to oversee the security program of the service provider. Additional guidance is provided in "Security Testing - Outsourced Systems," below.

INTRUSION DETECTION AND RESPONSE

Action Summary

Financial institutions should have the capability to detect and respond to an information system intrusion commensurate with risk. Risk mitigation practices include

- Preparation, including analysis of data flows, decisions on the nature and scope of monitoring, consideration of legal factors, appropriate policies governing detection and response, and the formation and equipping of response teams;
- Detection implementation, including the proper use of technology; and
- Response to an intrusion, including the containment and restoration of systems and appropriate reporting.

A maxim of security is "prevention is ideal, but detection is a must."[26] Security systems must both restrict access and protect against the failure of those access restrictions. When those systems fail, however, an intrusion occurs and the only remaining protection is a detection-and-response capability. The earlier an intrusion is detected, the greater the institution's ability to mitigate the risk posed by the intrusion. Financial institutions should have a capability to detect and react to an intrusion into their information systems.

INTRUSION DETECTION

Preparation for intrusion detection generally involves identifying data flows to monitor for clues to an intrusion, deciding on the scope and nature of monitoring, implementing that monitoring, and establishing a process to analyze and maintain custody over the resulting information. Additionally, legal requirements may include notifications of users regarding the monitoring and the extent to which monitoring must be performed as an ordinary part of ongoing operations.

Adequate preparation is a key prerequisite to detection. The best intrusion detection systems will not identify an intrusion if they are not located to collect the relevant data, do not analyze correct data, or are not configured properly. Even if they detect an intrusion,

[26] System Administration, Networking and Security Institute (SANS) Top 20, http://www.sans.org/top20.htm

the information gathered may not be usable by law enforcement if proper notification of monitoring and preservation of data integrity has not taken place.

Automated Intrusion Detection Systems (IDS)

Automated intrusion detection systems (IDS) use one of two methodologies, signature and heuristics. An IDS can target either network traffic or a host. The signature-based methodology is generally used on network traffic. An IDS that uses a signature-based methodology reads network packets and compares the content of the packets against signatures, or unique characteristics, of known attacks and known anomalous network traffic. When a match is recognized between current readings and a signature, the IDS generates an alert.

A general weakness in the signature-based detection method is that a signature must exist for an alert to be generated. Attacks that generate different signatures from what the institution includes in its IDS 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, rather than both known attacks and anomalous traffic. Another general weakness is in the capacity of the IDS to read traffic. If the IDS falls behind in reading network traffic, traffic may be allowed to bypass the IDS.[27] That traffic may contain attacks that would otherwise cause the IDS to issue an alert.

Proper placement of network IDS 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 IDS less sensitive than if it is placed inside the firewall. An IDS outside the firewall will generally alert on the greatest number of unsuccessful attacks. IDS monitoring behind the firewall is meant to detect and alert on hostile intrusions. Multiple IDS units can be used, with placement determined by the expected attack paths to sensitive data. Generally speaking, the closer the IDS is to sensitive data, the more important the tuning, monitoring, and response to IDS 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.[28]"

[27] IDS units that have a traffic rating, such as gigabit IDS, may allow traffic to bypass when traffic reaches a fraction of their rating.

[28] NIST Special Publication 800-41

"Tuning" refers to the creation of signatures that can distinguish between normal network traffic and potentially malicious traffic. Proper tuning of these IDS units is essential to reliable detection of both known attacks and newly developed attacks. 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 an IDS is not properly tuned, the volume of alerts it generates may degrade the intrusion identification and response capability.

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 signature method meant to focus on sophisticated attackers is protocol analysis, when the contents of a packet or session are analyzed for activity that violates standards or expected behavior. That method can catch, for instance, indicators that servers are being attacked using Internet control message protocol (ICMP).

Switched networks pose a problem for network IDS. Switches ordinarily do not broadcast traffic to all ports, and a network IDS 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.

Encrypted network traffic will drastically reduce the effectiveness of a network IDS. Since a network IDS only reads traffic and does not decrypt the traffic, encrypted traffic will avoid detection.

Some network IDS units allow the IP addresses associated with certain signatures to be automatically blocked. Financial institutions that use that capability run the risk of an attacker sending attack packets that falsely report the sending IP addresses as that of service providers and others that the institution needs to continue offering service, thereby creating a denial-of-service situation. To avoid such a situation, the institution also may implement a list of IP addresses that should not be blocked by the IDS.

Hosts also use a signature-based method. One such method 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 additional host-based signature method monitors the application program interfaces for unexpected or unwanted behavior, such as a Web server calling a command line interface.

Attackers can defeat host-based IDS systems using loadable kernel modules, or LKMs. A LKM is software that attaches itself to the operating system kernel. From there, it can redirect and alter communications and processing. With the proper LKM, 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. LKMs can also hide the use of the application program interfaces. Detection of LKMs is extremely difficult and is typically done through another LKM.

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. LKMs, 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.[29]

The heuristic, or behavior, method creates a statistical profile of normal activity on the host or network. 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.

Both signature-based and heuristic 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 IDS reports with less vigor, allowing real attacks to be reported by the IDS but not researched or acted upon. Additionally, they may tune the IDS 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 IDS systems. 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 IDS systems gather vast amounts of traffic which must be analyzed, sometimes manually, to generate a complete

[29] NIST Special Publication 800-41.

picture of an attack. Finally, unlike IDS, a honeypot does not pass packets without inspection when under a heavy traffic load.

Honeypots have two key disadvantages. 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.

Honeypots also introduce the risk of being compromised without triggering an alarm, then 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.

Operational Anomalies

Operational anomalies may be evidence of a broad number of issues, one of which is potential intrusion. Anomalies that act as intrusion-warning indicators fall into two categories, those apparent in system processing, and those apparent outside the system.

System processing anomalies are evident in system logs and system behavior. Good identification involves pre-establishing which system processing data streams will be monitored for anomalies, defining which anomalies constitute an indicator of an intrusion, and the frequency of the monitoring. For example, remote access logs can be reviewed daily for access during unusual times. Other logs can be reviewed on other regular cycles for other unusual behaviors. System behavior covers a broad range of issues, from CPU utilization to network traffic protocols, quantity and destinations. One example of a processing anomaly is CPU utilization approaching 100% when the scheduled jobs typically require much less. Anomalous behavior, however, may not signal an intrusion.

Outside the system, detection is typically based on system output, such as unusual Automated Clearing House transactions or bill payment transactions. Those unusual transactions may be flagged as a part of ordinary transaction reviews, or customers and other system users may report them. Customers and other users should be advised as to where and how to report anomalies. The anomalous output, however, may not signal an intrusion.

Central reporting and analysis of all IDS output, honeypot monitoring, and anomalous system behavior assists in the intrusion identification process. Any intrusion reporting

should use out-of-band communications mechanisms to protect the alert from being intercepted or compromised by an intruder.

INTRUSION RESPONSE

Intrusion detection by itself does not mitigate risks of an intrusion. Risk mitigation only occurs through an effective and timely response. The goal of the response is to minimize damage to the institution and its customers through containment of the intrusion, and restoration of systems.

The response primarily involves people rather then 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. Preparation involves defining the policies and procedures that guide the response, assigning responsibilities to individuals and 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 the proper personnel are available and notified.
- 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 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, 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 organization 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 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 their institution's policies are followed by the service provider and confidentiality of data and systems are maintained.

Institutions can assess best the adequacy of their preparations through testing (see "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 Suspicious Activity Report (Guidelines for filing are included in individual agency guidance); and
- Communication with effected parties.

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 considerations. Depending on the event, some or all of the elements of the security environment may change. Different people may be involved in operations, at a different physical location, using similar but different machines and software which may communicate over different communications lines. Depending on the event, 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. Testing these security considerations should be integrated with the testing of business continuity plan implementations.

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 have used insurance coverage as an effective method to transfer risks from themselves to insurance carriers. Insurance coverage is increasingly available to cover risks from security breaches or denial of service attacks. For example, 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 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 TESTING

Action Summary

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

- Basing their testing plan, test selection, and test frequency on the risk posed by potentially non-functioning controls;
- Establishing controls to mitigate the risks posed to systems from testing; and
- Using test results to evaluate whether security objectives are met.

Information security is an integrated process that reduces information security risks to acceptable levels. The entire process, including testing, is driven by an assessment of risks. The greater the risk, the greater the need for the assurance and validation provided by effective information security testing.

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 frequent and rigorous testing than low-risk systems. Because tests only measure the security posture at a point in time, frequent testing provides increased assurance that the processes that are in place to maintain security over time are functioning.

A wide range of tests exists. Some address only discrete controls, such as password strength. Others address only technical configuration, or may consist of audits against standards. Some tests are overt studies to locate vulnerabilities. Other tests can be designed to mimic the actions of attackers. In many situations, management may decide to perform a range of tests to give a complete picture of the effectiveness of the institution's security processes. Management is responsible for selecting and designing tests so that the test results, in total, support conclusions about whether the security control objectives are being met.

TESTING CONCEPTS AND APPLICATION

Testing Risks to 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 section 501(b) of the GLBA. Management also 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 provide 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.

Measurement and Interpretation of Test Results. Institutions should design tests to produce results that are logical and objective. Results that are reduced to metrics are potentially more precise and less subject to confusion, as well as being more readily tracked over time. The interpretation and significance of test results are most useful when tied to threat scenarios.

Traceability. Test results that indicate an unacceptable risk in an institution's security should be traceable to actions subsequently taken to reduce the risk to an acceptable level.

Thoroughness. Institutions should perform tests sufficient to provide a high degree of assurance that their security plan, strategy and implementation is effective in meeting the security objectives. Institutions should design their test program to draw conclusions about the operation of all critical controls. The scope of testing should encompass all systems in the institution's production environment and contingency plans and those systems within the institution that provide access to the production environment.

Frequency. Test frequency should be based on the risk that critical controls are no longer functioning. Factors to consider include the nature, extent, and results of prior tests, the value and sensitivity of data and systems, and changes to systems, policies and procedures, personnel, and contractors. For example, network vulnerability scanning on high-risk systems can occur at least as frequently as significant changes are made to the network.

INDEPENDENT DIAGNOSTIC TESTS

Independent diagnostic 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, as well as 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 to identify the extent to which a system can be compromised before the attack is identified and assess the response mechanism's effectiveness. Penetration tests generally are not a comprehensive test of the system's security and should be combined with other independent diagnostic tests 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 they adopt are appropriate for their 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 diagnostic 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 themselves 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.

Controls Over Testing. Certain testing can adversely affect data integrity, confidentiality, and availability. Management is expected to limit those risks by appropriately crafting test protocols. Examples of issues to address include the specific systems to be tested, threats to be simulated, testing times, the extent of security compromise allowed, situations in which testing will be suspended, and the logging of test activity. Management is responsible for exercising oversight commensurate with the risk posed by the testing.

Frequency. The frequency of testing should be determined by the institution's risk assessment. High-risk systems should be subject to an independent diagnostic 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.[30] 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 diagnostic 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.

OUTSOURCED SYSTEMS

Management is responsible for ensuring institution and customer data is protected, even when that data is transmitted, processed, or stored by a service provider. Service providers should have appropriate security testing based on the risk to their organization, their customer institutions, and the institution's customers. Accordingly, management and auditors evaluating TSPs providers should use the above testing guidance 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 testing performed at the service provider through review of timely audits and test results or other equivalent evaluations.

[30] The quarterly auditing and verification need not be by an independent source. See NIST Special Publication 800–41.

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. Monitoring and 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 re-

viewing 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 nontechnical vulnerabilities and develop appropriate mitigation solutions to address them. Examples include many controls discussed elsewhere in this booklet including
  - Establishing an effective configuration management 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 security self-assessments and audits to provide an ongoing assessment of policy compliance and ensure prompt corrective action of significant deficiencies.
- Security personnel should have access to automated tools appropriate for the complexity of the financial institution systems. Automated security policy and security log analysis tools can significantly increase the effectiveness and productivity of security personnel.

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 threat. Depending on the new threat or vulnerability, 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 testing 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, would 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.

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 since 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 organizations and others
   - 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.
2. Identify unique products and services and any required third-party access requirements.
3. Determine the extent of network connectivity internally and externally, access points (including gateways and modems), and multiple host computers from mainframes to file servers.
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 their 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 reasonable threats to the financial institution assets,
   - Analyzed its technical and organizational vulnerabilities, and
   - Considered the potential effect of a security breech on customers as well as the institution.
2. Determine whether the risk assessment provides adequate support for the security strategy, controls, and testing plan 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 relative to the risk to the institution.

1. Review security policies 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, and/or biometric controls and related enrollment and maintenance processes as well as database security.
- Network Access
  - Network access controls including firewalls
  - 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
- Software development and acquisition including change management
- Personnel security
- Media handling procedures and restrictions, including procedures for securing, transmitting and disposing of paper and electronic information.
- Intrusion detection and response

- Service provider oversight
- Business continuity
- Insurance
- Data security

2. Evaluate the policies 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 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 testing.

1. Evaluate the testing plan to determine whether the scope and timing of tests are supported by the risk assessment.
2. Review internal and external tests to ensure that they include adequate testing to validate the performance of key security controls. Key security controls include all of the components contained in Objective 4 above.
3. Ensure that the institution utilizes sufficient expertise to test more complex aspects of security, where appropriate (e.g., penetration testing, vulnerability assessments, and source code reviews).
4. Evaluate the degree of independence between the persons testing security from the persons administering security.
5. Determine the timeliness of reporting test results to senior management and evaluate the adequacy and timing of corrective action.
6. Determine that tests are performed in conformance with the testing plan, and that material revisions to the testing plan or test schedule are supported by changes to the risk assessment.
7. Determine that management and the security office reviews the tests to ensure they are complete, adequately performed, and that the results are properly analyzed.

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, intrusion detection, policy monitoring, enforcement, and reporting.

8. Evaluate management's ability to effectively control the pace of change to their 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 if 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 if 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., DNS), and other programs.

7. Compare the access control rules establishment and assignment processes to the access control policy for consistency.

8. Determine if 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.

3. 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).

4. Determine if 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.

5. Determine if 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.

6. Determine if unauthorized attempts to access authentication mechanisms (e.g., password storage location) are appropriately monitored, reported and followed up. 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.

7. Determine whether authentication error feedback (i.e., reporting failure to successfully log-in) during the authentication process provides a prospective attacker clues that may allow them to hone their attack. If so, obtain and evaluate a justification for such feedback.

8. Determine whether adequate controls exist to protect against replay attacks and hijacking.

9. 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.

10. 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.

11. 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.

12. Determine whether appropriate device and session authentication takes place, particularly for remote and wireless machines.

13. Review authenticator reissuance and reset procedures. Determine whether controls adequately mitigate risks from

    - Social engineering
    - Errors in the identification of the user
    - 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 if 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 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 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
   - Contingency planning

10. Determine if 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 NAT and split DNS are used to hide internal names and addresses from external users. (Note: Split DNS is a method of segregating the internal DNS from the external DNS.)
    - 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 if network-based IDSs are properly coordinated with firewalls (see "Intrusion Detection" procedures).
12. Determine whether logs of security-related events 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 if 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 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, and that configuration takes advantage of available object, device, and file access controls.
2. Determine if the configuration minimizes the functionality of programs, scripts, and plug-ins to what is necessary and justifiable.
3. Determine if 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 "Intrusion Detection and Response.")

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 if 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 workstations are prepared according to documented procedures for secure configuration or replication and that vulnerability testing takes place prior to deployment.

2. Determine whether workstations are 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 workstations are deactivated after a period of inactivity through screen saver passwords, server time-outs, powering down, or other means.

7. Determine whether systems are protected against malicious software such as Trojan horses, viruses, and worms.

E. PHYSICAL SECURITY

1. Determine whether physical security for information technology equipment and operations is coordinated with that of other institution organizations.

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 if 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 if the institution includes in its terms and conditions of employment the employee's responsibilities for information security.

3. Determine if the institution requires personnel with authority to access customer information and confidential institution information to sign and abide by confidentiality agreements.

4. Determine if 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 if employees have an available and reliable mechanism to promptly report security incidents, weaknesses, and software malfunctions.

6. Determine if an appropriate disciplinary process for security violations exists and is functioning.

G. APPLICATION SECURITY

1. Determine if operational software storage, program source, object libraries and load modules are appropriately secured against unauthorized access.
2. Determine if user input is validated appropriately (e.g. character set, length, etc).
3. Determine if appropriate message authentication takes place.
4. Determine if 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 requirements are determined for software, whether internally developed or acquired from a vendor.
2. Determine whether management appropriately considers either following a recognized security standard development process, or reference to widely recognized industry standards.
3. Determine if the group or individual establishing security requirements has appropriate credentials, background, and/or training.
4. Evaluate whether the software 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 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.

I. BUSINESS CONTINUITY—SECURITY

1. Determine if 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 if substitute processing facilities and systems undergo similar testing as production facilities and systems.

3. Determine if appropriate access controls and physical controls have been considered and planned for the former production system and networks when processing is transferred to a substitute facility.

4. Determine if the intrusion detection and 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 credential to fill in for another employee who is on vacation or out the office, this assignment would be a primary job responsibility.)

J. INTRUSION DETECTION AND RESPONSE

1. Identify controls used to detect and respond to unauthorized activities.

   - Review the schematic of the information technology systems for common intrusion detection systems.
   - Review security procedures for daily and periodic report monitoring to identify unauthorized or unusual activities.
   - Identify IT architectural design and intrusion detection systems that increase management's confidence that security is maintained (e.g., through the use of routers, host-based security, data segregation and information flows).

2. Determine if the IDSs identified as necessary in the risk assessment process are properly installed and configured.

3. 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.
4. Determine whether logs of security-related events are sufficient to assign accountability for intrusion detection system activities, as well as support intrusion forensics and IDS.
5. Determine if 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.
6. Determine if an appropriate process exists to authorize employee access to intrusion detection systems and that authentication and authorization controls limit access to and control the access of authorized individuals.
7. Determine if appropriate detection capabilities exist related to
   - System resource usage and anomalies,
   - Active host and network intrusion detection systems,
   - User related anomalies,
   - Operating and tool configuration anomalies,
   - File and data integrity problems, and
   - Vulnerability testing.
8. Determine whether an incident 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), and
   - Has appropriate authority and timely access to decision makers for actions that require higher approvals.
9. Evaluate the selection of systems to monitor and objectives for monitoring.
10. Determine whether the data and data streams to monitor are established and consistent with the risk assessment.

11. Determine whether users are appropriately notified regarding security monitoring.

12. Determine whether

    - Responsibilities and authorities of security personnel and system administrators for monitoring are established, and
    - Tools used are reviewed and approved by appropriate management with appropriate conditions for use.

13. Determine if the responsibility and authority of system administrators is appropriate for handling notifications generated by monitoring systems.

14. Determine if users are trained to report unexpected network behavior that may indicate an intrusion, and that clear reporting lines exist.

15. Determine if the security policy specifies the actions to be taken following the discovery of an unexpected, unusual, or suspicious activity (potential intrusion), and that appropriate personnel are authorized to take those actions.

16. Evaluate 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.

17. Determine if 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.

18. Determine if the information disclosure policy addresses the appropriate regulatory reporting requirements.

19. Determine if 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.

20. Determine if the policy requires all compromised systems to be restored before reactivation, through either rebuilding with verified good media or verification of software cryptographic checksums.

21. Determine whether all participants in intrusion detection and responses are trained adequately in the intrusion detection and response policies, their roles, and the procedures they should take to implement the policies.

K. SERVICE PROVIDER OVERSIGHT—SECURITY

1. Determine if contracts contain security requirements that at least meet the objectives of the Section 501(b) GLBA security 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 if institution oversight of third party provider security controls is adequate.
7. Determine if any third party provider access to the institution's system is controlled according to "Authentication and Access Controls" and "Network Security" procedures.
8. Determine if the contract requires secure remote communications, as appropriate.
9. Determine if 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.

L. 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 if 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, where 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 if 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 if cryptographic keys are destroyed in a secure manner when they are no longer required.

M. 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 if 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.

APPENDIX B: GLOSSARY

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 verification of identity by a system based on the presentation of unique credentials to that system.
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.
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
ISO	International Organization for Standards
IDS	Intrusion Detection System

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.
Vulnerability	A flaw that allows someone 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 6801 and 6805(b): Gramm–Leach–Bliley Act
- 18 USC 1030: Fraud and Related Activity in Connection with Computers

FEDERAL RESERVE BOARD

REGULATIONS

- 12 CFR 208.61: Minimum Security Devices and Procedures
- 12 CFR 208.62: Reports of Suspicious Activities
- 12 CFR 208.63: Procedures for Monitoring Bank Secrecy Act Compliance
- 12 CFR Part 208, Appendix D-1: Interagency Guidelines Establishing Standards for Safety and Soundness
- 12 CFR Part 208, Appendix D-2: Interagency Guidelines Establishing Standards for Safeguarding Customer Information (State Member Banks)
- 12 CFR 211.9: Interagency Guidelines Establishing Standards for Safeguarding Customer Information (Edge or agreement corporation)
- 12 CFR 211.24: Interagency Guidelines Establishing Standards for Safeguarding Customer Information (uninsured state-licensed branch or agency of a foreign bank)
- 12 CFR Part 225 Appendix F: Interagency Guidelines Establishing Standards for Safeguarding Customer Information (bank holding companies and their non-bank subsidiaries or affiliates (except brokers, dealers, persons providing insurance, investment companies, and investment advisors))

GUIDANCE

- SR Letter 02–18: Section 312 of the USA Patriot Act—Due Diligence for Correspondent and Private Banking Accounts
- SR Letter 02–6: Information Sharing Pursuant to Section 314(b) of the USA Patriot Act
- SR Letter 01–20: FFIEC Guidance on Authentication

- SR Letter 01–15: Safeguarding Customer Information
- SR Letter 01–11: Identity Theft and Pretext Calling
- SR Letter 00–17: Guidance on the Risk Management of Outsourced Technology Services
- SR Letter 00–04: Outsourcing of Information and Transaction Processing
- SR Letter 99–08: Uniform Rating System for Information Technology
- SR Letter 97–32: Sound Practices Guidance for Information Security for Networks

FEDERAL DEPOSIT INSURANCE CORPORATION

REGULATIONS

- 12 CFR Part 326, Subpart A: Minimum Security Procedures
- 12 CFR Part 326, Subpart B: Procedures for Monitoring Bank Secrecy Act Compliance
- 12 CFR Part 332: Privacy of Consumer Financial Information
- 12 CFR Part 353: Suspicious Activity Reports
- 12 CFR Part 364, Appendix A: Interagency Guidelines Establishing Standards for Safety and Soundness
- 12 CFR Part 364, Appendix B: Interagency Guidelines Establishing Standards for Safeguarding Customer Information

GUIDANCE

- 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)
- FIL–68–99: Risk Assessment Tools and Practices (July 7, 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–82–96: Risks Involving Client/Server Computer Systems (October 8, 1996)

NATIONAL CREDIT UNION ADMINISTRATION

REGULATIONS

- 12 CFR Part 721: Federal Credit Union Incidental Powers Activities
- 12 CFR Part 748: Security Program, Report of Crime and Catastrophic Act and Bank Secrecy Act Compliance
- 12 CFR Part 716: Privacy of Consumer Financial Information & Appendix
- 12 CFR Part 741: Requirements for Insurance

GUIDANCE

- NCUA Letter to Federal Credit Unions 02–FCU–11: Tips to Safely Conduct Financial Transactions over the Internet—An NCUA Brochure for Credit Union Members (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 Regulatory Alert 01–RA–03: Electronic Signatures in Global and National Commerce Act (E-Sign 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 (with Enclosure) (December 2000)
- NCUA Letter to Credit Unions 00–CU–07: NCUA's Information Systems & Technology Examination Program (October 2000)
- NCUA Letter to Credit Unions 00–CU–04: Suspicious Activity Reporting (see section on "Computer Intrusion") (June 2000)
- NCUA Letter to Credit Unions 00–CU–02: Identity Theft Prevention (May 2000)
- NCUA Regulatory Alert 99–RA–3: Pretext Phone Calling by Account Information Brokers (February 1999)
- NCUA Regulatory Alert 9–-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)
- NCUA Letter to Credit Unions 97–CU–1: Automated Response System Controls (January 1997)
- NCUA Letter to Credit Unions 109: Information Processing Issues (September 1989)

OFFICE OF THE COMPTROLLER OF THE CURRENCY

REGULATIONS

- 12 CFR Part 21, Subpart A: Minimum Security Devices and Procedures
- 12 CFR Part 21, Subpart B: Reports of Suspicious Activities
- 12 CFR Part 21, Subpart C: Procedures for Monitoring Bank Secrecy Act Compliance
- 12 CFR Part 30, Appendix A: [Interagency] Guidelines Establishing Standards for Safety and Soundness
- 12 CFR Part 30, Appendix B: [Interagency] Guidelines Establishing Standards for Safeguarding Customer Information

GUIDANCE

- OCC Bulletin 2001–47: Third-Party Relationships (November 1, 2001)
- OCC Advisory Letter 2001–8: Authentication in an Electronic Banking Environment (July 30, 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 2001–8: Guidelines Establishing Standards for Safeguarding Customer Information (February 15, 2001)
- OCC Advisory Letter 2000–12: Risk Management of Outsourcing Technology Services (November 28, 2000)
- OCC Alert 2000–9: Protecting Internet Addresses of National Banks (July 19, 2000)
- OCC Bulletin 2000–19: Suspicious Activity Report (June 19, 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 Bulletin 99–20: Certificate Authority Guidance (May 4, 1999)
- OCC Bulletin 98–38: Technology Risk Management: PC Banking (August 24, 1998)
- OCC Bulletin 98–3: Technology Risk Management (February 4, 1998)

OFFICE OF THRIFT SUPERVISION

REGULATIONS

- 12 CFR Part 555: Electronic Operations
- 12 CFR 563.177: Procedures for Monitoring Bank Secrecy Act Compliance
- 12 CFR 563.180: Suspicious Activity Reports and Other Reports and Statements
- 12 CFR Part 568: Security Procedures Under the Bank Protection Act
- 12 CFR Part 570, Appendix A: Interagency Guidelines Establishing Standards for Safety and Soundness
- 12 CFR Part 570, Appendix B: Interagency Guidelines Establishing Standards for Safeguarding Customer Information
- 12 CFR Part 573: Privacy of Consumer Financial Information

GUIDANCE

- CEO Ltr 70: Statement on On-Line Personal Computer Banking (June 23, 1997)
- 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 (June 1, 2000 (transmits final rule for privacy of consumer financial information)
- CEO Ltr 139: Identity Theft and Pretext Calling (May 4, 2001)
- CEO Ltr 143: Interagency Guidance on Authentication in an Electronic Banking Environment" (August 9, 2001) (transmits FFIEC document, Authentication in an Electronic Banking Environment)
- CEO Ltr 155: Interagency Guidance: Privacy of Consumer Financial Information. (February 11, 2002)
- Thrift Activities Handbook Section 341, Technology Risk Controls