iad INTERNAL AUDITORS DIVISION
An Affiliate of SIFMA™

# Internal Audit Guidelines

# Information Security

## February 2009

The Audit Guidelines (the "guidelines") are intended to provide members of the Internal Auditors Division (“IAD”), an affiliate of the Securities Industry and Financial Markets Association (“SIFMA”) with information for the purpose of developing or improving their approach towards auditing certain functions or products typically conducted by a registered broker-dealer. These guidelines do not represent a comprehensive list of all work steps or procedures that can be followed during the course of an audit and do not purport to be the official position or approach of any one group or organization, including IAD or any of its divisions or affiliates. Neither IAD, nor any of its divisions or affiliates, assumes any liability for errors or omissions resulting from the execution of any work steps within these guidelines or any other procedures derived from the reader's interpretation of such guidelines. In using these guidelines, member firms should consider the nature and context of their business and related risks to their organization and tailor the work steps accordingly. Internal auditors should always utilize professional judgment in determining appropriate work steps when executing an audit.

iad INTERNAL AUDITORS DIVISION
A Division of SIFMA

# TABLE OF CONTENTS

iad INTERNAL AUDITORS DIVISION
A Division of SIFMA

# I. Introduction and Background

# I. INTRODUCTION AND BACKGROUND

## A. Overview

A firm's information assets are one of the most valuable resources in business today. Information is increasingly vital for competitive success and essential for economic survival. In today's interconnected world, organizations must take specific and concrete steps to protect their information assets from unauthorized use and the risks generated by the subsequent misuse of that information, whether intentional or not.

The ISO/IEC 27002 (17799) Code of Practice for Information Security Management (ISO) is the most widely used framework by organizations around the world for information security. The overall purpose of the ISO is to provide a common basis and platform for developing organizational information security standards for all types of firms.

A key component of a good firm-wide information security program requires an assessment of risk as well as the development and implementation of an information security risk management program. An information security risk assessment process is utilized to determine the extent of potential threats and risks associated within the environment being evaluated. The best known information security risk assessment that is widely used by many firms is the NIST (National Institute of Standards and Technology) Special Publication 800-30. The NIST is published by the Technology Administration Department of Commerce and is considered public domain as well as industry "best practice".

A thorough risk assessment should include the following:

- Identifying and categorizing information that would be at risk if not secured properly.
- Identifying threats that could harm and, thus, adversely affect critical information security assets. Threats include such things as intruders, criminals, disgruntled employees, terrorists, and natural disasters.
- Estimating the likelihood that such threats will materialize based on historical information and judgment of knowledgeable individuals.
- Identifying and ranking the value, sensitivity, and criticality of information assets that could be affected should a threat materialize in order to determine which information security assets are the most important.
- Estimating, for the most critical and sensitive information security assets, the potential losses or damage that could occur if a threat materializes, including recovery costs.
- Identifying cost-effective actions to mitigate or reduce the risk. These actions can include implementing new organizational policies and procedures as well as technical or physical controls.

The results of a thorough risk assessment should be documented and an action plan developed to mitigate or otherwise manage the identified risks to information security assets. A risk management plan should at a minimum address the following activities:

- Prioritizing information security assets that should be secured.

- Verifying that information security is included in job responsibilities.
- Ensuring that confidentiality agreements are used with third party vendors, contractors, and other external parties that have access to a firm's information assets.
- Defining information security requirements for automated systems.
- Determining if security is applied to the handling of physical media, both onsite and off-site encrypted as appropriate.
- Verifying that security governance covers at a minimum the following areas:
  - Security Organization inclusive of an information security strategy and information security officer
  - Policies, guidelines, standards, and procedures for information security
  - Security awareness and training
  - Threat and risk assessment including vulnerabilities
  - Information and data classification and protection
  - Security administration and operations management processes inclusive of physical and logical security where applicable)
  - Monitoring and escalation to senior management

The Information Systems Audit and Control Association (ISACA) developed an audit program for information security that closely aligns with the ISO. The "ISACA Security Management Guidelines" is also used as a reference for the guidelines covered herein.

## B. Information Security Standards Background

Where appropriate the audit guidelines draw upon recommendations and best practices advocated by the following organizations:

### ISO/IEC 27002 (17799) Code of Practice for Information Security Management ("ISO")

ISO/IEC 27002 establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization. The objectives outlined provide general guidance on the commonly accepted goals of information security management. ISO/IEC 27002 contains best practices of control objectives and controls in the following areas of information security management:

- Security Policy - Developing, maintaining, approval and employee awareness.
- Organization of Information Security - Roles and responsibilities, senior management sponsorship.
- Asset Classification and Control - An inventory or register of the important assets associated with each information security system and insuring that each asset identified has an owner, the security classification defined and agreed, and its location identified.
- Risk Assessment and Mitigation - Assessing the risk of threats to information security classified by different asset classes (hardware, software, data, etc.) and a management plan to mitigate the identified threats and risks.
- Human Resource Security – Information security as applied in job definitions and resourcing requirements as necessary to support the security policy.
- Physical and Environmental Security – The physical locations of hardware and software used to store and process proprietary information.

- Communications and Operations Management - Operating procedures and process for ensuring policies are enforced and monitored.
- Access Control - Access control policy, user access management, and review of user rights with respect to proprietary information.
- Information Systems Acquisition, Development, and Maintenance – Information security requirements as applied to new systems or for enhancement to existing systems that store and process proprietary information.
- Information Security Incident Management - Incident reporting process, escalation, risk convergence reporting.
- Business Continuity Management - A managed process for maintaining operations and control of proprietary information with respect to business processes, hardware, and software that are used to store and process proprietary information.
- Compliance – Assurance that information security policy and processes are consistent with relevant statutory, regulatory and contractual requirements.

The control objectives and controls in ISO/IEC 27002 are intended to be implemented to meet the requirements identified by a risk assessment. ISO/IEC 27002 is intended as a common basis and practical guideline for developing organizational security standards and effective security management practices, and to help build confidence in inter-organizational activities.

The ISO/IEC 27002 (17799) Code of Practice for Information Security Management is available for download at:

http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=50297

### National Institute of Standards and Technology (NIST) Risk Management Guide

The guiding principle put forth by NIST with respect to information security is that an effective risk management process is an important component of a successful IT and information security program. The principal goal of an organization’s risk management process should be to protect the organization and its ability to perform their mission, not just its IT and data assets. Therefore, the risk management process should not be treated primarily as a technical function carried out by the IT experts who operate and manage the IT system, but as an essential management function of the organization. The components of the risk management processes discussed in this publication and as they relate to a standalone information security audit include the following:

- Risk Management Overview
- Risk Assessment
- Risk Mitigation
- Evaluation and Assessment

The Risk Management Guide, Special Publication 800-30, is available for download at: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

### ISACA Security Management Guidelines

ISACA provides control objectives for information, information security, and related technology as a governance framework and supporting tool. It allows firms to bridge the gaps amongst audit control requirements, technical issues and business risks. It is intended for use by business and IT management as well as IS auditors; therefore, its usage enables the understanding of business objectives and communication of good practices and recommendations to be made around a commonly understood and well respected framework and enables clear policy development and good practice for information security throughout organizations.

ISACA documentation is available for download on the ISACA web site, www.isaca.org/.

Some of the concepts provided in the ISACA framework and embodied in these audit guidelines include the following:

- Control Objectives - Generic statements of minimum good control in relation to information security.
- Management Guidelines - Guidance on how to assess and improve IT security of information assets. They provide a management-oriented framework for continuous and proactive self-assessment.
- Control Practices - Risk identification and value statements and implementation guidance for the control objectives.
- Assurance Guide - Guidance for each control area on how to obtain an understanding, evaluate each control, assess compliance and substantiate the risk of controls not being met.

## C. Audit Objective

The primary objective of an information security audit is to understand and confirm how its security function has been established with respect to information security. Additionally, it is important to evaluate the effectiveness and efficiency of the overall management framework for the firm’s information security function and identify the key specific aspects of that function.

This information security audit guideline, risk assessment and audit program provides detailed guidance to assess and evaluate the information security management framework in an organization. A good firm-wide information security management framework would include a comprehensive strategy to protect assets including information, data, and the corporate technology infrastructure. Additionally, it would include effective methods for monitoring and enforcing the policies and procedures set forth within the security management framework. Information Security is a critical component of the overall risk management effort and provides the means for protecting the firm’s confidential and sensitive information (e.g., personal data, financial and product information, customer information, and network information) and other critical assets. A good information security program helps promote a broad understanding of the security function, establishes policies, standards and procedures that highlight the firm’s key security risks and the steps being taken to address and mitigate them.

## D. Audit Scope

The scope of examinations covered by the audit guidelines may be used to determine the quality and effectiveness of the organization's governance of security related to information assets. The topic of information security is very broad in scope and could conceivably cover just about all security-related aspects (e.g., information security risk assessments, administration and monitoring of logical security, database security, physical security, application security, network security, development and maintenance of an Information Security Policy and Standards, and security incident reporting) of the firm. Many of these topics and their related security controls are typically covered in specific infrastructure audits (e.g., Windows, UNIX, Database, Networks, Data Center, and Electronic Communications). However, the areas that are not usually covered in any great detail are the functions that specifically relate to the governance of information security policies, procedures, and systems. It is these additional functions that will be covered by these audit guidelines, with a particular focus on the guidelines and principals set forth by ISO/IEC 27002. (See the SIFMA IAD website as separate guidelines may exist for the above noted infrastructure audits.)

## E. Risk

### Audit Risks

The following typical risks are assumed to be relevant to the audit of information security:

### Information Security Risks

Information systems have long been at some risk from malicious actions or inadvertent user errors and from natural and man-made disasters. In recent years, systems have become more susceptible to these threats because computers have become more interconnected and, thus, more interdependent and accessible to a larger number of individuals. In addition, the number of individuals with computer skills is increasing, and intrusion, or "hacking," techniques are becoming more widely known via the Internet and other media. If the technology environment is also not properly aligned to meet information security requirements, the firm can be subject to additional risks and threats to its information security assets.

Damage to, loss of, or unauthorized use of information security assets could cause both financial and reputational damage to a firm. Identifying and securing critical information security assets is critical to a firm's success and ability to continue operations, especially in today's inter-connected, electronic, and highly mobile global environments. The following risks are outlined for each of the ISO/IEC 27002 areas:

1. **Security Policy**

   Establishing information security policies and standards alone does not guarantee the security of information and data assets. The damage that can result from inadequate knowledge of existing policies and procedures could result in breaches of information security, compromised, lost, or stolen data, and other malicious practices that could disrupt the entire information security infrastructure. Without an awareness program and / or periodic training information security may not be operating at maximum levels.

### 2. Organization of Information Security

Without clearly defined responsibilities for creating, implementing, and ensuring compliance with information security policies information security within the organization may not be effective. Additionally, without a defined structure to enable clear reporting lines and communication to upper management poor segregation of duties may exist.

### 3. Asset Classification and Control

Without proper inventory and classification of data, applications and systems improper strategic and risk management planning could occur.

### 4. Risk Assessment and Mitigation

Management may not be able to properly assess the likelihood of an event occurring if the process to identify potential threats and vulnerabilities and their impact is not performed; specifically:

- A threat is the potential for an action to be exercised, either accidentally or intentionally, for the purpose of exploiting a specific vulnerability.
- Vulnerability is defined as a flaw or weakness in an information system, associated procedure, or existing control that can result in a breach or violation of the information security policy. Vulnerabilities have no impact if a relevant threat is not present.

### 5. Human Resource Security

Employees, contractors, and third parties may not know the importance of the organization’s security practices that could result in abuse (e.g., theft and misuse) of security.

### 6. Physical and Environmental Security

Failure to secure the physical locations of operational areas, hardware and software used to store and process proprietary information could result in unauthorized access and the malicious destruction or theft of proprietary information resulting in the inability to continue business operations, lost revenue, and / or reputational damage to the firm.

### 7. Communications and Operations Management

Without operating procedures and processes, policies may not be monitored and violations may not be addressed in a timely manner.

### 8. Access Controls

Without an access control policy, user access management, and reviews of user rights may not ensure that unauthorized persons do not gain access to a firm’s physical premises, resources, computer systems, or data for malicious and harmful purposes.

### 9. Information Systems Acquisition, Development, and Maintenance

The acquisition, testing, and implementation of third party software as well as the development and maintenance of internal applications may not have the proper oversight to prevent back channels and hidden code that could be used to gain unauthorized access to proprietary information assets. Test data used in non-production environments during the development and testing computer systems is often a copy of production data and requires its own set of access and control policies to prevent breaches of security information.

### 10. Information Security Incident Management

The lack of audit logs, active monitoring, and incident escalation may allow unauthorized breaches of the information security infrastructure to go undetected.

### 11. Business Continuity Management

Without a documented business continuity management and a business continuity plan ("BCP") the firm and its employees may not be able to survive a disaster and to re-establish critical operations required to support the business within the timeframes set out by the business managers. A partial recovery coupled with the failure to address the recovery of processing systems used to secure information assets could lead to the loss of proprietary information while the firm operates in a recovery mode.

### 12. Compliance

Compliance issues may arise if management and personnel are unaware of or do not fully understand their obligations with respect to information security and regulatory requirements or if oversight of the information security infrastructure and processes are not sufficient to ensure compliance.

### Prior Audit Issues

An effective audit process includes a firm's commitment to addressing issues that arise out of prior information security audits and therefore all audits should include a review of these follow-up activities. An individual or small group from the firm should be designated with the authority and responsibility to follow up and report on progress towards implementing all prior audit recommendations through coordination with appropriate management. They should also fulfill the obligation to communicate the implementation status of prior audit recommendations to executive sponsors, management, and internal auditors. This individual or small group should also be accountable to ensure implementation efforts fully resolve audit issues or findings on a timely basis. Failure to follow-up and resolve prior audit issues may impair a firm's ability to meet regulatory compliance obligations for information security assets such as e-mail and messaging systems.

iad INTERNAL AUDITORS DIVISION

A Division of SIFMA

# II. Audit Guidelines

# II. AUDIT GUIDELINES

| **Risk to Be Managed** | **Types of Controls to Manage / Eliminate Risks** | **Potential Audit Work Steps** |
|---|---|---|
| **A. Overall Scope** | | |
| Lack of awareness around factors that present the greatest degree of risk to the firm with respect to information security in order to support critical business operations and maintain operational integrity. | Determine examination scope and approach for reviewing information security with management.<br>The scope, objectives, and approach will be discussed with management prior to commencing the review.<br>Management's review and approval of final report. | • Interview management and appropriate information security operations staff to identify:<br>• Any significant changes in business strategy or internal business processes that could affect the operation of information security.<br>• Any material changes in the audit program, scope, or schedule related to information security activities.<br>• Key management changes.<br>• Information technology environments and changes to information security configuration or components.<br>• Changes in key service providers (messaging, archival and retrieval, back-up / recovery, etc.).<br>• Any other internal or external factors that could affect the information security process.<br>• Determine management's consideration of newly identified threats and vulnerabilities to the organization's information security process. Consider:<br>• Technological and security vulnerabilities<br>• Internally identified threats<br>• Externally identified threats (including known threats published by information sharing organizations)<br>• Review and discuss all audit issues raised during the current examination with management and include responses prior to report issuance. |

| Risk to Be Managed | Types of Controls to Manage / Eliminate Risks | Potential Audit Work Steps |
|---|---|---|
| **B. Security Policy** | | |
| **B.1 Information Security Policy** | | |
| Security policies and standards are not documented resulting in lost, stolen, or misuse of strategic information. | An Information Security Policy has been developed and documented to identify the Company's information security objectives.<br>Security Policy and Standards should be comprehensive and address all areas of the firm. | • Verify that Information Security Policies have been developed.<br>• Determine if the relevant policies, procedures, guidelines and standards documents are up-to-date, accurate, complete, signed off by management and published.<br>• Verify that they include information about owners, revision information, scope, roles and responsibilities and relevant controls.<br>• Obtain and review the policy to determine if the policy includes the following:<br>  • States both the mandate and the charter from senior management supporting the goals and principles of information security.<br>  • Highlights the business risks associated with a breakdown in information security.<br>  • Defines information security, responsibilities, and the high-level principles to be observed.<br>  • Requires that information is protected in terms of its requirements for availability, integrity, and confidentiality.<br>  • Prohibits unauthorized or personal use of the organization's information and systems.<br>  • States that disciplinary action will be taken against individuals who violate its provisions. |
| The information security policy may not be appropriate or effective. | Effective security policies are based on best practices and a robust process that identifies and categorizes the risk for the firm. | • Determine if the Information Security Policy has been developed based on best practices by reviewing the following:<br>  • Developed based on past experiences the organization has had with security breaches, and includes sections addressing items such as- "restriction on sharing of IDs and passwords between |

| Risk to Be Managed | Types of Controls to Manage / Eliminate Risks | Potential Audit Work Steps |
|---|---|---|
| | | users; modification of access after an employee has been terminated or changed departments and / or functions; highlighting users who may be signing on from someone else's workstation to determine if it is appropriate; etc.<br>• Existence of security best practices and monitoring tools and programs for all key systems.<br>• Contain key performance indicators (KPIs) that are used to assess the organizations security policies.<br>• Application of access policies to users and controls to restrict access to information and computer systems. |
| Unauthorized access to confidential information results in reputational damage. | The identification and categorization of risks provide sound solutions for optimizing allocation of resources.<br>Guidance on securing confidential data should limit access to authorized individuals on a need to know basis using access controls should be addressed in the policy. | • Application of access policies to users and steps to control access to information and computer systems.<br>• Existence of security best practices for all key systems and are they monitored.<br>• Verify if Information Security Policies exist with respect to handling, protection and management of personal data and that they are documented, signed off by senior management and published.<br>• Determine if the Information Security Policies include data identification and classification over the personal data. |
| **B.2 Review and Approval** | | |
| The information security policy may not support management objectives in protecting strategic company assets. | An Information Security Policy should be approved by all management and stakeholders as well as communicated and acknowledged by company personnel. | • Verify that senior management is responsible for reviewing and approving security policies.<br>• Determine through interviews with Security Management if an approved Information Security Policy has been developed and documented to identify the firm's information security objectives such as: |

| Risk to Be Managed | Types of Controls to Manage / Eliminate Risks | Potential Audit Work Steps |
|---|---|---|
| | The Information Security Policies should be reviewed, approved by senior management, and updated periodically. | • Assess rights to IT resources<br>• Monitoring and reporting on security violations<br>• Password administration procedures and enforcement<br>• Verify that the policy has been communicated to company personnel who are required to sign and acknowledge the contents of the Information Security Policy.<br>• Determine if independent privacy oversight and review mechanisms have been established.<br>• Determine whether access control policies are periodically reviewed, approved and updated in response to new threats, capabilities, business requirements or access violations. |
| **B.3 Communicate the Information Security Policy** | | |
| Security policies and standards are not communicated to all employees resulting in ineffective and inconsistent security levels. | Information Security Policies should be periodically communicated throughout the firm.<br>All employees, contractors, and vendors should be aware of and understand relevant sections of the Information Security Policies and that they are responsible for adhering to it. | • Verify that the policies exist on the intranet and are available for all employees to access.<br>• Ensure that a process exists to verify that all employees have read the policies and understand the sections relevant to them.<br>• Verify that the policies have been communicated effectively to all employees, consultants, contractors, and external parties.<br>• Determine if third party contracts include clauses to ensure that consultants and contractors will comply with the firm's security policy as well as keep the firm's data confidential. |

| Risk to Be Managed | Types of Controls to Manage / Eliminate Risks | Potential Audit Work Steps |
|---|---|---|
| **C. Organization of Information Security** | | |
| **C.1 Security Governance** | | |
| Data integrity and confidentiality strategy for the firm may be compromised without adequate governance and oversight ultimately increasing the operational risk of the firm. | Adequate governance framework exists by the Board of directors and oversight is provided through their sponsorship of the security program.<br>There should be direction and commitment to information security by senior management.<br>Security framework and supporting documentation has been formally communicated to all relevant parties. | • Verify if a security strategy (e.g., mandate, framework, charter, and mission) within the firm has been documented.<br>• Determine if the security mandate corresponds with the scale and complexity of the firm's operations.<br>• Determine the adequacy of the governance framework over the Board of directors and the oversight they provide and their sponsorship of the security program within the bank.<br>• Determine if executive sponsorship exists and supports the information security program.<br>• Determine if the security framework and supporting documentation has been formally communicated to all relevant parties and stakeholders. |
| **C.2 Roles and Responsibilities** | | |
| Security Organization<br>Ineffective security due to poor definition and understanding of security roles and inadequate resources and authority for information security. | There should be a defined structure to enable clear reporting lines and communication to upper management.<br>There should be a formally approved organization chart of the Security Governance function and sub-functions exist internally within the firm. | • Determine if there is a person designated who represents the leadership and overall management aspect of information security.<br>• Determine if a formally approved organization chart of the security governance function and sub-functions exists internally within the firm.<br>• Discuss with responsible management the reporting lines in place for the responsibility of the information security function. Determine if there is a security committee either locally and / or globally that is used to discuss and decide security requirements.<br>• Determine if management requests an independent review of controls, policies, standards, and procedures periodically and when significant. |

| Risk to Be Managed | Types of Controls to Manage / Eliminate Risks | Potential Audit Work Steps |
|---|---|---|
| | | • Identify if a dedicated "Information Security Officer", who has overall responsibility for Information Security, has been appointed to review the business process for Information Security implications; and that his / her duties, authority and reporting structure have been documented.<br>• Determine if the firm's security management and / or security officer are included in the firm's emergency management committee, and if emergency security response plans have been developed for each of the firm's key facilities, including a point of contact for each. |
| Information Security Coordination<br>Control weaknesses due to unclear assignment of responsibilities and an inadequate security function ultimately increasing the operational risk of the firm. | A security administration function exists and is located at an appropriate organization level to ensure proper enforcement of Information Systems security policies and procedures.<br>Security efforts are coordinated across the firm.<br>Specialists support various platforms and applications and are responsible for security of the application and / or operating systems. | • Determine through interviews with security management if:<br>  • A security administration function exists.<br>  • Clear documentation of security administration roles and responsibilities exist and has been appropriately approved.<br>  • The function is located at an appropriate organization level to ensure proper enforcement of Information Systems security policies and procedures.<br>  • The administration function is adequately staffed.<br>• Determine what groups or roles are actively involved in information security within the firm.<br>• Verify if an information security committee has been established, which comprises of key stakeholders / users / senior management from various departments whose purpose is to oversee and coordinate security issues throughout the firm; and examine meeting minutes and / or other information to determine how effectively they are executing their responsibilities. |

| **Risk to Be Managed** | **Types of Controls to Manage / Eliminate Risks** | **Potential Audit Work Steps** |
|---|---|---|
| Segregation of Duties<br>Breakdown of controls, major availability problems, fraud, etc. can be caused by a single individual. | Staff responsibilities are allocated in such a way as to ensure segregation of duties.<br>Access to administration functions for multiple platforms (e.g., operating system, database, applications) should be properly segregated. | • Determine what security administration functions are distributed to the various people (including Information Security) throughout the organization. Establish whether any security functions are incompatible with each other. Such examples of potential incompatible duties are:<br>• Security administration<br>• Security monitoring and incident reporting<br>• Policy setting<br>• Risk management<br>• Determine which platforms / infrastructure that the Information Security Group is responsible for. Review the security permissions for each of the platforms / infrastructure and determine appropriateness of segregation of functions. |
| **C.3 Security Staff Training** | | |
| Weak information security may be caused by incompetent staff responsible for the operation, administration or maintenance of the environment. | Information Security staff has a minimum level of experience and there are ongoing training plans in place to ensure that all staff have the requisite skill set. | • Discuss with management how experienced the Information Security staff is, and what ongoing training is performed to ensure that their skills are updated. |
| **C.4 Strategy and Project Management** | | |
| Strategy and Benchmarks<br>There is no clear strategic plan or objectives for the Information Security. | Important security related projects should be discussed with CIO and IT managers in informal sessions where specific security strategy and objectives will be decided. | • Verify that the information security strategic plan addresses the needs of the business and reflects the business strategy and that each new project has representation from the Security Organization within the firm. |

| Risk to Be Managed | Types of Controls to Manage / Eliminate Risks | Potential Audit Work Steps |
|---|---|---|
| Progress Reports<br>Senior IT management is not kept up to date with developments in Information Security. Management information regarding Information Security project status (progress, cost vs. budget) against defined plans is not produced and disseminated appropriately. | Project progress reports and other updates should be produced regularly and distributed to appropriate recipients. | • Identify Information Security projects and ascertain how project progress is tracked and reported.<br>  • Are reports prepared on a regular basis?<br>  • Who receives the reports? Are the reports adequate?<br>• Review whether reports are complete and accurate and produced within an acceptable timeframe.<br>• Examine Security Projects over the past year to determine if they have been delivered on time, and on budget. |
| External Parties<br>Information security risks may not be identified before engaging into operations with an external party. | Procedures should exist for permitting third party access to the firm's resources. These procedures could be in the form of a security risk assessment or impact analysis. | • Determine if there is a process for assessing the risk of allowing third-parties access to our firm's resources.<br>• Describe how external parties are made aware of their information security responsibilities as it relates to the firm.<br>• Determine if there is a formal access control policy regarding third-party access.<br>• Determine if the third-party agreements / contracts include firm requirements for information security. |
| **D. Asset Classification and Control** | | |
| **D.1 Accountability of Assets** | | |
| Inventory Assets<br>Lack of an adequate inventory of assets crucial to information security will hinder risk assessment and mitigation plans thereby resulting in the possible loss, theft, or damage of proprietary information. | The firm should periodically inventory and review its information security assets. | • Determine what information is accounted for as assets (e.g., computer systems, software applications, and operating systems).<br>• Verify that inventories are taken on a regular basis and that appropriate reviews are scheduled by individuals responsible for information security. |

| **Risk to Be Managed** | **Types of Controls to Manage / Eliminate Risks** | **Potential Audit Work Steps** |
|---|---|---|
| **D.2 Security Classification** | | |
| Classification of Information<br>The firm may not adequately protect all important and critical assets. Unnecessary vulnerabilities and risks could exist. | The firm should evaluate its information and systems in order to establish the appropriate criticality classification to the data. Thereafter the Organization should have approved security procedures for the treatment of each classified layer of data.<br>All assets should be accounted for and inventoried. The inventory should be maintained and updated as needed.<br>All assets should be assigned an owner. | • Determine if an information security classification scheme is used and if critical programs and data within the bank have been specifically identified and classified with respect to security requirements. Classifications should consider the following:<br>  • Specify that information and systems should be classified according to its criticality, sensitivity, and vulnerability to particular threats.<br>  • Take account on the business impact of a loss of confidentiality, integrity, and availability.<br>  • Apply to all information in electronic and paper form and all software and hardware.<br>  • Be applied to new systems at their development stage and existing systems.<br>  • Consider users and usage of data as non-classified, internal use, restricted distribution, secret, or insider info.<br>• Determine whether critical information and systems are distinguished from other information and systems, recorded in an inventory maintained at a firm level, signed-off by a business owner, and protected in line with its classification.<br>• Determine if there is an assignment of assets to a specific individual to ensure that the information security policy is followed. |
| **E. Risk Assessment and Mitigation** | | |
| **E.1 Risk Assessment Policies and Procedures** | | |
| Since risks and threats change over time, it is critical that organizations maintain and update risk mitigation plans. | Efficient and effective implementation of the firm's information security risk assessment programs and | • Determine if the firm has a risk assessment policy that addresses the following:<br>  • Has senior management support and involvement. |

| **Risk to Be Managed** | **Types of Controls to Manage / Eliminate Risks** | **Potential Audit Work Steps** |
|---|---|---|
| Failure to periodically reassess risks and reconsider the appropriateness and effectiveness of the policies and controls they have selected may result in damage or loss of information security assets from unidentified threats and vulnerabilities. | factors that help ensure that the organization benefits from the expertise and experience of their senior managers and staff, that risk assessments were conducted efficiently, and that the assessment results led to appropriate remedial actions. | • Designates a responsible person or group for conducting the assessment.<br>• Refers to a procedure for conducting the assessment.<br>• Involves business and technical experts.<br>• Produces an action plan to mitigate identified risks.<br>• Holds business units responsible for mitigating risks.<br>• Insure that properly defined risk assessment procedures include at a minimum the following:<br>• Specifies key activities to be undertaken, which include carrying out security classifications and risk analysis, safeguarding important records, monitoring, reporting and correcting suspected security weaknesses and reporting them to management.<br>• Who was responsible for initiating and conducting risk assessments?<br>• Who was to participate?<br>• What steps were to be followed?<br>• How disagreements were to be resolved?<br>• What approvals were needed?<br>• How assessments were to be documented?<br>• How documentation was to be maintained?<br>• To whom reports were to be provided? |
| **E.2 Information Security Risk Assessment** | | |
| <u>Threats and Vulnerabilities</u><br>Failure to identify the potential unauthorized access, use, disclosure, disruption, or destruction of information and systems that support the | The firm should conduct risk assessments of the risk and magnitude of harm that could result from unauthorized access. | • Determine if the Information Security function has conducted a threat / risk assessment of security exposures in accordance with the firm's threat / risk assessment program.<br>• Determine whether there is a risk assessment process that includes the identification of threats and vulnerabilities, likelihood determination, |

| **Risk to Be Managed** | **Types of Controls to Manage / Eliminate Risks** | **Potential Audit Work Steps** |
|---|---|---|
| operations and assets of the firm may create operational risk. | | and impact analysis.<br>• Determine whether reliable sources such as NIST, CERT, SANS, and / or FEMA are used to help identify potential threats.<br>• Determine if threat sources (natural threats, human threats, and environmental threats) are considered for the risk assessment process.<br>• Determine if the risk assessment process includes the control level of effectiveness that ultimately determines the residual risk level.<br>• Determine if a report of the risk assessment results is created for management that includes control recommendations that need to reduce any remaining significant risks.<br>• Determine if an Information Security impact assessment has been performed for the business.<br>• Determine if the assessment addresses the collection, transmission, maintenance and disclosure of secure information that may be carried out in more than one operating location. |
| **E.3 Critical Business Applications** | | |
| Application Risks<br>Lack of an understanding of the criticality of an application that has access to sensitive data may result in a business impact of a loss of confidentiality, integrity, or availability of data. | Critical business applications that have access to information security and data assets requires a more stringent set of information security controls than other applications. | • Determine if information security requirements are assessed for new or existing applications based on criteria used for risk assessment.<br>• Determine if applications (new and existing) are classified using a security classification scheme based on its security requirements. The scheme should take account of the:<br>• Business impact of a loss of confidentiality, integrity, or availability.<br>• Sensitivity of information stored in or processed by the application.<br>• Vulnerability of the application to particular threats.<br>• Type (including transaction processing, process control, funds |

| **Risk to Be Managed** | **Types of Controls to Manage / Eliminate Risks** | **Potential Audit Work Steps** |
|---|---|---|
| | | transfer, customer focus, and desktop applications)<br>• Size (e.g., applications supporting many users or just a few) |
| **E.4 Risk Mitigation** | | |
| Risk Mitigation Strategy<br>Failure to mitigate risk from potential threats and vulnerabilities may result in loss, destruction, or malicious change to information security assets. | There should be a process in place for prioritizing, implementing, and maintaining the appropriate risk-reducing measures recommended from the risk assessment process. | • Determine if risk mitigation strategies and processes have been developed and put in place that addresses the threats and vulnerabilities documented within the threat / risk matrix.<br>• Determine if there is an approach for implementing controls based on the risk level. |
| **F. Human Resource Security** | | |
| **F.1 Security in Job Definition and Resourcing** | | |
| Failure to include information security as each employee's responsibility will hinder awareness programs and result in breaches harmful to the firm. | Include information security in job responsibilities, personnel screening and policy setting,<br>Make use of confidentiality agreements as terms and conditions of employment. | • Determine that security roles and responsibilities as laid in Organisation's information security policy are documented where appropriate. This should include general responsibilities for implementing or maintaining security policy as well as specific responsibilities for protection of particular assets, or for extension of particular security processes or activities.<br>• Determine if verification checks on permanent staff were carried out at the time of job applications. This should include character reference, confirmation of claimed academic and professional qualifications and independent identity checks.<br>• Determine if employees are asked to sign Confidentiality or non-disclosure agreement as a part of their initial terms and conditions of the employment and that the agreement covers the security of the information processing facility and organisation assets.<br>• Determine if terms and conditions of the employment covers the employee's responsibility for information security. Where |

| Risk to Be Managed | Types of Controls to Manage / Eliminate Risks | Potential Audit Work Steps |
|---|---|---|
| | | appropriate, these responsibilities should continue for a defined period after the end of the employment.<br>• Determine if there is a process for termination responsibilities. Determine whether management defined termination and change of employment process for information security. Does the process include the removal of access rights? |
| **F.2 User Awareness, Education, and Training** | | |
| Security Awareness and Training<br>Employees and users may not be aware of good security practices, leading to shared passwords, unlocked workstations, etc., increasing the risk of unauthorized access.<br>The security policy does not prohibit employees from using the firms systems for non business and purposes that are not work related. | A Security Awareness Program reminding individuals of the security policies of the firm, and their responsibility and accountability exists.<br>There should be appropriate training and notification to employees to remind them of the importance of maintaining information security.<br>Awareness of information security should be maintained via effective awareness programs covering all individuals with access to sensitive information or systems. | • Review the security awareness and training program to determine if it is consistent with information security policies.<br>• Verify if the information security policies and procedures have been communicated to the persons concerned with correspondence and / or training.<br>• Determine if appropriate security training is provided to both security specialists as well as to employees of the firm such as routine periodic awareness sessions to inform and remind individuals of their security responsibilities, issues, and that concerns and briefings are conducted regarding responsibilities and accountability attached to the security screening levels.<br>• Review the security awareness and training program to assess Determine if it provides clear and comprehensive guidance to employees on acceptable and unacceptable use of confidential, sensitive, and proprietary information.<br>• Review the compliance manual to determine if guidance on protecting confidential documents is included and determine if employees are aware of the manual. |

| **Risk to Be Managed** | **Types of Controls to Manage / Eliminate Risks** | **Potential Audit Work Steps** |
|---|---|---|
| **G. Physical and Environmental Security** | | |
| **G.1 Secure Areas** | | |
| Unauthorized access to the data centre or development workspaces where proprietary information is processed may cause a breach in information security and reputational harm to the firm. | Physical security perimeter and physical entry controls should employed for all areas of an organization where proprietary information is captured, stored, and processed. This includes securing Offices, rooms and data processing facilities where access to proprietary information may be obtained. | • Verify if physical border security facility has been implemented to protect Information processing service areas. Some examples of such security facility are card control entry gate, walls, manned reception, etc.<br>• Determine if entry controls are in place to allow only authorized personnel into various areas within organization where proprietary information is processed.<br>• Determine if the rooms, which have the information processing service areas, are locked or have lockable cabinets or safes.<br>• Determine if information processing service areas are protected from natural and man-made disaster.<br>• Determine if there is any potential threat from neighbouring premises.<br>• Determine if there exists any security control for third parties or for personnel working in secure area and that information is only distributed on need to know basis.<br>• Determine if the delivery area and information processing area are isolated from each other to avoid any unauthorized access.<br>• Determine if a risk assessment was conducted to determine the security in such areas. |
| **G.2 Equipment Security** | | |
| Unauthorized access to the equipment used to store and process proprietary information may cause a breach in information security | Firms should establish plans for equipment site protection including power supplies, cabling security, and equipment maintenance. These plans | • Determine if equipment is located in appropriate places to minimise unnecessary access into work areas.<br>• Determine if the items requiring special protection were isolated to reduce the general level of protection required. |

| **Risk to Be Managed** | **Types of Controls to Manage / Eliminate Risks** | **Potential Audit Work Steps** |
|---|---|---|
| and reputational harm to the firm. | should also include securing of equipment off-premises and secure disposal or re-use of discarded equipment. | • Determine if controls were adopted to minimise risk from potential threats such as theft, fire, explosives, smoke, water, dist, vibration, chemical effects, electrical supply interfaces, electromagnetic radiation, and flood.<br>• Determine if there is a policy towards eating, drinking and smoking on in proximity to information processing equipment.<br>• Determine if environmental conditions are monitored which would adversely affect the information processing facilities.<br>• Determine if the equipment is protected from power failures by using permanence of power supplies such as multiple feeds, uninterruptible power supply (ups), backup generator, etc.<br>• Determine if the power and telecommunications cable carrying data or supporting information services are protected from interception or damage.<br>• Determine if the equipment is maintained as per the supplier’s recommended service intervals and specifications and that maintenance is carried out only by authorized personnel.<br>• Determine if logs are maintained with all suspected or actual faults and all preventive and corrective measures.<br>• Determine if appropriate controls are implemented while sending equipment off premises.<br>• Determine if any equipment usage outside an organisation’s premises for information processing is authorized by management.<br>• Determine if the security provided for equipment while outside the premises are on par with or more than the security provided inside the premises.<br>• Determine if storage device containing sensitive information are physically destroyed or securely over written prior to termination of |

| Risk to Be Managed | Types of Controls to Manage / Eliminate Risks | Potential Audit Work Steps |
|---|---|---|
| | | usage. |
| **G.3 General Controls** | | |
| Failure by employees to secure workstations and other sources of proprietary information assets may result in lost, stolen, or damaged data. | Firms should maintain and enforce a clear desk and clear screen policy.<br>Removal of firm property by employees should be restricted and where permitted monitored by security personnel. | • Determine if automatic computer screen locking facility is enabled. This would lock the screen when the computer is left unattended for a period of time.<br>• Determine if employees are advised to leave any confidential material in the form of paper documents, media, etc., in a locked manner while unattended.<br>• Determine if equipment, information or software can be taken offsite without appropriate authorisation.<br>• Determine if spot checks or regular audits were conducted to detect unauthorized removal of property.<br>• Determine if individuals are aware of these types of spot checks or regular audits. |
| **H. Communications and Operations Management** | | |
| **H.1 Operating Procedures** | | |
| A lack of published operating procedures and guidelines that support the information security policy may result in security beaches to information systems and facilities. | Information security operating procedures should be developed and maintained by management for users of information systems and facilities. | • Determine if there are procedures that address the relevant content within the Information Security Policies and Standards. |

| Risk to Be Managed | Types of Controls to Manage / Eliminate Risks | Potential Audit Work Steps |
|---|---|---|
| **H.2 Monitoring** | | |
| General<br>Lack of monitoring requirements defined in writing, agreed with senior management and documented as part of the Information Security Policy may result in undetected breaches of information security assets. | Active monitoring should be performed periodically and keep senior management informed of key risks as well as encourage "owners" to remedy unacceptable risks. | • Determine if active monitoring occurs across all levels of security (physical, access, network, etc.) as part of the firm's security program. Select a sample and verify if the monitoring activity has been carried out appropriately.<br>• Determine the types of monitoring tools in use, the security events monitored, and the systems monitored with respect to the following:<br>  • Compliance with information security policies and procedures.<br>  • The threat level within the organization.<br>  • The business impact from loss.<br>  • Monitored from a centralized location.<br>  • Prioritized by security risk to the organization. |
| Audit Logging<br>Lack of audit logs and their periodic review may result in undetected breaches of information security assets. | Audit logs of key systems should be available. The retention of these logs should be in compliance with applicable regulations and firm policies. | • Determine if there is a written policy for requiring audit logging.<br>• Determine if time synchronization is used on systems participating in audit logging.<br>• Verify that audit logs are monitored and reviewed and that the frequency is adequate to address threats in a timely manner. |
| Security Monitoring<br>Lack of regular security monitoring as appropriate for the amount of risk to the firm may result in undetected breaches of information security assets. | Significant problems, incidents and errors should be identified, logged, analyzed, communicated to relevant parties for correction, resolved on a timely basis, and escalated to Management.<br>Logs are kept in a centralized log repository with appropriate access permissions. | • Determine if access violations to information or systems are logged.<br>• Determine if information about the security condition of the firm is provided to senior management, a security committee, individuals in charge of critical business applications, and information security management. Information should:<br>  • Provide decision-makers with an informed view of the adequacy of their information security arrangements.<br>  • Reveal areas where improvement is needed.<br>  • Identify information and systems that are subject to unacceptable risks. |

| Risk to Be Managed | Types of Controls to Manage / Eliminate Risks | Potential Audit Work Steps |
|---|---|---|
| | | • Highlight actions to mitigate the risks.<br>• Verify if escalation procedures are defined and implemented to support timely resolution and reporting to Management.<br>• Determine if post mortem meetings are required for significant problems, incidents and errors. They should involve relevant personnel and cover causes, effects, and resolutions. |
| Security Certification<br>Lack of a security certification may indicate inadequate security, control, and review of information security assets. | The firm should conduct an assessment of the key security controls to determine the extent to which the controls are implemented correctly and operating as intended. | • Determine if Information Security personnel periodically assesses the security controls to determine if the controls are effective.<br>• Determine if tools are used to determine the effectiveness (e.g., scanning hosts for known vulnerabilities) of information security. For example: COPS or SATAN. |
| Protection of Logs<br>Unauthorized access to security logs may provide someone the ability to hide unauthorized access to information assets. | Audit and security event logs should be protected from unauthorized tampering or access to ensure the integrity of the data. | • Determine what controls are in place to protect security and audit logs.<br>• For audit logs that contain sensitive information, determine if special care is taken to protect the audit logs from unauthorized disclosure.<br>• Determine how the firm ensures that the security and audit logs are not being altered or tampered with.<br>• Determine if the logs are retained according to firm policy. |
| Media Handling<br>Unprotected media could be compromised. | Media of all types should be protected from unauthorized disclosure or removal, tampering, or destruction. | • Determine if there are policies and procedures for the management of removable media.<br>• Determine whether risks are associated with removable media included in an information security awareness program. |

| **Risk to Be Managed** | **Types of Controls to Manage / Eliminate Risks** | **Potential Audit Work Steps** |
|---|---|---|
| **I. Access Controls** | | |
| **I.1 Access Controls to Information Assets** | | |
| <u>Access Control Policy</u><br>The physical premises, assets and data of the firm may not be adequately secured without an adequate understanding of potential exposures and without an active monitoring program, ultimately increasing the operational risk of the firm. | Management should develop and publish an access control policy that is part of the overall Information Security Policy and Standards.<br>A series of access-related controls should be developed and implemented by management, ranging from policies, guidelines, and processes to actual safeguards that control access to information and data.<br>The user access policy should ensure that all security access requests (physical and logical) are formally documented and approved utilizing a security access request form / system. The security access request forms should be filed and maintained for future reference. | • Determine if the firm's Information Security Policy and Standards include access control policies.<br>• Verify that access to the firm's resources is restricted according to clearly defined access control policies.<br>• Verify that documented procedures for requesting access to the various resources within the firm (Servers, Applications, and Building etc.) exist.<br>• Verify that authorized processes are used to add, modify and remove access, including standing and emergency / temporary access and those exceptions are identified and investigated.<br>• Determine if the procedures for security access requests utilize a security access request form or automated system and test a sample of existing users to insure that the documented processes were followed.<br>• Determine if the security access request forms are filed and maintained for future reference.<br>• Verify that access permissions are removed or re-evaluated on material changes in job responsibilities.<br>• Verify that access permissions are periodically reviewed by management, and the process facilitates effective identification and remediation of issues.<br>• Determine if only authorized system administrators have standing access to administrative functions.<br>• Determine if access permissions are appropriate and granted on a need-to-have basis. |

| Risk to Be Managed | Types of Controls to Manage / Eliminate Risks | Potential Audit Work Steps |
|---|---|---|
| User Access Management<br>Unauthorized access to a firm's physical premises, assets and data could lead to information security breaches. | Access to the firm's information processing environment should be authenticated and authorized in accordance with a formal policy and method.<br>User access should take the least-privileged approach when granting rights and permissions.<br>Management should develop a clear set of procedures that are driven by policy to create and delete users.<br>User access management should ensure that all authorized systems users are assigned individual user IDs and confidential sign-on passwords to ensure accountability for network and application activities. | • Determine if the firm has written procedures for the creation and deletion of user accounts.<br>• Understand how the level of access for each user is determined.<br>• Determine if HR is involved in the creation and deletion of user accounts.<br>• Verify that access to the data centre, physical workspaces, and any locations where secure data could be accessed is authorized and restricted.<br>• Verify that contracts or service agreements with third parties include clauses on information security and protection over data, disclosure of data, and confidentiality of data.<br>• Determine if all authorized systems users are assigned individual user IDs and confidential sign-on passwords to ensure accountability for network and application activities.<br>• Verify that each user has been assigned a unique user ID and confidential password.<br>• Verify that no generic IDs are used.<br>• Verify that IDs are not shared amongst users. |
| Review of User Access Rights<br>Application system programs, data and on-line reports are not secured from unintentional or unauthorized access and individuals may be granted access to system resources which are not compatible with their job function, ultimately increasing the operational risk | Access rights should be reviewed on a regular basis by qualified staff not responsible for account creation to ensure that the rights are in alignment with roles and responsibilities. | • Determine how frequently user access rights are reviewed.<br>• Determine if there is a formal process in place to review user access rights. Determine if the process can help identify issues related to segregation of duties (access appropriate for the job being performed).<br>• Determine if privileged accounts are reviewed more frequently.<br>• Verify that the procedures surrounding the granting of Access privileges to new hires, personnel changing job responsibilities, and personnel who have been terminated or resigned are followed and if access privileges are assigned on a business-need-only-basis |

| **Risk to Be Managed** | **Types of Controls to Manage / Eliminate Risks** | **Potential Audit Work Steps** |
|---|---|---|
| of the firm. | | (including remote access). |
| Accountability<br>Users may not assume responsibility for adherence to information security policies and procedures with respect to individual access to controlled systems and data. | Users should assume responsibility for adherence to information security policies and procedures with respect to individual access to controlled systems and data. | • Verify that each logon ID has one designated owner and the owner is documented.<br>• Determine if changes to logon ID and group access permissions are captured and contain sufficient level of detail to identify the process or person that caused the change, as well as the time and type of change.<br>• Verify that significant events are logged and include information about (1) time, (2) source and target objects, and (3) event that occurred in sufficient level of detail. Event logs are kept for an appropriate length of time.<br>• Determine if event log information can be read and modified only by authorized individuals.<br>• Verify that new logon IDs are unique and different from logon IDs assigned previously to other persons.<br>• Determine that default privileged logon IDs with publicly known passwords have been disabled or removed.<br>• Verify that all sensitive systems require logon credentials (e.g., passwords, certificates, keys, etc.) for write / modify access, or restricts logon access to a specific source and target system.<br>• Verify that authorized groups and processes exist to facilitate creation of and changes to authentication credentials (e.g., passwords, keys, certificates, etc.).<br>• Verify that authentication credentials (e.g., passwords, keys, certificates, etc.) comply with security standards.<br>• Verify that unsuccessful consecutive logon attempts are identified and result in account lockout or notifications to logon ID owners and |

| **Risk to Be Managed** | **Types of Controls to Manage / Eliminate Risks** | **Potential Audit Work Steps** |
|---|---|---|
| | | Security Operations. |
| IT Data Security<br>Access to strategic, confidential, and secure data stored by IT systems may not be controlled, monitored, and logged. | Access to strategic, confidential, and secure data stored by IT systems should be controlled, monitored, and logged. | • Verify that password controls are available in the IT systems and meet the firm's standards.<br>• Determine if access to data through the following means by employees, contractors, and third parties is properly requested and authorized.<br>  • Databases and query access<br>  • Business and system applications<br>  • File servers and / or operating systems<br>  • Internal and external Web applications<br>• Verify that privileged accounts with access to the data are identified, documented and approved by management and that access is reviewed and approved annually.<br>• Verify that system IDs with access to data used in accessing application, databases, data warehouses and web have owners defined.<br>• Determine if user administration functions are restricted to authorized personnel.<br>• Verify that all access to data and updates are logged and that accountability is maintained.<br>• Verify if personal data is encrypted when transmitted over the Internet, email or unsecured transmission portal.<br>• Determine if procedures exist to periodically check data security procedures.<br>• Determine if procedures exist to identify unauthorized software (such as, keystroke loggers) and unauthorized access attempts. |

| Risk to Be Managed | Types of Controls to Manage / Eliminate Risks | Potential Audit Work Steps |
|---|---|---|
| Telecommuting and Mobile Computing<br>Failure to secure equipment and services used to deliver mobile computing access in a manner similar to on-site facilities could result ion the theft or loss of proprietary information. | Policies should be in place to protect mobile computing equipment, access, and services that make off-site access possible for employees. | • Determine if a formal policy is adopted that takes into account the risks of working with computing facilities such as notebooks, palmtops, etc., off-site and in unprotected environments.<br>• Determine if training was arranged for staff to use mobile computing facilities to raise their awareness of the additional risks resulting from this way of working and controls that need to be implemented to mitigate the risks.<br>• Determine if there is any policy, procedure and / or standard to control telecommuting activities, this should be consistent with organisation's security policy.<br>• Determine if suitable protection of telecommuting equipment is in place against threats such as theft of equipment, unauthorized disclosure of information, etc. |
| **J. Information Systems Acquisition, Development, and Maintenance** | | |
| **J.1 Security Requirements for Systems** | | |
| Failure to identify security requirements as part of new system specifications leads to system software that cannot adequately safeguard information security assets. | Firms should develop processes that ensure security requirements consistent with security policies are included in analysis and specifications for the acquisition, development, and maintenance of software applications. | • Determine if security requirements are incorporated as part of business requirement statement for new systems or for enhancement to existing systems.<br>• Verify that security requirements and controls identified reflect business value of information assets involved and the consequence from failure of security.<br>• Verify that risk assessments are completed prior to commencement of system development. |

| Risk to Be Managed | Types of Controls to Manage / Eliminate Risks | Potential Audit Work Steps |
|---|---|---|
| **J.2 Security in Application Systems** | | |
| Failure of software applications that create, access, update, and store proprietary data to adequately safeguard access to that data. | Firms should develop a software development framework that incorporates security components in the following areas:<br>• Input data validation<br>• Control of internal processing<br>• Message authentication<br>• Output data validation<br>• Read, write, and update database operations | • Determine if data input to application system is validated to ensure that it is correct and appropriate.<br>• Determine if the controls such as: different type of inputs to check for error messages, procedures for responding to validation errors, defining responsibilities of all personnel involved in data input process, etc., are considered.<br>• Determine if areas of risks are identified in the processing cycle and validation checks were included. In some cases the data that has been correctly entered can be corrupted by processing errors or through deliberate acts.<br>• Determine if appropriate controls are identified for applications to mitigate from risks during internal processing. The controls will depend on the nature of the application and the business impact of any corruption of data.<br>• Determine if an assessment of security risk was carried out to determine if Message authentication is required; and to identify most appropriate method of implementation if it is necessary.<br>• Message authentication is a technique used to detect unauthorised changes to, or corruption of, the contents of the transmitted electronic message.<br>• Determine if the data output of application system is validated to ensure that the processing of stored information is correct and appropriate to circumstances. |

| Risk to Be Managed | Types of Controls to Manage / Eliminate Risks | Potential Audit Work Steps |
|---|---|---|
| **J.3 Cryptographic Controls** | | |
| Failure to secure data during transmission between trusted parties results ion the loss or theft of proprietary information. | Firms should maintain, review, and update policies on use of cryptographic controls, encryption, digital signatures, non-repudiation services, and key management in application systems that transmit or copy proprietary information. | • Determine if there is a policy in use for cryptographic controls and the protection of information during transmission or copying.<br>• Determine if a risk assessment was carried out to identify the level of protection the information should be given.<br>• Determine if encryption techniques are used to protect data.<br>• Determine if assessments were conducted to analyze the sensitivity of the data and the level of protection needed.<br>• Determine if digital signatures were used to protect the authenticity and integrity of electronic documents.<br>• Determine if non-repudiation services were used, where it might be necessary to resolve disputes about occurrence or non-occurrence of an event or action.<br>• Determine if there is a management system is in place to support the organisation's use of cryptographic techniques such as secret key technique and Public key technique.<br>• Determine if the key management system is based on agreed set of standards, procedures and secure methods. |
| **J.4 Application Development Environments** | | |
| Inadequate oversight of the development environment and its test data, which is often a copy of production data, could lead to unintended breaches of security information. | In a manner similar to the protection of production assets; firms should have a policy for the control of development software, the protection of system test data, and access control to program source library. | • Determine if there are any controls in place for the implementation of software on operational systems. This is to minimise the risk of corruption of operational systems.<br>• Determine if system test data is protected and controlled. The use of operational database containing personal information should be avoided for test purposes. If such information is used, the data should be depersonalised before use.<br>• Determine if strict controls are in place over access to program source |

| **Risk to Be Managed** | **Types of Controls to Manage / Eliminate Risks** | **Potential Audit Work Steps** |
|---|---|---|
| | | libraries. This is to reduce the potential for corruption of computer programs. |
| **J.5 Security in Development Support Processes** | | |
| Lack of proper safeguards on the processes used to move application development projects into production could result in covert channels and Trojan code being used to steal proprietary information. A covert channel can expose information by some indirect and obscure means. Trojan code is designed to affect a system in a way that is not authorized. | Firms should develop and document formal processes for the following:<br>• Change control procedures<br>• Technical review of operating system changes<br>• Technical review of operating system changes<br>• Outsourced software development | • Determine if there are strict control procedures in place over implementation of changes to the information system. This is to minimise the corruption of information system.<br>• Determine if there is a process or procedure in place to ensure application system is reviewed and tested after change in operating system.<br>• Determine if there are any restrictions in place to limit changes to software packages.<br>• Verify that vendor supplied software packages are used without modification. If changes are deemed essential the original software should be retained and the changes applied only to a clearly identified copy. All changes should be clearly tested and documented, so they can be reapplied if necessary to future software upgrades.<br>• Determine if there are controls in place to ensure that non-approved changes are not introduced into new or upgraded system.<br>• Determine if there are controls in place over outsourcing software. The points to be noted include; Licensing arrangements, escrow arrangements, contractual requirement for quality assurance, testing before installation to detect Trojan code, etc. |

| Risk to Be Managed | Types of Controls to Manage / Eliminate Risks | Potential Audit Work Steps |
|---|---|---|
| **K. Information Security Incident Management** | | |
| **K.1 Reporting Information Security Events** | | |
| Security Architecture<br>A security infrastructure may not be in line with the firm's overall technology and business strategy and therefore my not provide high performance and scalability. | A robust security infrastructure in line with the firm's overall technology and business strategy should provide high performance and scalability. | • Verify that the security architecture is in line with the Organization's overall technology and business strategy and has been approved by the relevant technology and business management.<br>• Determine if a technology architecture team exists that has responsibility for integrating the wide range of security applications, devices and reporting tools used within the organization as well as for assuring high performance and scalability across the enterprise. |
| Incident Reporting Process<br>Lack of regular security breach incident reporting and follow-ups may result in undetected breaches of information security assets. | Incident management should identify and resolve incidents effectively, minimize their business impact and reduce the risk of similar incidents occurring.<br>Security events and the impact that these events have on the firm should be communicated to business. | • Determine if the firm has a formal information security incident reporting process. The incident management process should:<br>  • Ensure incidents are reported to a single point of contact.<br>  • Specify requirements for the recording of incidents.<br>  • Include categorizing incidents by type and prioritizing them according to their impact.<br>  • Define procedures for dealing with incidents (including investigation, planning of remedial action, resolution, communication with users, and documenting actions taken).<br>• Determine if there are incident handling capability for security incidents that include preparation, detection and analysis, containment, eradication, and recovery.<br>• Determine if all firm employees are trained and made aware of their responsibilities for quickly reporting information security incidents.<br>• Verify that the results of each incident analysis are documented, including cause, effect, resolution and suggested improvements.<br>• Determine what security incident management processes are in place to report the results of the above monitoring and / or incidents and to |

| **Risk to Be Managed** | **Types of Controls to Manage / Eliminate Risks** | **Potential Audit Work Steps** |
|---|---|---|
| | | escalate issues to the appropriate level of management and the staff who need to take corrective action. |
| **K.2 Reporting Security Weaknesses** | | |
| <u>Reporting Security Weaknesses</u><br>Failure to identify and report security weakness events and follow-up activities may result in undetected breaches of information security assets. | Processes for monitoring adherence to the Organization's security policies and procedures should be in place to identify security weaknesses, escalate the issue to the appropriate department / personnel to take immediate corrective action and report the item to Management through a formal process. | • Determine what processes / controls are in place to monitor and identify adherence to the Organization's security policies and procedures and if they are effective.<br>• Determine if the firm requires all users to report suspected and identified security weaknesses to appropriate authorities.<br>• Determine if Information Security communicates any security events / activities to the Operational Risk Management group.<br>• Determine if critical security vulnerabilities are identified and evaluated and appropriate patches or workarounds are implemented timely.<br>• Determine if a Security Violation Report exists and review it with respect to the following:<br>  • Determine if it is adequate in reporting violations.<br>  • Determine if it is backed up and maintained for an appropriate length of time.<br>  • Determine if it is routinely reviewed and appropriately escalated to the relevant security, IT and / or business management.<br>• Determine if an audit trail of security administration activities is maintained and reviewed.<br>• Verify that the appropriate level of security, IT and / or business management are reviewing reports of security violations and weaknesses. |

| Risk to Be Managed | Types of Controls to Manage / Eliminate Risks | Potential Audit Work Steps |
|---|---|---|
| **K.3 Responding to Threats and Mitigating Risk** | | |
| Responding to Threats and Mitigating Risk<br>The Firm may not have adequate procedures for responding to specific threats. | Procedures have been developed to respond to specific threats identified as part of the threat matrix. | • Verify that procedures exist for responding to threats.<br>• Determine that the appropriate areas, level of management or law enforcement get involved based on the incident's severity.<br>• Determine if procedures for handling security incidents take into consideration the severity of the issue.<br>• Verify that a process exists for examining how well the organization is doing in regards to security threats. Does this process include harnessing event and incident data that can be used to recommend necessary technologies, policies, and procedure changes to improve the security architecture and minimize security threats? |
| **L. Business Continuity Management** | | |
| Lack of Business Continuity Management and a BCP plan that specifically addresses information security processing requirements may result in:<br>• Increased inability to support information security applications and protect proprietary data in recovery mode<br>• Deterioration of security and increased likelihood of data breaches<br>• Expensive recovery costs for stolen, lost, or damaged data | Firms must include in their business continuity management process specific steps and actions to insure continuity of security over proprietary information assets. This is accomplished through the following activities with respect to information security needs:<br>• Business continuity and impact analysis<br>• Writing and implementing continuity plan<br>• Business continuity planning framework | • Determine if there is a managed process in place for developing and maintaining business continuity throughout the organisation. This might include Organisation wide Business continuity plan, regular testing and updating of the plan, formulating and documenting a business continuity strategy, etc.<br>• Determine if events that could cause interruptions to information security systems and processes such as equipment failure, flood and fire are identified in the business continuity plan and whether a risk assessment was conducted to determine impact of such interruptions specifically on information security.<br>• Determine if a strategy plan was developed based on the risk assessment results to determine an overall approach to business continuity for information security processing needs.<br>• Determine if plans were developed to restore business operations with required information security safeguards within the required time |

| Risk to Be Managed | Types of Controls to Manage / Eliminate Risks | Potential Audit Work Steps |
|---|---|---|
| | - Testing, maintaining and re-assessing business continuity plan | frame following an interruption or failure to business processes.<br>- Verify that the plan is regularly tested and updated.<br>- Determine if there is a single framework for business continuity planning and that the framework is maintained to ensure that all plans are consistent and identify priorities for testing and maintenance.<br>- Determine if the framework identifies conditions for activation and individuals responsible for executing each component of the plan.<br>- Verify that business continuity plans are tested regularly to ensure that they are up to date and effective.<br>- Determine if business continuity plans are maintained and updated through regular reviews to ensure their continuing effectiveness.<br>- Determine if procedures were included within the organizations change management program to ensure that business continuity concerns are appropriately addressed. |
| **M. Compliance** | | |
| Compliance failure or oversight leads to information security breaches and non-compliance with regulations putting the firm at risk. | Compliance policies and those responsible for overseeing them, should address the following concerns with respect to information security:<br>- Identification of applicable legislation and regulations<br>- Intellectual property rights (IPR)<br>- Safeguarding of organizational records<br>- Data protection and privacy | - Determine if all relevant statutory, regulatory and contractual requirements were explicitly defined and documented for each information system.<br>- Determine if specific controls and individual responsibilities to meet these requirements were defined and documented.<br>- Determine if there exist any procedures to ensure compliance with legal restrictions on use of material in respect of which there may be intellectual property rights such as copyright, design rights, trade marks.<br>- Determine if proprietary software products are supplied under a license agreement that limits the use of the products to specified machines. The only exception might be for making own back-up |

| Risk to Be Managed | Types of Controls to Manage / Eliminate Risks | Potential Audit Work Steps |
|---|---|---|
| | of personal information<br>• Prevention of misuse of information processing facility<br>• Regulation of cryptographic controls<br>• Collection of evidence requirements | copies of the software.<br>• Determine if important records of the firm are protected from loss destruction and falsification.<br>• Determine if there is a management structure and control in place to protect data and privacy of personal information.<br>• Determine if use of information processing facilities for any non-business or unauthorised purpose, without management approval is treated as improper use of the facility, logged, and reviewed by security personnel.<br>• Determine if during the system log-on process a warning message is presented on the computer screen indicating that the system being entered is private and that unauthorised access is not permitted.<br>• Determine if the regulation of cryptographic control is consistent with applicable regulations.<br>• Determine if the process involved in storing and collecting information to be used as evidence is in accordance with legal and industry best practices. |
| **N. Prior Audit Issues** | | |
| Prior and / or ongoing issues that impair a firm from operating a compliant and effective information security infrastructure. | Review of prior issues, resolution, and meeting of previously established target dates. | • Obtain a copy of prior information security audit issues that related to this review and perform issue follow-up to ensure that actions are adequately resolved.<br>• Review past reports for outstanding issues or previous problems. Consider:<br>  • Regulatory reports of examination.<br>  • Internal and external audit reports, including SAS 70 reports.<br>  • Organization's overall risk assessment and profile.<br>• Review management's response to issues that were raised since the |

| **Risk to Be Managed** | **Types of Controls to Manage / Eliminate Risks** | **Potential Audit Work Steps** |
|---|---|---|
| | | last examination. Consider:<br>• Adequacy and timing of corrective action.<br>• Resolution of root causes rather than just specific issues.<br>• Existence of any outstanding issues. |
| **O. Conclusions and Action Plan** | | |
| Failure to address the information security audit gaps that impair a firm from maintaining safe, secure, and reliable control of information assets that subsequently impair business operations, profitability, as well as place the firm in non-compliance with regulations. | Discuss corrective action and communicate findings with management and audit sponsors. | • Identify gaps in the information security audit.<br>• Determine actions needed to close gaps.<br>• Assign responsibility to action items.<br>• Determine target date for each action.<br>• Ensure review of action items becomes part of the continuous follow up process, as well as part of the next audit if not resolved and closed by then. |

iad INTERNAL AUDITORS DIVISION
A Division of SIFMA

# III. Glossary

# III. GLOSSARY

The definitions in this section shall apply to the terms as used in the audit guidelines. Where terms are not defined in this section or within another chapter, they shall be defined using their ordinarily accepted meanings within the context in which they are used.

| | |
|---|---|
| Access Controls | A manual or automated process to grants or revokes the right to access a physical location, manual records, or computer data and applications. The Access Control mechanism also controls what operations the user may or may not make. Access Control systems include:<br>• Entry to a physical location.<br>• File permissions, such as create, read, edit or delete on a file server.<br>• Program permissions, such as the right to execute a program on an application server.<br>• Data rights, such as the right to retrieve or update information in a database. |
| Application | A computer program or group of computer programs (software) that provide automated processing for a specific business purpose, i.e. accounting. |
| Application Development Environment | A non-production and usually less secure computer environment that software engineers used to write and test computer programs. |
| Assets | The hardware, software, and other resources used for the processing of information. |
| Best Practices | A group of standards or guidelines developed by qualified industry groups, individuals, or firms with respect to securing proprietary information. |
| Cryptographic Controls | Controls and services such as encryption, digital signatures, or non-repudiation services that are used to secure data during transmission between two parties usually over unsecured non-private networks. |
| Equipment | Computer servers, disk storage devices, network components, interface terminals, and other hardware used to store and process proprietary information. |
| Incident | A specific event or instance representing a breach of information security. |
| Information Systems | Refers to a computer-based system of data records and software applications that process information in an organization. |
| Logs | A computer record of transactions or events, e.g. a record of the date, time, and user ID for each time an employee uses his ID to access a secured area. |
| Media | Hard drives, floppy disks, and other physical devices used for the storage of proprietary information. |
| Mobil Computing | Access to a firm’s computer systems and applications by using a laptop or remote non-company PC from an off site location and via a public network. |

| | |
|---|---|
| Physical Environment | The locations of business operational areas as well as computer hardware and software used to store and process proprietary information. |
| Project Management | The business process of managing computer application development for the creation of a unique product, service or result. A project is a finite endeavor having specific start and completion dates undertaken to create a quantifiable deliverable. |
| Secure Areas | Physical locations whose access is limited to authorized personnel through use of an access control process. |
| Security Governance | The framework, organizational and management structure, and policies and procedures used to manage, implement, and oversee information security. |
| User | A person, employee or qualified external party that has access to and uses a computer application or information system. |
| Telecommuting | The practice of using remote computer equipment and telecommunication technologies to facilitate work at a site away from the traditional office location and environment. |

The Audit Guidelines (the "guidelines") are intended to provide members of the Internal Auditors Division (“IAD”), an affiliate of the Securities Industry and Financial Markets Association (“SIFMA”) with information for the purpose of developing or improving their approach towards auditing certain functions or products typically conducted by a registered broker-dealer. These guidelines do not represent a comprehensive list of all work steps or procedures that can be followed during the course of an audit and do not purport to be the official position or approach of any one group or organization, including IAD or any of its divisions or affiliates. Neither IAD, nor any of its divisions or affiliates, assumes any liability for errors or omissions resulting from the execution of any work steps within these guidelines or any other procedures derived from the reader's interpretation of such guidelines. In using these guidelines, member firms should consider the nature and context of their business and related risks to their organization and tailor the work steps accordingly. Internal auditors should always utilize professional judgment in determining appropriate work steps when executing an audit