Internal Auditors

SIFMA Society

UNIX Data Security

October 2010

Internal Auditors

SIFMA Society

TABLE OF CONTENTS

Internal Auditors

SIFMA Society

I. Introduction and Background

I. INTRODUCTION AND BACKGROUND

A. Overview

Many firms' information assets are stored on UNIX[1] servers and this information is collected, shared, and published in a variety of ways in distributed computing environments supported by UNIX servers. It has become widely recognized that information assets (data) 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 UNIX data assets from unauthorized use and the risks generated by the subsequent misuse of that information, whether intentional or not.

The combination of highly publicized data breaches and stricter regulatory compliance demands is pushing data security to the foreground. There exists in many firms today a fragmented approach to UNIX data security since many security professionals are not familiar with the security aspects in a UNIX environment, while many security professionals are familiar with network and desktop security. This is beginning to change as the importance of securing UNIX becomes more apparent in the face of increasing threats.

The primary objective of a UNIX data security audit is to understand and confirm how a firm's security function operates UNIX tools that may be used to collect, share, and publish data. Additionally, it is important to evaluate the effectiveness and efficiency of the overall management framework for the firm's UNIX data security function and identify the key specific aspects of that function.

This UNIX data security audit guideline, risk assessment and audit program provides detailed guidance to assess and evaluate the UNIX data security management framework in an organization. A UNIX data security management framework or "best practice" would include a comprehensive strategy to protect assets including information, data, and the technology infrastructure used to process that data. Additionally, it would include effective methods for monitoring and enforcing the policies and procedures set forth within the security management framework. UNIX data 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 UNIX data security program helps promote a broad understanding of the security function, and establishes policies, standards and procedures that highlight the Firm's key security risks and the steps being taken to address and mitigate them.

A key component of a UNIX data security program requires an assessment of risk as well as the development and implementation of a UNIX data security risk management program. A UNIX data security risk assessment process is utilized to determine the extent of potential threats and associated risks within the environment being evaluated.

[1] In this document, the term "UNIX" shall be understood to include UNIX-compatible operating systems, such as Linux and Solaris, unless otherwise indicated.

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 UNIX data 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 the judgment of knowledgeable individuals.
- Identifying and ranking the value, sensitivity, and criticality of data assets that could be affected should a threat materialize in order to determine which UNIX data assets are the most important.
- Estimating, for the most critical and sensitive UNIX data 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 UNIX data security assets. A risk management plan should at a minimum address the following activities:

- Prioritizing UNIX data security assets that should be secured.
- Verifying that responsibility for UNIX data security is assigned.
- 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 UNIX data security requirements.
- Determining if security is applied to the handling of physical media, both onsite and off-site, and if data is encrypted as appropriate.
- Verifying that security governance covers at a minimum the following areas:
    - Security Organization inclusive of a UNIX data security strategy and UNIX data security officer
    - Policies, guidelines, standards, and procedures for UNIX data 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

B. Examination Objectives

The three main objectives of an audit of UNIX data security are:

- To determine the adequacy of controls over logical access to the UNIX environment.
- To understand and assess the UNIX control environment, including security administration procedures, registration and maintenance, password maintenance, file and directory control, network security, and system configurations as defined in the Firmwide Information Security Policy and Standards.
- To ensure that the security and audit features of the operating system, as well as manual procedures for security management and administration, are used effectively (e.g., system administrators' access to critical UNIX system and data files are properly controlled and monitored).

C. Examination Scope

The scope of examinations covered by the audit guidelines may be used to determine the quality and effectiveness of the organization's best practices and governance of security related to UNIX operating systems. The topic of UNIX data security is very broad in scope and could conceivably cover just about all security-related aspects of the Firm's IT infrastructure (e.g., UNIX environment risk assessments; administration and monitoring of logical security, database security, physical security, application security and network security; the development and maintenance of a UNIX Data Security Policy and Standards document; and security incident reporting). Many of these topics and their related security controls are typically covered in specific infrastructure and security audits (e.g., Windows, UNIX, Database, Networks, Data Center, and Electronic Communications) as well as in an information security audit guideline previously published by the Internal Audit Society (IAS) of SIFMA. Some aspects of these audit guidelines are included here in order to make the UNIX data security audit guideline complete and a standalone document for the purpose of conducting a thorough audit. However, the areas that are not usually covered in any great detail are the functions that specifically relate to the best practices and governance of UNIX data security policies, procedures, and systems. It is these ancillary functions that will be covered in more detail by these audit guidelines.

D. Risk

UNIX data is subject to threats that cannot be handled by firewalls, intrusion detection, and other defenses alone. Threats are constantly evolving and becoming more sophisticated and specialized. For example, recent attacks take advantage of memory backdoors present in database software. The people posing threats to financial services firms have evolved from lone hackers proving their technical prowess to organized and highly capable groups working in the service of organized crime syndicates. This has changed the nature of intrusion attempts from simple penetration and damage to stealth and data theft for financial gain or reputational damage.

Concurrently with the change in the nature of the external threats, there is increasing attention being given to insider threat and reputational damage caused by individuals within the organization, either maliciously or accidentally. Insiders bent on stealing data have a much greater chance of success than outsiders.

The criminalization of the threat landscape also has an impact on "crimes of opportunity" committed by insiders. It is often easier and quicker to bribe an insider with access privileges than to attempt hacking from the outside. It is therefore evident that perimeter and network security measures are not enough to stop such breaches. Many regulatory compliance requirements focus on privileged insiders as well, with special attention given to those whose actions have gone unmonitored in the past.

A thorough audit of the UNIX data environment requires an understanding of the threats and risks unique to this environment. This section provides a background on the risks to be addressed by an audit of UNIX data.

Audit Risks

A successful audit requires executive support of the audit process. As with any other firm initiative, if the ownership and accountability of the audit are not defined clearly from the beginning and communicated to appropriate staff, the audit may not operate as effectively as it could. Areas of concern include:

- Executive responsibility for the audit process
- Allocation of sufficient resources and budget for audits
- Awareness by personnel of management's role in the audit process

UNIX Data 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 UNIX data security requirements, the firm can be subject to additional risks and threats to its UNIX data security assets.

Damage to, loss of, or unauthorized use of UNIX data security assets could cause both financial and reputational damage to a firm. Identifying and securing critical UNIX data 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 UNIX Data Security Risks are further detailed with expected controls and procedures in the Audit Guidelines matrix.

A. Overall Scope

The start of an effective audit process is to insure that all stakeholders are aware of and agree the scope and purpose of the audit in order to insure that there is awareness and consensus around factors that present the greatest degree of risk to the firm with respect to UNIX data security. Failure to do so effectively could impact critical business operations and operational integrity.

B. Security Policy

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

C. Organization of UNIX Data Security

Without clearly defined responsibilities for creating, implementing, and insuring compliance with UNIX data security policies, UNIX data 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.

D. 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.

- 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 UNIX data security policy. Vulnerabilities have no impact if a relevant threat is not present.

E. Human Resource Security

Employees, contractors, and third parties may not know the importance of the organization's security practices, which could result in security breaches (e.g., theft, misuse). Roles may not be properly defined with segregation of duties to insure that UNIX data security policies are implemented effectively.

F. 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.

G. Network and Internet Security

Lack of controls over the UNIX environment's access to internal networks, external networks, and the Internet may result in unauthorized persons gaining access to a firm's UNIX resources, computer systems, or data for malicious and harmful purposes.

H. UNIX Configuration Management

Properly securing a UNIX environment requires an understanding and setting of all relevant UNIX configuration files and parameters. Failure to do so could permit unauthorized systems controlled by outside persons gaining access to a firm's UNIX resources for malicious and harmful purposes.

I. User Administration and Access Control

Lack of a user access control policy, user access management, and reviews of user rights may result in unauthorized persons gaining access to a firm's computer systems or data for malicious and harmful purposes.

J. Monitoring and Support

The lack of audit logs, active monitoring, and incident escalation may allow unauthorized breaches of the UNIX data security infrastructure to go undetected. Lack of proper change control procedures may result in changes to configuration files and installation of unauthorized applications, thereby compromising UNIX data security.

K. Backup, Recovery, and BCP

Without documented business continuity plans (BCP) and the ability to backup and subsequently recover UNIX hardware, software and data, 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 UNIX data assets could also lead to the loss of proprietary information while the Firm operates in a recovery mode.

L. Prior Audit Issues

An effective audit process includes a firm's commitment to addressing issues that arise out of prior UNIX data 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, IT 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 UNIX data security assets such as e-mail and messaging systems.

M. Conclusions and Action Plan

An effective audit process also includes documenting conclusions drawn from an audit and developing an action plan to address current gaps. Failure to address the UNIX data security audit gaps may impair the Firm's ability to maintain safe, secure, and reliable control of information assets. This may subsequently impact business operations and profitability, and place the firm in non-compliance with regulations.

Internal Auditors

SIFMA Society

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 UNIX data security in order to support critical business operations and maintain operational integrity.	The scope, objectives, and approach are discussed with management prior to commencing the review of UNIX data security.
	
	Management reviews and approves the final report.
		• Interview management and appropriate UNIX data security operations staff to identify:
		  • Any significant changes in business strategy or internal business processes that could affect the operation of UNIX data security
		  • Any material changes in the audit program, scope, or schedule related to UNIX data security activities
		  • Key management changes
		  • Information technology environments and changes to UNIX data security configuration or components
		  • Changes in key service providers (messaging, archival and retrieval, backup/recovery, etc.)
		  • Any other internal or external factors that could affect the UNIX data security process
		• Determine management's consideration of newly identified threats and vulnerabilities to the organization's UNIX data security process. Consider:
		  • Technological and security vulnerabilities
		  • Internally identified threats
		  • Externally identified threats (including known threats published by information sharing organizations)
		• 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 UNIX Data Security Policy		

Security policies and standards are not documented, resulting in lost, stolen, or misuse of strategic information.	Policies and standards are in place regarding security configuration standards governing the UNIX environment, as well as the processes of implementing changes to the UNIX environment.	• Obtain and review all relevant firm-wide policies and standards affecting the UNIX environment.
		• Determine if the relevant policies, procedures, guidelines and standards documents are up-to-date, accurate, complete, signed off by management and published.
		• Verify that they include information about owners, revision information, scope, roles and responsibilities and relevant controls.
		• Obtain and review the policy to determine if the policy includes the following:
		  • The mandate and the charter from senior management supporting the goals and principles of UNIX data security
		  • Highlights the business risks associated with a breakdown in UNIX data security
		  • Defines UNIX data security, responsibilities, and the high-level principles to be observed
		  • Requires that information is protected in terms of its requirements for availability, integrity, and confidentiality
		  • Prohibits unauthorized or personal use of the organization's information and systems
		  • States that disciplinary action will be taken against individuals who violate its provisions
		• Determine if the UNIX policy contains the following:
		  • Access rights to IT resources
		  • Monitoring and reporting on security violations
		  • Password administration procedures and enforcement
		  • Configuration Management

Risk to Be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
		• Change Management • Definition of roles and responsibilities • Procedures for operating system risk assessment • Procedure for cost benefit analysis • Definition of security perimeter • Definition of UNIX security awareness program
B.2 Best Practices		

The UNIX Data 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 UNIX Data Security Policy has been developed based on best practices by verifying the following:
		  • The policy reflects the organization's past experience with security breaches. Common topics might include: addressing restrictions on sharing of ids and passwords among users, modification of access after an employee has been terminated or has changed functions, and checking for appropriate sign-on from atypical workstations.
		  • The existence of security best practices and monitoring tools and programs for all key systems.
		  • The definition of key performance indicators (KPI's) that are used to assess the organization's security policies.
		  • The application of access policies to users and controls to restrict access to information and computer systems.

B.3 Regulatory and Corporate Compliance		
Applicable federal/state/local laws, regulations, and rules and corporate policies are not addressed in the UNIX Data Security Policy, resulting in compliance issues.	Management has identified all legal and regulatory requirements and controls to be applied where appropriate or included into the policy requirements.	• Interview compliance staff to understand key regulatory issues and insure that relevant sections are addressed in the UNIX Data Security Policy. • Obtain/discuss relevant regulatory requirements with management. If required, review the process management uses to ensure continuous

Risk to Be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
	Compliance policies and those responsible for overseeing them have addressed the following concerns with respect to UNIX data security: • Identification of applicable legislation and regulations • Intellectual property rights (IPR) • Safeguarding of organizational records • Data protection and privacy of personal information • Prevention of misuse of information processing facility • Regulation of cryptographic controls • Collection of evidence requirements	compliance with regulations. • Review corporate policy and insure that relevant sections are addressed in the UNIX Data Security Policy. • Determine if all relevant statutory, regulatory and contractual requirements were explicitly defined and documented for each information system. • Determine if specific controls and individual responsibilities to meet these requirements were defined and documented. • Determine if there are procedures to ensure compliance with legal restrictions on use of material for which there may be intellectual property rights such as copyright, design rights, trade marks. • 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 backup copies of the software to be used on backup equipment. • Determine if important records of the Firm are protected from loss, destruction and falsification.
B.4 Review and Approval		
Management is unaware of potential risks/vulnerabilities to the organization and/or has not mitigated key UNIX data security risks.	Management has reviewed and approved the UNIX Data Security Policy. The UNIX Data Security Policy supports the business objectives of the firm.	• Verify that senior management has reviewed and approved the UNIX Data Security Policy. • Determine that the UNIX Data Security Policy supports the organization's objectives. • Verify that a risk assessment was used as the basis for the UNIX Data Security Policy.

Risk to Be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
B.5 Communication of UNIX Policy, Procedures and Guidelines		
Security policies and standards are not communicated to all employees, resulting in ineffective and inconsistent security levels.	Policies and procedures are adequately communicated and available to IT support personnel.	• Verify that the UNIX policies, procedures and guidelines have been communicated and are readily available to all employees, consultants, contractors, and external parties. • 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.
C. Organization of UNIX Data Security		
C.1 Security Governance		
Data integrity and confidentiality strategy for the Firm may be compromised without adequate governance and oversight, thereby increasing the operational risk of the Firm.	Adequate governance framework is established by the Board of Directors and oversight is provided through their sponsorship of the security program. Senior management provides direction and commitment to UNIX data security. Security framework and supporting documentation have been formally communicated to all relevant parties.	• Verify if a Security Strategy (mandate, framework, charter, mission, etc.) within the Firm has been documented. • Determine if the security mandate corresponds with the scale and complexity of the Firm's operations. • Determine the adequacy of the governance framework established by the Board of Directors, the oversight they provide and their sponsorship of the security program within the Firm. • Determine if executive sponsorship exists and supports the UNIX data security program. • Determine if the security framework and supporting documentation have been formally communicated to all relevant parties and stakeholders.
C.2 Organization and Reporting Lines		
<u>Security Organization</u> Ineffective security due to poor	Roles and responsibilities for supporting the UNIX	• Discuss with responsible management the reporting lines in place for groups responsible for UNIX configuration, administration,

Risk to Be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
definition and understanding of security roles and inadequate resources and authority for UNIX data security support staff.	infrastructure are defined.	deployment (i.e., install patches and upgrades) and support. • Determine if there are specific roles and responsibilities assigned to the UNIX group. • Determine if there is a technology owner of the UNIX operating system. • Request an organizational chart for the UNIX operating system support structure. • Determine if roles and responsibilities are defined. • Determine if there is a security committee either locally and/or globally that is used to discuss and decide security requirements.

<u>UNIX Data Security Coordination</u>
Control weaknesses due to unclear assignment of responsibilities and an inadequate security function ultimately increase 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.
	
	Security efforts are coordinated across the firm.
	
	Specialists support various platforms and applications and are responsible for security of the applications and/or operating systems.
		• Determine through interviews with security management if:
		  • A security administration function exists.
		  • Clear documentation of security administration roles and responsibilities exists and has been appropriately approved.
		  • The function is located at an appropriate organization level to ensure proper enforcement of Information Systems security policies and procedures.
		  • The administration function is adequately staffed.
		• Determine what groups or roles are actively involved in UNIX data security within the firm.
		• Verify that a UNIX data security committee has been established,
		comprised of key stakeholders/users/senior management from various departments, whose purpose is to oversee and coordinate security issues throughout the Firm. Examine meeting minutes and/or other information to determine how effectively the committee is executing its responsibilities.
		• Discuss responsibilities of UNIX personnel with appropriate

Risk to Be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
		management. Identify gaps, overlaps or unclear assignments of responsibilities.

Segregation of Duties
Breakdown of controls, major availability problems, fraud, etc., can be caused by single individuals.
	Staff responsibilities are allocated in such a way as to ensure segregation of duties.
	
	Access to administration functions for multiple platforms (e.g., operating system, database, applications) is properly segregated.
		• Review the organizational structure of the UNIX IT Security group.
		• Obtain staff job descriptions, if available.
		• Determine which security administration functions are distributed to various people (including UNIX data security staff) throughout the organization. Establish whether any security functions are incompatible with each other. Examples of potentially incompatible duties are:
		  • Security administration
		  • Security monitoring and incident reporting
		  • Policy setting
		  • Risk management
		• Determine which platforms/ infrastructure the UNIX data security group is responsible for. Review the security permissions for each of the platforms/ infrastructure and determine appropriateness of segregation of functions.
		• Establish whether IT staff are performing functions which are incompatible with each other. Examples of potentially incompatible duties are:
		  • Installation and maintenance of the UNIX applications
		  • Security Administration (set up/change user access, violation and exception reporting, review/follow-up, etc.)
		  • Computer operations, application development, system maintenance, and systems programmers
		  • Security monitoring

Risk to Be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
C.3 Strategy and Project Management		

Progress Reports
Senior IT management is not kept up-to-date with developments in UNIX data security.
Management information regarding UNIX data security project status (progress, cost vs. budget) against defined plans is not produced and disseminated appropriately.
	Project progress reports and other updates are produced regularly and distributed to appropriate recipients.	• Identify UNIX data security projects and ascertain how project progress is tracked and reported.
		  • Are reports prepared on a regular basis?
		  • Who receives the reports? Are the reports adequate?
		• Review whether reports are complete and accurate and produced within an acceptable timeframe.
		• Examine security projects over the past year to determine if they have been delivered on time and on budget.

C.4 Staff Training and Experience		
Weak UNIX data security may be caused by inexperienced staff responsible for the operation, administration or maintenance of the environment.	UNIX support personnel have the training and experience required to perform their roles and responsibilities adequately.	• Request documentation of experience of the UNIX support organization members. • Request documentation of training and certifications of the UNIX support organization. • Correlate training and experience of UNIX support members to job responsibilities and assess if there are potential opportunities for training. • Determine if the UNIX support organization has implemented cross-training to mitigate possible single points of weakness. • Determine how the UNIX support organization stays informed of potential security threats.
C.5 Staff Management		
There is an inadequate level of support for the UNIX environment with no	Plans are in place to ensure the continued availability of adequate resources to support	• Review the UNIX organizational chart and determine if there are current vacancies and if adequate coverage is available.

Risk to Be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
contingency plans in place in the event that key individuals are unavailable.	UNIX. Backup roles and cross-training are in place.	• Request documentation on UNIX staffing levels. • Determine if planning is performed to determine future resource requirements.
C.6 Third Party and Vendor Management		
UNIX data security risks may not be identified before engaging in operations with an external party.	Procedures exist for permitting third-party access to the Firm's resources. These procedures may be in the form of a security risk assessment or impact analysis. They are incorporated in agreements with third-party vendors that provide software and support and are kept up-to-date.	• Determine if there is a process for assessing the risk of allowing third parties to access the Firm's resources. • Describe how external parties are made aware of their UNIX data security responsibilities as this relates to the Firm. • Determine if there is a formal access control policy regarding third-party access. • Determine if the third-party agreements/contracts include the Firm's requirements for UNIX data security.
D. Risk Assessment and Mitigation		
D.1 Risk Assessment Policies and Procedures		

Since risks and threats change over time, it is critical that organizations maintain and update risk mitigation plans. 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 UNIX data from unidentified threats and vulnerabilities.	The Firm's risk assessment programs with respect to UNIX data security are efficiently and effectively implemented.
	
	Key factors are identified that help ensure that the organization benefits from the expertise and experience of their senior managers and staff, that risk assessments are conducted efficiently, and that the assessment results lead to
		• Determine if the Firm has a risk assessment policy that addresses the following:
		  • Has senior management support and involvement
		  • Designates a responsible person or group for conducting the assessment
		  • Refers to a procedure for conducting the assessment
		  • Involves business and technical experts
		  • Produces an action plan to mitigate identified risks
		  • Holds Business Units responsible for mitigating risks
		• Insure that properly defined risk assessment procedures include at a minimum the following:

Risk to Be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
	appropriate remedial actions.	• What activities are to be undertaken, including: security classifications and risk analysis; safeguarding important records; monitoring, reporting and correcting suspected security weaknesses; and reporting them to management • Who is responsible for initiating and conducting risk assessments • Who is to participate • What steps are to be followed • How disagreements are to be resolved • What approvals are needed • How assessments are to be documented • How documentation is to be maintained • To whom reports are to be provided • Determine if there is a process to incorporate the results of a risk assessment into the UNIX Data Security Policy.
D.2 UNIX Data Security Risk Assessment		
Threats and Vulnerabilities Failure to identify the potential unauthorized access, use, disclosure, disruption, or destruction of information and systems that support the operations and assets of the Firm may create operational risk.	The Firm conducts risk assessments of the risk and magnitude of harm that could result from unauthorized access.	• Determine if the UNIX data security function has conducted a threat / risk assessment of security exposures in accordance with the firm's threat / risk assessment program. • Determine whether reliable sources such as NIST, CERT, SANS, and/ or FEMA are used to help identify potential threats. • Determine if threat sources (natural threats, human threats, and environmental threats) are considered for the risk assessment process. • Determine if the risk assessment process includes the control level of effectiveness that ultimately determines the residual risk level. • Determine if a report of the risk assessment results is created for management that includes control recommendations needed to reduce

Risk to Be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
		any remaining significant risks. • Determine if a UNIX data security impact assessment has been performed for the Business. • 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.
D.3 UNIX Vulnerability Assessment		
Lack of periodic vulnerability assessments permits changes to the security environment, resulting in unauthorized access.	Vulnerability assessments are conducted to evaluate security controls over the UNIX environment. Corrective actions for issues are identified and implemented in a timely manner.	• Review security assessments performed over the UNIX environment in the past 12 months. • Verify that issues identified by the assessments are included in the Threat and Vulnerability process.
D.4 Critical UNIX Business Applications		

Application Risks
Lack of an understanding of the criticality of an application that has access to sensitive UNIX data may result in a loss of confidentiality, integrity, or availability of data.
	Critical business applications that have access to UNIX data security and data assets are provided with a more stringent set of UNIX data security controls than other applications.	• Determine if UNIX data security requirements are assessed for new or existing applications based on criteria used for risk assessment.
		• Determine if applications (new and existing) are classified using a security classification scheme based on their security requirements. The scheme should take account of the following:
		  • Business impact of a loss of confidentiality, integrity, or availability
		  • Sensitivity of information stored in or processed by the application
		  • Vulnerability of the application to particular threats
		  • 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) • Size (e.g., applications supporting many users or just a few)
D.5 Risk Mitigation Strategy		
Failure to mitigate risk from potential threats and vulnerabilities may result in loss, destruction, or malicious change to UNIX data security assets.	There is a process in place for prioritizing, implementing, and maintaining the appropriate risk-reducing measures recommended from the risk assessment process.	• Determine that risk mitigation strategies and processes have been developed and put in place that address the threats and vulnerabilities documented within the threat/risk matrix. • Determine if there is an approach for implementing controls based on the risk level.
E. Human Resource Security		
E.1 Security in Job Definition and Resourcing		
Failure to include UNIX data security as each employee's responsibility will hinder awareness programs and result in breaches harmful to the Firm.	UNIX data security is included in job responsibilities, personnel screening and policy setting. Confidentiality agreements are included in the terms and conditions of employment.	• Determine that security roles and responsibilities as described in the organization's UNIX Data 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. • Determine if verification checks on permanent staff were carried out during the job application process. This should include character reference, confirmation of claimed academic and professional qualifications and independent identity checks. • Determine if employees are asked to sign a confidentiality or non-disclosure agreement as a part of their initial terms and conditions of employment and that the agreement covers the security of the information processing facility and organizational assets. • Determine if the terms and conditions of employment cover the employee's responsibility for UNIX data security. Where appropriate, these responsibilities should continue for a defined period after the

Risk to Be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
		end of the employment. • Determine if there is a process for termination responsibilities. Determine whether management has defined a termination and change of employment process for UNIX data security personnel. Does the process include the removal of access rights?
E.2 Security Awareness, Education, and Training		
Employees and users may not be aware of good security practices, leading to shared passwords, unlocked workstations, etc., which increase the risk of unauthorized access. The security policy does not prohibit employees from using the Firm's systems for purposes that are not work or business related.	A Security Awareness program is in place to remind individuals of the security policies of the Firm, and their responsibility and accountability for security issues. Appropriate training and notification is provided to employees to remind them of the importance of maintaining UNIX data security. Awareness of UNIX data security is 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 UNIX data security policies. • Verify that the UNIX data security policies and procedures have been communicated to the persons concerned with correspondence and/or training. • Determine if appropriate security training is provided to employees of the Firm, including security specialists. This includes routine periodic awareness sessions to inform and remind individuals of their security responsibilities. Also, briefings should be conducted regarding responsibilities and accountability attached to security screening levels. • Review the security awareness and training program to determine if it provides clear and comprehensive guidance to employees on acceptable and unacceptable use of confidential, sensitive, and proprietary information. • Review the compliance manual to determine if guidance on protecting confidential documents is included and determine if employees are aware of the manual.
F. Physical and Environmental Security		
F.1 Secure Areas		
Unauthorized access to the	Physical security perimeter and	• Through discussions with area management and review of available

Risk to Be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
data center or development workspaces where proprietary information is processed may cause a breach in UNIX data security and reputational harm to the Firm.	physical entry controls are 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.	documentation, verify that procedures for securing the UNIX environment exist. • Verify that a physical border security facility has been implemented to protect information processing service areas. Some examples of such a security facility are: card-controlled entry gate, walls, manned reception area, etc. • Determine if entry controls are in place to allow only authorized personnel into various areas within the organization where proprietary information is processed. • Determine if the rooms containing the information processing service areas are locked or have lockable cabinets or safes. • Determine if information processing service areas are protected from natural and man-made disasters. • Determine if there is any potential threat from neighbouring premises. • Determine if there exists any security control for third parties or for personnel working in secure areas and that information is only distributed on a need-to-know basis. • Determine if the delivery area and information processing area are isolated from each other to avoid any unauthorized access. • Determine if a risk assessment was conducted to determine the security in such areas.
F.2 Equipment Security		
Unauthorized access to the equipment used to store and process proprietary information may cause a breach in UNIX data security and reputational harm to the	The Firm has established plans for equipment site protection including power supplies, cabling security, and equipment maintenance. These plans also include securing of equipment	• Determine if equipment is located in appropriate places to minimize unnecessary access into work areas. • Determine if the items requiring special protection are isolated to reduce the general level of protection required. • Determine if controls have been adopted to minimize risk from

Risk to Be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
Firm.	off-premises and secure disposal or re-use of discarded equipment.	potential threats such as theft, fire, explosives, smoke, water, dust, vibration, chemical effects, electrical supply interfaces, electromagnetic radiation, and flood. • Determine if there is a policy regarding eating, drinking and smoking in proximity to information processing equipment. • Determine if environmental conditions which would adversely affect the information processing facilities are monitored. • Determine if the equipment is protected from power failures by using facilities such as multiple feeds, uninterruptible power supply (UPS), backup generators, etc. • Determine if the power and telecommunications cables carrying data or supporting information services are protected from interception or damage. • 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. • Determine if logs are maintained with all suspected or actual faults and all preventive and corrective measures. • Determine if appropriate controls are implemented when sending equipment off premises. • Determine if any equipment usage outside an organization's premises for information processing is authorized by management. • Determine if the security provided for equipment while outside the premises are on par with or more than the security provided inside the premises. • Determine if storage devices containing sensitive information are physically destroyed or securely over-written prior to termination of usage.

Risk to Be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
F.3 General Controls		
Failure by employees to secure workstations and other sources of proprietary information assets may result in lost, stolen, or damaged data.	The Firm maintains and enforces a clear desk and clear screen policy. Removal of Firm property by employees is restricted. Approved property removal is monitored by security personnel.	• Determine if an automatic computer screen locking facility is enabled. This would lock the screen when the computer is left unattended for a period of time. • Determine if employees are advised to leave any confidential material in the form of paper documents, media, etc., in a locked manner while unattended. • Determine if equipment, information or software can be taken offsite without appropriate authorization. • Determine if spot checks or regular audits are conducted to detect unauthorized removal of property. • Determine if individuals are aware of these types of spot checks or regular audits.
G. Network and Internet Security		
G.1 Modems and Dialup Security		
Improper configuration of modems could allow unauthorized access to UNIX systems.	Modems are secured and configured to prevent unauthorized access and use.	• Determine if modems are located in a physically secure area. • Verify that remote configuration, testing, and the escape sequence are disabled. • Determine if modem phone numbers are publicized. • Verify that call-forwarding is disabled on incoming phone lines. • Determine if third-party billing is disabled so that people will not be able to bill their calls to the modem line. • Determine that if the connection is lost the computer will kill the associated process and log out the user. • Verify that caller-ID is enabled on incoming lines to the modem.

Risk to Be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps

		• Determine if call-back security should be initiated.
		  o Determine that modems are segregated between inbound and outbound call handling
		• Verify that the SLIP protocol has been disabled.
		• Review the /dev directory for rough modems.
		• Determine ownership of devices:
		  o %ls –lgd /dev/modem subdirectory
		  o Permissions for inbound modems set to 600 and owned by root or uucp
		• Search for unauthorized modems using the Firm's networks via a telephone scanner.
		• Verify that users do not attain special privileges when running cu or tip-use cu or tip to connect to remote machine, shell escape
		  o (! command) and determine your identity (id command). Identity should be that of the user and not root or uucp
		• Verify that tip and cu programs exit if user is logged out or the connection is dropped.
		• Verify that the modem hangs up when tip or cu exits.

G.2 NFS-Network File System		
Improper configuration of UNIX network file systems could allow unauthorized access to UNIX systems.	Network file systems are secured and configured to prevent unauthorized access and use.	• Determine if firewalls and routers block NFS packets. • Determine that the NFS version is the latest variable in TCP mode. • Determine if netgoups is used to restrict the export of filesystems to a small set of local machines. • Determine if there are facilities to mount file systems that specify the nosuid option.

Risk to Be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps

		• Determine that no clients mount from NFS servers from outside the organization.
		• Determine if it is possible to disable the honouring of SUID files and devices on mounted partitions.
		• Verify that Export filesystems is read only when possible.
		• Verify that root ownership of exported files and directories is used.
		• Determine if group write permissions are removed from exported files and directories.
		• Verify that the following conditions are met:
		  o Do not export server executables
		  o Do not export home directories
		  o Do not allow users to log into the NFS server
		  o Do not have files available if not required
		  o Export read only if possible ro=clients in the export file or dfstab file
		  o Protection modes properly set: 755 for programs, 644 for data files.
		• Verify that other data and information are not stored on NFS servers unless the information will be made accessible to clients.
		• Verify that files and directories owned by root are non group writeable.
		• Verify that filesystems that contain world-writable directories cannot be exported. e.g.
		  o /tmp, /usr/tmp. /usr/spool/uucppublic
		• Determine if the kernel variable nfs_portmon is set to one.
		  o This will prohibit NFS requests unless they come from

Risk to Be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
		privileged ports. o Linux-set secure option for an exported directory in /etc/exports is the same as nfs_portmon • Determine that client is not exporting files that should be secured. o Showmount –e =>lists the hosts export directories that can be mounted. o Example %/usr/etc/showmount –e acme.org • Determine if Secure NFS has been enabled on server and client o Server-secure option on in exports or dfstab file o Client-/etc/fstab or /etc/vfstab • Verify that the RPC portmapper does not accept proxy requests. • Verify that remote users are not allowed to issue mknod commands on partitions they export to a Firm's server. • Verify that mount partitions NOSUID is possible • Verify that mount partitions NODEV if available • Verify that root ownership is set on files and directories exported remotely. • Assess which machines should receive world or group writable directories.
G.3 Secure TCP and UDP Services		
Improper configuration of TCP and UDP Services could allow unauthorized access to UNIX systems.	TCP and UDP services are secured and configured to prevent unauthorized access and use.	• Review the /etc/inetd.conf file to determine what services are being offered to the Internet. • Determine if there are change control procedures and processes applied to the /etc/inetd.conf file. • Review controlled access to servers through host-based firewalls:

Risk to Be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
		○ Determine if host-based firewalls have been implemented. ○ Run ipfw to list all the current rules. • Review use of TCP Wrappers with Server Administrator. ○ Obtain: /etc/hosts.allow /etc/hosts.deny /etc/syslog.conf ○ Search for tcpd in /etc/inetd.conf ○ Run tcpdchk and tcpdmatch • Verify that chargen and echo are disabled on machines which are connected to the Internet. • Verify that the systat service is disabled. It provides status information about a computer to other computers. ○ Comment it out in the /etc/inetd.conf file. • FTP ○ Determine that the ftpd program is up to date. ○ Determine that /etc/ftpusers contains the accounts root, uucp, bin, ingress, nobody, daemon and any other account that is not associated with a person. (These are accounts that are not allowed to use ftp to transfer files.) ○ Determine that the ftp service is set up as passive rather than active (passive is preferred). ○ Determine if the ftp account usage is monitored. • Determine that there is only one sshd_config file and one ssh_config file.
Use of telnet may lead to session hijacking or packet	Telnet is not used for remote login to any service that	• Determine if telnet service has been disabled or if there are policy

Risk to Be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
sniffing.	requires authentication or that passes confidential information.	guidelines for its use.
An attacker is able to learn about the system through default messages.	Default SMTP banners have been modified/sanitized to mask sendmail information.	• Perform telnet localhost SMTP and determine if the sendmail version is displayed. • Perform telnet localhost SMTP and then help command. Determine if the sendmail version is displayed.
An attacker is able to gain privileged access due to non-user account aliases.	The mail alias file has been reviewed and aliases not required have been deleted or commented out.	• /etc/mail/aliases • An alias is associated with all non-user accounts. • Access to the alias file has been reviewed and approved. • The decode alias line has been commented out.
	Sendmail options have been hardened to prevent hijacking of the service.	• Request contents of sendmail.mc file: o Define (‘confSMTP_LOGIN_MSG’,’$j smtp service; $b’)dnl ▪ Modifies SMTP banner to show only host name ($j) ▪ Modifies SMTP banner to show only current time ($b) o Define(‘confPRIVACY_FLAGS’, options)dnl ▪ Options: • novrfy-disables VRFY command • noexpn-disables EXPN command • neeedmailhelo-requires HELO before a MAIL command • needverfyehelo-requires a HELO before a VRFY command • needexpnhelp-requires a HELO before a EXPN

Risk to Be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
		command • authwarnings-enables several authentication warnings • nonverb-disables VERB command • goaway-all of the above • Restrictmailq-restricts use of the mailq command. • Determine that sendmail will not deliver mail directly to a file. • Ensure that sendmail does not have a wizard password in the config file. • Determine that users with access to the sendmail.cf file have been reviewed and are appropriate. • Delivery of mail to programs is disabled if not required.
SMTP commands with security concerns have not been disabled, allowing access by an attacker.	SMTP commands that provide information about the organization have been disabled or modified.	• Determine if the following commands have been disabled: o EXPN o VRFY o WIZ o DEBUG o HELP
Email server is used as a spamming device relay.	The relaying of third-party mail (spam) has been restricted.	• Users are authenticated: o IP address-the system is configured with a set of IP addresses that are allowed unrestricted relaying. o User name and password-authentication mechanisms that are part of Extended SMTP are used here. o External Mechanism- POP before SMTP-user is required to be able to download message using POP before allowed

Risk to Be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
		unrestricted SMTP access. • Messages that are not authenticated are only accepted for a preconfigured set of domains.
System problems go unaddressed because the email to system accounts is not monitored.	The /var/spool/mail directory is monitored for email to system accounts. Aliases are created for system accounts.	• Review the alias file and determine that aliases have been created for system accounts.
The name server is compromised and the system is unable to resolve queries. This results in slowing or stopping productivity.	The name server is hardened against attack.	• DNS zone transfers are limited. • The name server is configured to disallow recursive queries by outsiders. o Review allowed recursion o Review access to the name server • The name server is running the latest version with all patches applied. • The name server is running as a non-root user and in a chroot jail environment. • Run name server daemon in the non-root user in a jail environment.
A rogue DHCP server is providing erroneous information to clients, resulting in clients being disabled or compromised.	Rogue DHCP servers are scanned for on the network on a regular basis.	• Request evidence that rogue DHCP servers are scanned for on the network.
The TFTP command is not disabled or restricted, allowing a user to retrieve files which may compromise system	TFTP is run in a restricted environment and requested from specific IP addresses.	• Determine if TFTP is allowed to run on the system. • Determine if the TFTP environment is restricted. • Determine if the TFTP environment is configured to respond only to

Risk to Be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
security, e.g., the password file.		particular IP addresses. o TCP wrappers and /etc/hosts.allow file
The finger command is not disabled, thereby revealing information that can be used in a social engineering attack.	The finger command is disabled or secured.	• Determine if finger has been disabled. o Comment out finger in the /etc/inetd.conf file o Replace finger with a static message directing the user to a standard firm directory
Unencrypted authentication passwords are intercepted with a password sniffer and reused by the attacker, thereby allowing access to the Firm's information.	APOP or Kerberos authentication is employed when using POP or IMAP.	• Request evidence that APOP or Kerberos authentication is employed if using POP or IMAP.
The portmapper is flooded with fake requests, slowing or prohibiting responses to valid requests which impacts overall productivity.	Access to RPC portmapper is disabled or restricted.	• Request evidence that access to RPC portmapper has been disabled or restricted.
Confidential firm information is exposed due to weak access controls around the NNTP service.	NNTP access is restricted.	• Request a copy of the access control list for the NNTP service.
Due to a lack of synchronization, mission-critical applications fail to function.	Servers are synchronized with a time standard.	• Request evidence that servers are synchronized with a time standard. o Verify the NTP service is running • Verify that the most recent version of NTP is running. • Verify in the NTP configuration file that the hosts from which the

Risk to Be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
		NTP service may receive updates are specified.
Inappropriate access to SNMP allowed services to be shut down or disabled.	SNMP has been disabled or restrictions on usage are in place.	• Request evidence that SNMP has been disabled. • Verify that the default community string has been changed. • Determine if write access has been disabled or is not required. • Determine that devices have access control lists for SNMP. • Verify that all SNMP traffic from the outside is blocked. • Verify that SNMP is not running on any security infrastructure systems, e.g., firewalls, IDS.
An attacker is able to probe for valid accounts on the system because system commands with inherent security weaknesses have not been disabled.	Systems commands with inherent security weaknesses have been disabled.	• Request evidence from the /etc/inetd.conf that rexec has been disabled. • Request evidence that rlogin and rsh have been disabled.
An attacker is able to take advantage of the trusted host and user environment to obtain control of systems and files.	Trusted hosts and users are disabled or restricted.	• Remove or comment out rshd and rlogind in the inetd.conf file if not required. • Perform periodic scans for the .rhosts files. • All .rhosts files are mode 600. • Remove user names from the ./etc/r.equiv file. • Remove (+) from the ./etc/hosts.equiv file. • Remove .rhosts files if not required. • Non-essential trusted hosts are removed. • Restrict printing access to printing software via /etc/hosts.lpd.

Risk to Be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
Routing packets are accepted by an outside source, which can result in bringing the network down or can be used to eavesdrop on communications.	Incoming RIP packets are blocked and static routes are used where possible and practical.	• Request evidence that incoming RIP packets are blocked. o If using a single gateway, RIP should be disabled.
Weak terminal emulator security provides the opportunity for an attacker to eavesdrop on communications.	The terminal emulator has enhanced authentication enabled.	• Evaluate the authentication enabled for the terminal emulator and determine if it is adequate. o Kerberos o Secure RPC o Magic cookies • Determine if X11 is running through SSH. o The configuration file sshd_config will include the line X11Forwarding yes
G.4 RPC-Remote Procedure Calls		
Improper configuration of remote procedure calls could allow unauthorized access to UNIX systems.	Remote procedure calls are secured and configured to prevent unauthorized access and use.	• Determine that AUTH_NONE is not in use. • Verify that RPC service rexd is disabled if possible. o rexd checks for the presence of the RPC service. • Verify that a short window is used for Secure RPC authentication. • Determine that portmapper does not perform proxy forwarding. • Determine if rexd has been disabled if not required. o rexd is the RPC server for remote command execution.
G.5 Restricted Services		
Improper usage of restricted services could allow	Unneeded and unnecessary services are restricted or	• The following services are removed or commented out if not required

Risk to Be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
unauthorized access to UNIX systems.	disabled.	for operations: /etc/inetd.conf o admind o echo o chargen o time o daytime o finger o httpd o ntalk o rlogin o rexd o rexecd o netstat o rstat o ruser o rwhod o systat o talk o tcpmux o tffp o uucp o walld

Risk to Be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
H. UNIX Configuration Management		
H.1 UNIX Configuration Controls		

Unauthorized privileged access to the production UNIX environment causes loss or corruption of UNIX data.	Security parameters are configured to protect the UNIX servers in accordance with industry best practices and baseline requirements.	• Through discussions with area management and review of available documentation, verify the procedures for securing the UNIX environment including:
		  • UNIX security baseline compliance (i.e., Enterprise Systems Management [ESM] process)
		  • Procedures for verifying security parameters for compliance with UNIX baseline standards (e.g., inetd.conf, file permissions, ssh, nfs)
		  • Procedures for securing virtual server management (i.e., Hardware Management Console [HMC]) and related server frames
		  • Documentation of the security procedures for granting and tracking exceptions to baseline configurations
		• Review documentation to determine if UNIX hardening settings are included in security baseline policy (i.e., ESM Policy).
		• Review ESM report samples to ensure that ESM generates reports daily. Obtain the follow-up records to ensure that the exceptions from ESM reports are timely addressed.
		• Verify that ESM reports all the exceptions beyond SSH with DSA public key authentication. Obtain the UNIX settings in the production environment and identify any discrepancies with best practices. By comparing with the exceptions recorded in ESM reports, identify the gaps between the real exceptions and ESM-reported exceptions.
		• Identify UNIX server configurations that are not verified by baseline compliance scripts (e.g., requirements to change passwords, presence of exportable partitions and regular review of access rights based on

Risk to Be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps

		"least necessary privilege" standard).
		• Review sample servers for the following:
		  • Assess adequacy of access controls by obtaining /etc/group file, /etc/passwd file, sodoer file and sulog files and insure compliance with UNIX security procedures.
		  • Identify files granted access permissions to accounts / groups other than "root". Include a review of the directory permissions on all critical directories (e.g., /bin, /dev, /etc, /lib, /root, /shlib). Assess whether access is based on business need and follow up on discrepancies.
		  • Compare the netstat -na and netstat -r outputs with inetd.conf configurations. Identify connections and associated local IP addresses on the netstat output and reconcile to the services defined in the inetd.conf against baseline standards. Assess services and associated IP addresses. Identify and document discrepancies.
		  • Obtain listings of the /etc/hosts.equiv file and determine the hosts for which "r" commands have been allowed, if any, and which usernames are specified as being allowed on remote machines to log on to the local machine without a password. Assess appropriateness.

H.2 Managing Virtual Servers		
Virtualization of servers subverts controls implemented for traditional servers.	Access to virtual server management platforms is restricted on a business need basis.	• Review the process and procedures for the hardware management console (HMC) management system. Review the controls for user account management and verify that procedures are in compliance with corporate policies. • Verify that virtual servers are implemented as per secure design guidelines (e.g., grouping servers by risk and/or security

Risk to Be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
		requirements). • Review the virtual servers in each "frame" and determine if configuration is based on risk requirements and/or best practices security guidelines.
H.3 UNIX Build Management		
Server configuration is inadequately documented and documentation is not updated on a timely basis when changes are made.	UNIX server configuration performed by the UNIX support group is documented and the documentation is regularly updated for changes.	• Review documentation regarding the build configuration of servers. • Obtain any other server configuration documentation not covered by the standard server build. • Assess whether such documentation is adequate as a record of configuration changes and whether these are assessed and reviewed.

Uncontrolled server configuration compromises the integrity of processing.	A standard server build, incorporating standard versions, releases and service packs, is implemented. Supported OS versions are used.	• Review documentation relating to the standard server builds for each version of UNIX in production in order to:
		  • Confirm that UNIX default services are removed or disabled.
		  • Establish what software versions, releases and service packs have been implemented. Confirm that the OS versions are supported by the vendor.
		  • Establish whether deviations from the standard build are approved.

Production servers with non-compliant builds could potentially become unsecured.	A procedure is in place to ensure that the production build is in compliance with the Information Security Policy.	• Review with the UNIX admin/engineer the procedure to ensure that the production build is in compliance with the Firm's IS policy.
There is no procedure in place to cover changes to UNIX server configuration, leading to a risk that changes are not	UNIX Admin group is responsible for adapting and configuring the UNIX standard	• Review the process for distributing newly developed builds to production UNIX servers. • Review the procedure followed to implement configuration changes

Risk to Be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
tracked or authorized, which may cause disruption to the business.	build.	with the Server Administrator. Ensure that it incorporates authorization, testing and user notification steps. • Identify recent major changes and the timing of those changes. Review the type of notice given to users.
Changes to the configuration are not reflected in the disaster recovery (DR) servers and the DR Plan (DRP).	As part of configuration control procedures, there is a requirement to update the relevant DR servers and DRP.	• Review with IT personnel that all configuration changes are reflected in DR servers and any changes to procedures are also reflected in the DRP.
H.4 Networking Configuration		
Use of unsecured services may compromise the Firm's data.	The use of "r" commands (rlogin, rsh, rexec) is not allowed in the production environment. (Note that "r" commands transmit data across the network as clear text.)	• Determine whether "r" commands are allowed in the production environment. • Determine whether "r" commands are in /etc/inetd.conf.
There is an inadequate setting for the UNIX time service, and the server clock may not have the accurate time.	The local server's clock is synchronized to a central time server.	• Review UNIX time service with the Server Administrator. • Verify configuration options for /etc/xinetd.d/time. Example; service time { type = INTERNAL id = time-stream socket_type = stream protocol = tcp user = root wait = no

Risk to Be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
		disable = yes } • Verify configuration options for /etc/ntp.conf
Inadequate settings for telnet service may result in unauthorized access to the production environment and/or production disruption.	The UNIX build document includes a procedure for setting up the telnet service that is in compliance with the Firm's information security standards.	• Verify that the configuration options for /etc/xinetd.d/telnet are in compliance with security standards.
The hosts.equiv file allows hosts and users to use the "r" commands (e.g., rlogin, rsh or rcp) without supplying a password.	The UNIX build document includes a procedure for setting up hosts.equiv that is in compliance with the Firm's information security standards.	• Review the procedure for setting up /etc/hosts.equiv. • Confirm that the host.equiv contents are authorized. • Solaris script section 3.020 and A6.3b
$home/.rhosts do not provide adequate security.	The UNIX build document includes a procedure for setting up .rhosts that is in compliance with the Firm's information security standards.	• Review the procedure for setting up .rhosts. • Determine that the .rhosts contents are authorized.
Unsecured anonymous ftp and tftp may result in unauthorized access.	Anonymous ftp is securely configured. Use of tftp is restricted.	• Review procedure for setting up anonymous ftp. • Determine whether anonymous ftp is allowed. • Confirm that ftp services are disabled.
UNIX server may allow authentication via an un-authorized domain.	Only authorized authentication domains are allowed.	• Review the NIS configuration procedure with the UNIX group. • Select a sample of UNIX servers and determine whether the NIS settings are authorized. • Obtain nsswitch.conf, and assess if its settings are for authorized

Risk to Be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
		domains only.
Failure to adequately restrict user access to the command line increases the risk of a system outage occurring as a result of a user accessing and using critical system functions inappropriately. In addition, an unauthorized individual may gain inappropriate access via command line functionality.	User accounts are not provided with command line (shell) access to the UNIX operating system unless this is necessary for their job functions.	• Review with the UNIX Server Administrator if command line access restrictions are in place. If so, determine what shells are restricted and how. They can be restricted on a shell basis or by using scripts that present menu-only access to users.
Failure to lock unattended consoles increases the risk of an information security compromise by an unauthorized individual with physical access to the server.	The server console is locked when unattended.	• Review if the server console is locked when unattended.
H.5 File and Directory Controls		
System files and directories can be changed by unauthorized users.	System files are properly protected using appropriate permissions.	• Verify whether permissions are appropriate for critical system directories using: • $ls -l (directorynames like /etc, /bin, /sbin, /usr/bin, /usr/sbin, /usr/ucb, /usr/lib

User home directories may be accessed by persons who are not the owners of the directory, leading to a risk of unauthorized access to	User home directories are secured using appropriate permissions.	• Verify that the UNIX system directory is not granted with xx7.
		  • $find /{system directories} -type f \(-perm -2 \) -ls
		• Check permissions of users' home directories as follows:
		  • awk –F: '$4>20 && length ($6) >0 {print "ls –ld " $6}

Risk to Be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
sensitive user data.		</etc/passwd \ | sort –u |sh | more • Assess whether permissions are appropriate.
The umask setting is inadequately set such that files and directories created by users (in particular, those with sensitive accounts such as root) are not properly secured when they are created.	For administrative and privileged users, umask is set at 077 (no group or world access). For normal users, this is set at 027 (group read, no world access). Root's umask does not restrict group or world access to files and directories created by root.	• Check umask settings of users by checking contents of /.profile or /.cshrc. Ensure that privileged users have a value of 077, and other users have a value of 027. • Check umask setting in /etc/default/login. Should be set with 022.
A user running a program or script which has the suid set will assume an effective uid the same as the owner of the program while they are running it. Similarly they assume the group ID if the sgid bit is set. This poses a security threat if the script or program can be interrupted, leaving the user in a shell with the inherited uid or gid.	Suid or sgid files and scripts are not used, or if required, are recorded and monitored regularly.	• Review all suid and sgid files/scripts and their permissions with the following: • find / -type f \(-perm -4000 -o -perm -2000 \) –ls • Review with UNIX Server Administrator the procedure for granting SUID and GUID.
The presence of files and directories with unassigned owners may result in unauthorized access to	A procedure is in place to ensure proper ownership of UNIX file/directory objects.	• Verify that each directory and file has an owner and is permissioned correctly so that only owners and administrators can alter contents.

Risk to Be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
confidential data and systems.		

Inadequate configuration of samba may result in unauthorized access to confidential data and/or the production system.	A samba implementation standard has been documented and approved by the Information Security Officer.	• Review samba configuration file and assess the option settings.
		  • /etc/sysconfig/samba
		  • /etc/samba/smb.conf
		  • encrypt passwords = yes
		  • smb password file = [location of samba passwd file]
		• Determine that the security over the password file is adequate.

I. User Administration and Access Control		
I.1 Group Access Control		
Group access and membership is not reviewed, resulting in the compromise of restricted data or resources.	Groups and group members are reviewed for appropriateness.	• Review the /etc/group file for appropriateness. • Verify that those in the wheel group are authorized to have root access. • Verify that those with GID=0 are appropriate.
I.2 Superuser Restrictions		

Accountability is compromised because the user's identity cannot be verified.	Only authorized users can assume the identity of another user.	• Determine that those who have the su command are authorized.
		• Determine that failed su attempts are logged:
		  • var/log/messages
		  • var/adm/sulog

	Only authorized users have the ability to execute commands as superuser (sudo).	• Determine that those who have the sudo command are authorized. • /etc or /usr/local/etc • Review the /etc/sudoers file to determine that the commands these users are permitted to run are appropriate.

Risk to Be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
		• Access is restricted to /bin/su.
	The superuser account is restricted where applicable and accountability is enforced.	• Determine if the superusers must first log in as themselves before su to superuser. • Determine if login as root is restricted to secure terminals.
	Only those authorized have the ability to change groups.	• Determine that those with the newgrp command are authorized.
I.3 Access Controls		
Access Control Policy 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 has developed and published an access control policy that also includes and addresses UNIX Data Security access controls. A series of access-related controls has been developed and implemented by management, including policies, guidelines, and processes to safeguard access to UNIX information and data. The user access policy ensures that all logical security access requests are formally documented and approved utilizing a security access request form and automated system. The security access request forms are filed and	• Verify that logical access to the Firm's UNIX resources is restricted according to clearly defined access control policies. • Verify that documented procedures for requesting access to the various UNIX resources within the Firm (servers, applications, and files, etc.) exist. • Verify that authorized processes are used to add, modify and remove access, including standing and emergency/temporary access, and that exceptions are identified and investigated. • 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. • Determine if the security access request forms are filed and maintained for future reference. • Verify that access permissions are removed or re-evaluated when material changes in job responsibilities occur. • Verify that access permissions are periodically reviewed by management, and the process facilitates effective identification and remediation of issues.

Risk to Be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
	maintained for future reference.	• Determine if only authorized system administrators have standing access to administrative functions. • Determine if access permissions are appropriate and granted on a need-to-have basis.
User ID Management The lack of controls in place for the UNIX ID creation procedure may result in unauthorized access to the UNIX environment.	A procedure has been documented for managing UNIX logon ID's (UID) and addresses the following: • There is a formal procedure for creating new UNIX logon ID's. • UID's are not duplicated or re-used. • Invalid UNIX accounts are disabled. • A formal review of the terminated users list is done periodically. • A formal review of the transferred users list is done periodically. • Contractor and Temporary Accounts are configured to expire after a specified period of time.	• Determine if the Firm has written procedures for the creation and deletion of UNIX user accounts. • Understand how the level of access for each user is determined. • Determine if HR is involved in the creation and deletion of user accounts. • Review with the UNIX Server Administrator and IT Management the procedures for creating new UNIX logon ID's. • Select a sample of new UNIX ID request forms (Remedy) and determine whether there is appropriate approval documented. • Verify if UID's are unique for sample /etc/passwd files. • Determine if all authorized systems users are assigned individual user ID's and confidential sign-on passwords to ensure accountability for network and application activities. • Verify that each user has been assigned a unique user ID and confidential password. • Verify that no generic ID's are used. • Verify that ID's are not shared among users. • Verify that service accounts (non-user) have an owner. • Review with the UNIX Server Administrator and IT Management the procedures to terminate a UNIX logon ID. • Verify a sample of terminated users from HR termination reports and determine that these UNIX logon ID's have been terminated in a

Risk to Be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps

		timely manner.
		• Review with the UNIX Server Administrator and IT Management how they ensure that UID's of terminated users are not reassigned to new users. Assess if the procedure is adequate.
		• Review with the UNIX Server Administrator and IT Management the procedures to transfer employees.
		• Determine whether UNIX access rights for transferred employees are properly re-assigned.
		• Verify that contracts or service agreements with third parties include clauses on UNIX data security and protection of data, disclosure of data, and confidentiality of data.
		• Obtain a list of contractor and temporary accounts and verify that their expiration dates are set in accordance with the Firm's policy.
		• Determine that dormant accounts are automatically disabled after a period of time.
		• Determine if account logins are restricted by time of day.
		• Determine that there are no open or guest accounts.
		  • Determine if restricted shells are applied to open or guest accounts.
		  • Determine if a restricted file system is created for open or guest accounts chroot() or jail().

<u>Review of User Access Rights</u> Application system programs, data and on-line reports are not secured from unintentional or unauthorized access. Individuals may still have	Access rights are 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. • 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). • Determine if privileged accounts are reviewed more frequently.

Risk to Be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
access to system resources which are no longer compatible with their job function. These situations ultimately increase the operational risk of the firm.	A process to re-certify the UNIX logon ID and its access rights is performed semi-annually.	• 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 (including remote access). • Review with the UNIX Server Administrator and IT Management the procedures to periodically certify UNIX ID's. • Obtain and inspect a sample of recertification reports to confirm that a process is in place for certifying active UNIX ID's and their privilege permissions.
Accountability	Users are required to assume responsibility for adherence to UNIX data security policies and procedures with respect to individual access to controlled systems and data.	• Verify that each UID has one designated owner and the owner is documented. • Determine if changes to UID 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. • 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. Verify that event logs are kept for an appropriate length of time. • Determine if event log information can be read and modified only by authorized individuals. • Verify that new UID's are unique and different from UID's assigned previously to other persons. • Determine that default privileged UID's with publicly known passwords have been disabled or removed. • Verify that unsuccessful consecutive logon attempts are identified and result in account lockout or notifications to UID owners and Security

Risk to Be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
		Operations. • Review commands that can be run without a password.
I.4 Password Administration		

A weak password policy may result in unauthorized access to confidential data and systems.	A password configuration standard that requires a strong password parameters setting is documented within the Firm's IS policy.	• Check whether the system checks for a passwd confirm that /etc/default/login has (PASSREQ=YES).
		• Check the contents of the following files and commands:
		  • /etc/default/passwd (PASSLENGTH=, MAXWEEKS=, MINWEEKS=).
		  • etc/shadow
		  • Yppasswd, passwd, admintool
		• Check permission for the files above and ensure contents are not stored in cleartext.
		• Verify that user accounts are locked or disabled after a specified number of failed logon attempts.
		• Verify password and group file consistency checks.
		• Verify that passwords are encrypted:
		  • Identified in the /etc/passwd file
		  • X signifies the password is encrypted
		  • Username**:X**:UID:GID:User's full name:user's home directory: user's shell

I.5 UNIX Server Access		
<u>Root and Root Equivalent</u> The root account is not administered in a controlled manner. For instance, it may	A procedure has been documented for managing Root Accounts and addresses the	• Review with the UNIX server Administrator and IT Management the procedures covering the use of the root account. For example: What are daily operational tasks? Do they use their own personal UNIX

Risk to Be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
by shared among a large number of staff and used for a variety of purposes. This increases the risk of unauthorized access to the root account. Device files relating to physical devices at the console can be accessed from any terminal. Without the disabling of root remote login there is a risk that unauthorized persons may take full control of the production machine.	following: • Root account is not used for daily operational tasks. It is used only for single, specific tasks that cannot be performed under other accounts. • Passwords are different for clients and different types (builds) of servers. • Only a limited number of personnel know the root account password and these personnel are tracked. • Interactive root login is disabled for all terminals except a secure console. If root login is required, users login under their normal user account and then use /bin/su command to switch to root (note that the absolute path should be used). • Defined procedures exist in the event the root account is compromised. • Root's execution search path does not include the working directory or	accounts? Is SU limited to specific commands? • Obtain listing of personnel who know the root account password. • Determine what procedures would be undertaken if the root account were compromised. One way to find out if the root account is compromised is to monitor the integrity of root startup files, e.g., ownership, permission and contents of /.login, /.profile, /.cshrc, /.kshrc, /.emacs, /.exrc, /.forward, /.rhosts and /.Xdefaults. • Identify any accounts with UID0 (superusers) using: awk –F: '{if ($3=="0") print $1}' /etc/passwd: • Determine whether the root shell is changed (e.g., from /bin/bash to /sbin/nologin). • Check the execution path of the root by running: # echo $PATH. • Ensure that this does not include the current directory (no single dot or an empty entry) and that the directory is not world writeable.

Risk to Be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
	directories writeable by others.	
Remote root login Device files relating to physical devices at the console can be accessed from any terminal. Without the disabling of remote root login there is a risk that unauthorized persons may take full control of the production machine.	Remote root login is disabled. Device files relating to physical devices at the console (keyboard, mouse, microphone, and speaker) cannot be accessed from any other terminal.	• Review with the UNIX Server Administrator and IT Management the procedures for remote access. • Verify that remote root login is restricted. • Verify that the /etc/ssh/sshd_config file has "PermitRootLogin" set to "no". • Check that /etc/default/login contains the following line for secured consoles, which restricts remote root login: CONSOLE=/dev/console • Verify that the /etc/security file is empty. Determine if the file permission is appropriate (e.g., 600).
UID's Less Then 100 Users may be allocated UID's below 100 (system accounts) and may accidentally gain access to system files or other networked systems.	Users are not assigned UID's below 100. UID's below 100 are normally reserved for system accounts.	• Check the /etc/passwd file and identify any non-system accounts with UID's below 100 (below 500 for Linux).
Sudoers File Users have excessive privileges via the sudoers file (which allows users to have defined root privileges under their normal user ID).	There is a formal approval procedure regarding the modification of the sudoers file. All changes to the file are logged and the log and file is reviewed on a periodic basis to ensure that privileges are not excessive.	• Review with the UNIX Server Administrator and IT Management the procedures for the configuration of the sudoers file. • Determine if the sudoers file contents are appropriate (e.g., be careful with ALL:ALL).

Risk to Be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
Crontab Command Permitting general access to the crontab command allows an individual to run a command or a job at a later date from the cron command queue with system privileges.	Access to the system crontab command is restricted to authorized individuals.	• Determine if the files 'cron.allow' or 'cron.deny' exist and what their contents are. If 'cron.allow' exists, only the users within this file are allowed access while if 'cron.deny' exists, all users have access except the individuals listed within this file.
SU Command Usage Failure to use fully qualified command names when executing root commands increases the risk of an administrator accidentally running an alternate, and possibly malicious, version of a program located in another directory, with administrator privileges.	When using the 'SU' command to gain root access or when using any command while logged in as root, only fully qualified command names (i.e., full path and command name) are used.	• Review with the UNIX Server Administrator and IT Management the procedures for SU and verify that these require administrators to type '/usr/bin/su' instead of 'su' to run the command. Review any logs related to 'su' and root. Review the PATH and how it is configured.
Pluggable Authentication Modules (PAM) The lack of a formal security procedure for setting up PAM may result in an inconsistent and unsecured environment.	There is a formal procedure for setting up PAM. PAM is used to authenticate users to LDAP.	• Review with the UNIX Server Administrator and IT Management the procedures for managing PAM. • Verify that PAM settings are appropriate (e.g., unnecessary reply message). Obtain /etc/pam.d and /etc/LDAP.conf. Obtain /etc/pam.conf. • Determine how the procedure restricts NULL password. • Determine if the file permission setting for PAM configuration files is appropriate (e.g., 611).

Risk to Be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
J. Monitoring and Support		
J.1 Monitoring		

General
Lack of monitoring requirements defined in writing, agreed with senior management and documented as part of the UNIX Data Security Policy may result in unauthorized access to the UNIX environment.
	Active monitoring is performed periodically and senior management is kept informed of key risks.	• Review with the UNIX Server Administrator and IT Management the UNIX monitoring procedures including:
		  • Procedures for monitoring the availability and performance of UNIX servers.
		  • Procedures for monitoring, recording, reporting and resolving UNIX security events (e.g., superuser logon/logoff, failed attempts to login to root).
		  • Procedures for retention of the audit logs.
		  • Documentation of the procedures for server log maintenance and preservation.
		  • Procedures to monitor, escalate and report critical events (e.g., deviations from baseline settings) to appropriate personnel.
		• Determine if active monitoring occurs across all levels of UNIX security (physical, logical access, network, etc.) as part of the Firm's security program. Select a sample of monitoring results and verify if the monitoring activity has been carried out appropriately.
		• Determine the types of monitoring tools in use, the security events monitored, and the systems monitored with respect to the following:
		  • Compliance with UNIX data security policies and procedures.
		  • The threat level within the organization.
		  • The business impact from loss.
		  • Monitoring from a centralized location.
		  • Prioritization by security risk to the organization.

Audit Logging Lack of audit logs and their	Auditing, logging and monitoring programs are in use	• Review the UNIX audit logging procedures with the UNIX Server Administrator and IT Management:

Risk to Be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
periodic review may result in undetected UNIX breaches.	to log any potential occurrences of suspicious activity. Audit logs are reviewed on a regular basis.	• Ensure there is a written policy requiring audit logging. • Determine if logging is activated through review of the appropriate UNIX parameters. • Determine the file permissions over the audit logs and verify the controls in place to prevent unauthorized modifications to the audit logs. • Determine if log retention procedures are being adhered to. • Verify that audit logs are monitored and reviewed and that the frequency is adequate to address threats in a timely manner. • Review with the UNIX Server Administrator and IT Management the procedures for monitoring/auditing programs in use and logs reviewed. • Verify that the following logs are checked: • Users of the su command [var/adm/sulog or in syslog if syslog=yes in /etc/default/su • Log of failed login attempts • Verify that Cron activity (/var/cron/log if cronlog=yes in /etc/default/cron –) is also logged in the syslog • *.warn;*.err /var/log/syslog • *.kern /var/log/kernel • *.warn;*.err @loghost • *.kern @loghost • Obtain sample logs from several servers for the last 2 months. • Verify that all the devices are monitored, and that the important information associated with events, i.e., time, source address, and user ID, are recorded.

Risk to Be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
		• Assess whether these are detailed enough to permit timely identification of security issues.

Protection of Logs
Unauthorized access to security logs may provide the ability to hide unauthorized access to UNIX assets.
	Audit and security event logs are protected from unauthorized tampering or access to ensure the integrity of the data.
	
	Directories and files which contain the output of logs and security tools are secured against unauthorized modification.
		• Review with the UNIX Server Administrator and IT Management the audit log settings that have been configured and ensure that file permissions of the logs are appropriately defined.
		• Determine what controls are in place to protect security and audit logs.
		• For audit logs that contain sensitive information, determine if special care is taken to protect the audit logs from unauthorized disclosure.
		• Determine how the Firm ensures that the security and audit logs are not being altered or tampered with.
		• Determine if the logs are retained according to Firm policy.
		• Verify that group and world permissions are not granted for the following log files:
		  • Solaris
		  • Syslog directories (configured in syslog.conf)
		  • /var/adm/sulog
		  • /var/adm/loginlog
		  • /var/cron/log
		• Identify directories or files used for the logging and auditing of any security tools used to insure that these are also adequately secured.
		  • Obtain /etc/syslog.conf and determine whether logs are enabled
		  • Determine permission setting for log files is appropriate (ls –laR /var/log).

Security Monitoring Lack of regular security	Significant problems, incidents	• Review with the UNIX Server Administrator and IT Management the

Risk to Be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps

monitoring as appropriate for the amount of risk to the firm may result in undetected breaches of UNIX data security assets.	and errors are identified, logged, analyzed, communicated to relevant parties for correction, resolved on a timely basis, and escalated to Management.
	Logs are kept in a centralized log repository with appropriate access permissions.
		procedures for security monitoring.
		• Determine whether there is adequate monitoring of key security areas (e.g., fail-logon attempt, access key/critical system configuration files).
		• Determine if access violations to information or systems are logged.
		• Determine if information about the security condition of the UNIX environment is provided to senior management, a security committee, individuals in charge of critical business applications, and UNIX data security management. Information should:
		  • Provide decision-makers with an informed view of the adequacy of their UNIX data security arrangements.
		  • Reveal areas where improvement is needed.
		  • Identify information and systems that are subject to unacceptable risks.
		  • Highlight actions to mitigate the risks.
		• Verify if escalation procedures are defined and implemented to support timely resolution and reporting to management.
		• Determine if post-mortem meetings are required for significant problems, incidents and errors. They should involve relevant personnel and cover causes, effects, and resolutions.

<u>Server Monitoring</u> Without monitoring, system errors may not be discovered and fixed in a timely manner.	A formal and automated monitoring procedure is in place to alert the UNIX Server Administrator if the server and/or services are not functioning properly. A formal monitoring procedure	• Review with the UNIX Server Administrator and IT Management the monitoring procedures for the UNIX environment. • Determine if the monitoring procedures are adequate. • Review with the UNIX Server Administrator and IT Management the disk space capacity monitoring procedures for the UNIX environment. • Determine if the monitoring procedures are adequate to alert the

Risk to Be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
	is in place to alert the UNIX SA about disk space capacity issues.	UNIX SA about the disk space status.
J.2 Responding to Threats and Mitigating Risk		
Failure to respond to identified threats and security breaches results in unauthorized access to UNIX data.	Procedures have been developed to respond to specific threats identified as part of the threat matrix.	• Verify that procedures exist for responding to threats. • Determine that the appropriate areas, level of management or law enforcement get involved based on the incident's severity. • Determine if procedures for handling security incidents take into consideration the severity of the issue. • Verify that a process exists for examining how well the organization is doing with regard 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?
J.3 Problem Management		
Without problem management procedures, issues remain unresolved and may seriously impact critical business operations.	Procedures are in place to standardize how problems are reported, prioritized, logged, tracked, escalated, and resolved. Problem incidents are prioritized, documented, and tracked within Remedy.	• Review with the UNIX Server Administrator and IT Management how problems are reported, prioritized, logged, tracked, escalated and resolved. • Review a sample of Remedy tickets and determine whether problems were escalated and resolved properly.
J.4 Change Management		
Deploying untested patches may result in production system disruption.	There is a formal change management procedure for deploying UNIX patches.	• Select a sample of patches and determine whether they are tested prior to being deployed to production. • Determine whether the application owner approved the migration.

Risk to Be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
Deploying untested hosts may result in disruption. Deploying hosts without all the components and patches defined in the current build could result in security vulnerabilities that allow unauthorized use.	There is a process for deploying new UNIX hosts, including installing all the OS elements and patches for the UNIX build, and testing the hosts prior to putting them into use.	• Review with the UNIX Server Administrator and IT Management the process for deploying new UNIX hosts.
J.5 Server Inventory Management		
An accepted method for inventorying UNIX servers and the level to which individual components should be recorded is not formalized. As a result, server inventories do not contain sufficient information and are not up-to-date. Inconsistencies in the approach to inventorying may lead to key UNIX servers not being adequately supported.	An accepted method for inventorying servers and the level to which individual components should be recorded has been formally defined and documented. These inventories are updated on a regular basis.	• Review with the UNIX Server Administrator and IT Management the method being used for inventorying servers. • Determine whether the method is accurate and whether the inventory contains enough information to accurately reflect and describe the UNIX server inventory. • Verify that the inventory is updated on a regular basis and that there is a procedure for updating the inventory when new servers are added or old servers removed.

Risk to Be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
K. Backup, Recovery, and BCP		
K.1 Business Continuity Management		

Lack of Business Continuity Management and a Business Continuity Plan (BCP) that specifically addresses UNIX data processing requirements may result in:
• Increased inability to support UNIX applications and protect proprietary data in recovery mode
• Deterioration of security and increased likelihood of data breaches
• Expensive recovery costs for stolen, lost, or damaged UNIX data
	The Firm has included in its Business Continuity Management process specific steps and actions to insure continuity of UNIX processing. This is accomplished through the following activities with respect to UNIX data security needs:
	• UNIX environment impact analysis
	• Writing and implementing a Business Continuity Plan
	• Testing, maintaining and re-assessing the Business Continuity Plan
	• Disaster recovery scenarios and procedures are documented and tested periodically
		• Determine if there is a managed process in place for developing and maintaining Business Continuity throughout the organization and that it addresses the UNIX environment.
		• Determine if events that could cause interruptions to the UNIX environment 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 the UNIX environment.
		• Determine if a strategic plan was developed based on the risk assessment results to determine an overall approach to business continuity for UNIX processing needs.
		• Determine if plans were developed to restore business operations with required UNIX data security safeguards within the required time frame following an interruption or failure to business processes.
		• Verify that the plan is regularly tested and updated.
		• Determine if the framework identifies conditions for activation and individuals responsible for executing the UNIX component of the plan.
		• Determine if business continuity plans are maintained and updated through regular reviews to ensure their continuing effectiveness.
		• Review with the UNIX Server Administrator and IT Management the UNIX BCP plans including the following:
		  • Procedures for backup of UNIX-based servers
		  • Contingency procedures for the UNIX environment
		  • Disaster recovery test results

Risk to Be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
		• Procedures for periodic testing of the recovery of the UNIX environment
K.2 UNIX Backup and Recovery		
The lack of UNIX backup procedures hinders the ability to recover the UNIX operating system and mission-critical UNIX applications.	A formal UNIX backup procedure is documented and tested regularly.	• Review with the UNIX Server Administrator and IT Management the UNIX backup procedure. • Assess the procedure for comprehensiveness and completeness and verify that it includes the UNIX OS and applied patches. • Review with the UNIX Server Administrator and IT Management the UNIX recovery procedures for the UNIX environment. • Assess the procedures for comprehensiveness and completeness (e.g., whether they include recovery timelines). • Obtain and review evidence of backup activity.
K.3 UNIX Contingency Environment		
The lack of a UNIX contingency environment hinders the ability to recover the UNIX operating system and mission- critical UNIX applications.	A physical UNIX production backup environment exists in a different location than the primary production environment.	• Determine whether there is a procedure to ensure that the contingency environment mirrors the production environment. • Review the failover procedures from primary to backup, the amount of manual intervention required, and the length of time it takes to insure that it meets business recovery needs as documented in the Business Continuity Plan. • Verify that all the production access controls are also replicated in the backup environment. • Verify that these procedures are periodically tested by reviewing the results of a recently conducted disaster recovery test.
L. Prior Audit Issues		
Prior and/or ongoing issues	Management conducts a review	• Obtain a copy of prior UNIX data security audit issues that related to

Risk to Be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps

exist that prevent the Firm from operating a compliant and effective UNIX data security infrastructure.	of prior issues, and addresses the resolution of open issues and the meeting of previously established target dates.	this review and perform issue follow-up to ensure that actions are adequately resolved.
		• Review past reports for outstanding issues or previous problems. Consider:
		  • Regulatory reports of examination
		  • Internal and external audit reports, including SAS 70 reports
		  • Organization's overall risk assessment and profile
		• Review management's response to issues that were raised since the last examination. Consider:
		  • Adequacy and timing of corrective action
		  • Resolution of root causes rather than just specific issues
		  • Existence of any outstanding issues

M. Conclusions and Action Plan		
Failure to address the UNIX data security audit gaps may impair the Firm's ability to maintain safe, secure, and reliable control of information assets. This may subsequently impact business operations and profitability, and place the firm in non-compliance with regulations.	Audit findings are communicated to management and audit sponsors. Corrective actions are discussed with the appropriate groups.	• Identify gaps in the UNIX data security audit. • Determine actions needed to close gaps. • Assign responsibility to action items. • Determine target date for each action. • Ensure that review of action items becomes part of the continuous follow-up process, as well as part of the next audit if these have not been resolved and closed by then.

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 grant or revoke 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: • Entry to a physical location. • File permissions, such as create, read, edit or delete on a file server. • Program permissions, such as the right to execute a program on an application server. • 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, e.g., accounting.
Application Development Environment	A non-production and usually less secure computer environment that software engineers use 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 UNIX data 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.
Mobile 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 UNIX data 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.

IV. UNIX Configuration Files

Critical UNIX Configuration Files for Audit Review

1	Output of /etc/cron.allow, /etc/cron.deny, /etc/at.allow and /etc/at.deny files.
2	Output of '/etc/login.defs' file.
3	Output of /etc/shadow file.
4	Output of /etc/passwd file
5	Output of /etc/group file
6	Output of /etc/sudoers
7	Output of '/var/log/sulog' or '/var/log/secure' file
8	Output of /etc/securetty
9	Output of /etc/inetd.conf and contents of /etc/xinetd.d directory
10	File permissions for /, /bin, /sbin, /usr/bin, /usr, /etc and /var directories.
11	Output of '/etc/syslog.conf' file
12	Output of '/var/log/secure'
13	Output of /var/log/sulog' and '/var/log/messages'
14	Output of '/etc/hosts.equiv' file
15	Output of .rhosts' files

Default PAM Configuration
The following PAM modules are implemented in the PAM libraries on UNIX.

Name	Description	Notes
pam_console	Console Module	Implements the "CONSOLE" and "USERS" defaults feature for login.
pam_deny	Locking Out Module	Returns an authentication failure.
pam_dialpass	Dialup Password Module	Implements */etc/dialups*, */etc/d_passwd* authentication.
pam_ftp	FTP Module	Implements Anonymous FTP Authentication (i.e., prompts for an email password).
pam_lastlog	Last Login Module	Maintains the */var/log/lastlog* file.
pam_listfile	List-File Module	Denies or allows services based on an arbitrary file.
pam_mail	Mail Module	This module looks at the user's mail directory and indicates whether the user has any mail in it.
pam_nologin	No Login Module	If */etc/nologin* exists but is empty, the message `Logins currently disabled` is returned and access is denied.
pam_permit	Promiscuous Module	Returns authentication success.
pam_rhosts	rhosts Module	Provides authentication as described on rhosts(4), as used by **rlogin**, **rsh**, and similar utilities.
pam_rootok	Root Access Module	Provides root access without requiring a password.
pam_shells		
pam_UNIX	UNIX Password Module	The following options are always enabled: **bigcrypt** **likeauth** **nis** **nodelay** **shadow** If **pam_UNIX** was *not* used to authenticate (e.g. **rsh** command), the **pam_UNIX** account management function skips all password

		expiration checks. If the **nullok** option is not set for the account management function, and the authenticating user has no password, the module returns PAM_NEW_AUTHTOK_REQD (same as if password was expired). This is needed to implement the **login** PASSREQ and MANDPASS features.
pam_warn	Warning Logger Module	Logs information about a proposed authentication or password update.