Planned Audit Program Steps for Perimeter and Internal Network Security

I Situation/ Background:

What Risk or Requirement justifies a specific Audit (Implementation of the Tactical guidance and associated functional requirements)?

- 1. What critical business process or function needs to be assessed and why (BIA or Risk Assessments)?
- 2. What precedence is there for an investigation or the gathering of evidence?
- 3. What regulatory or policy compliance issue(s) exist to support the goal(s) and objective(s) for a specific audit?
- 4. How does this one audit fit into the bigger picture, e.g., time, resources, the Tactical / Strategic goals, and other auditor agencies that will audit our institution?
- 5. Is the goal to place emphasis upon Risk Assessment, Risk Management, or Risk Avoidance?
- 6. What <u>Critical Process Information</u> is available to support the goals and objectives for a specific audit? The question to ask is "What threats and their associated vulnerabilities exist?" "What is the likelihood of those events occurring?" and "What controls are in place to mitigate the risk?"
- 7. Will the process be deductive (investigation of predefined particulars to prove some hypotheses) or inductive (the collection of facts that may or may not reveal patterns or activities that introduce risk)?



Pre-Audit considerations

- 8. Understand the categories of risk and how they may or may not apply:
 - a. Strategic Affects the entities' ability to achieve goals and objectives
 - b. Compliance Affect compliance with laws and regulations, safety and environmental issues, litigation, conflicts of interest, etc.
 - c. Reputational Affects reputation, public perception, political issues, etc.
 - d. Financial Affects loss of assets, technology, etc.
 - e. Operational Affects on-going management processes and procedures
- 9. Define what is to be audited and associate outcomes scope and criteria.
 - a. What process of examining and validating documents, data, processes, procedures, systems, or other activities will be used to ensure that the audited entity complies with objectives?
 - b. What set of business rules, system control, government regulations, or security policies will be used to measure and determine compliance of the audited entity?
- 10. Define expected outcomes or results for which the audit will produce, e.g., a report which identifies ..., goals or objectives resulting from the audit.
- 11. Measure impact of risk in terms of key business roles or functional areas of the entity being audited

- a. History of institution or entity being audited (scope of offerings as related to IT systems or services)
- b. Financial Statements
- c. Student and Faculty FTE and ratios or significant changes in personnel
- d. Applicable trends that are affecting other educational institutions or associated entities

Conclusion of Situation / background Assessment(s)

The information systems network infrastructure should be assessed to identify specific vulnerabilities associated with known High Risk threats to determine if the proper controls (assess the indicators) are effectively being applied to mitigate risks. The need for the audit is based upon a(n) ... (annual risk assessment process verifying controls by rotating through all USG Institutions every three to four years). There are ... (no specific regulatory or compliance issues being addressed, though the GTA's current emphasis upon FISMA compliance via NIST should be considered). The audit will be a(n) inductive process focusing upon the institutions current ... (risk management processes and associated activities versus avoidance or assessment, since the audit is not assessing any new implementations or the investigation of an identified issue). The scope and criteria for current key business goals and associated functions for the institutions are ... (unknown and will require prior coordination with Institution's POC to ensure high risk or critical resources are identified ahead of time so an appropriate precedence is established and time allocated to ensure risk mitigation controls can be properly assessed). The overall methodology for information system analysis will be a top down approach. This approach will first identify key business functions and their associated business goals and objectives. Once these are identified and agreed upon for each business function, the key associated requirements, resources, and processes will be identified and assessed to determine if risk is being managed. Focus will be upon Control Practices and Responsibility and Accountability associated with key activities with an expected CMMI level 3 criteria for High Risk Critical processes.



II Mission (goals and objectives): The OIA IT department will conduct an audit of <u>Audited Institution or entity name</u> on <u>date of onsite audit</u> to validate that appropriate controls and procedures exist to mitigate the potential threat of inappropriate access being allowed to High risk critical campus network infrastructure and information resources.

III Execution (Procedural Steps):

1. The explanation of how critical characteristics of the mission will be complete (EWP emphasis - what steps and / or processes involved to complete the mission):

- a. Controls to be assessed are: preventive, detective, corrective, administrative, technical, and physical
- b. Review previous audit findings, e.g., State, Federal, or USGBOR
- c. Audit programs / processes to support the mission and target specific application of controls and the individuals who will complete each set of tasks and the time to be invested during the audit
 - i. Perimeter Network Security (25%) ______ (auditor name)
 - ii. Internal Network Security (50%) ______ (auditor name)
 - iii. Remote Access (25%) _____ (auditor name)
- 2. Key Characteristics and Operational Environment
 - a. Policy on mobile computing, teleworking, etc.
 - b. Clear understanding and presentation of Network topology with defined and controls for ingress and egress points
 - c. Clearly defined DMZ or other areas proxied for various purposes
 - d. Routing and switching protocols / ports and network segmentation clearly defined
 - e. Firewall policy and implementation clearly defined and effective
 - f. Network services and utilization of services defined and controlled
 - g. Network management systems defined and controlled
 - h. Network connection requirements or limitations access layer via port, wireless, website (internet)
 - i. Operating Systems and Applications providing services
 - i. Access is controlled
 - ii. Systems properly secured and patched
 - j. Other business owner responsibilities?
 - k. Key systems to be evaluated are the major network support systems associated with user use or access:
 - i. Banner
 - ii. PeopleSoft
 - iii. Other database systems (alumni System)
 - iv. Directory and network services (NDS, AD, LDAP, DNS, DHCP, etc.)
 - v. PCI-DSS / One Card system / POS / TOS
 - vi. Email
 - vii. Network resources and associated policies and procedures for:
 - 1. NOC
 - 2. Administration
 - 3. Auxiliary Services
 - 4. Faculty
 - 5. Students
 - viii. Internal and external network devices
 - I. Checklist identified for Systems evaluated?
 - i. Internal Control Checklist Questionnaire for NetSec.doc
 - ii.
 - iii.
 - iv.
- 3. Standards for the Audit Methodology
 - a. Standards for the execution of the audit will comply with IIA guidance. Processes or outcomes will be measured using Industry Standard businesses practices identified in ISACA (CoBIT4.01) and the following additional guidelines where applicable.
 - i. USG Information Technology Security Guidelines (Apr 2003)

- ii. Board of Regents Business Procedure Manual (Jan 2005)
- iii. Limited application using the ISO 27000 series, ITIL, and common practices
- b. CMMI level 3 will be the minimum criteria for measuring key processes for maturity
- 4. Scheduled objectives and milestones of the audit (programs and process) to support the mission

Objectives / Milestones	Auditor Responsible	Time / Hours	Start	End
,				

IV Command, Control, & Communication:

- Key Leadership contact information and communication procedures or protocol expected
 a. Key shareholders (contact information):
 - , i.
 - ii.
 - iii.

iv.

- b. Are they any special requirements or considerations outside of our normal operations?
- 2. Logistics Resources required to complete the mission Identify & coordinate logical requirements

a.

b.

c.

- d. Support needs at audited entity to conduct the program steps
- e. Coordination and scheduling with audited entity POC in how the audit evidence will be gathered and what resources need to be made available to the auditors e.g., people for interviews, IT systems, documentation, etc.
- f. Any additional cost or logistical concerns
- 3. Communications notification and dialogue required to complete the mission
 - g. Key shareholders regular situational audit updates to the audited entity
 - h. Interviewees coordination and conduct
 - i. Administration or Operational Services, e.g., IT, HR, etc
 - ii. Functional Faculty
 - iii. Auxiliary Service or outside agencies contracted to support the audited entity

i. Colleagues (peer auditors) and superiors – special or general guidance as the process progresses

V Safety (physical or political considerations):

- 1. Sensitivity to issues that are local to the audited entity
- 2. Physical safety concerns
 - a. Assessments involving or around resources or equipment that is hazardous
 - b. Avoidance of placing the auditor in a situation that could compromise the integrity of the evidence being gathered or their personal character

Methods for Assessing the Controls for Perimeter and Network Security (DS5 01-11)

• Through inquiry and observation, determine if the security management function effectively interacts with key enterprise functions, including areas such as risk management, compliance and audit.

• Review the process for identifying and responding to security incidents, selecting a sample of recorded incidents. Through inquiry and review of supporting documentation, determine whether appropriate management action has been taken to resolve the incident.

• Select a sample of employees and determine if computer usage and confidentiality (non-disclosure) agreements have been signed as part of their initial terms and conditions of employment.

• Review the IT security strategy, plans, policies and procedures to determine their relevance to the organization's current IT landscape, and determine when they were last reviewed and updated.

• Review the IT security strategy, plans, policies and procedures, and verify that they reflect the data classification.

• Interview stakeholders and users on their knowledge of the IT security strategy, plans, policies and procedures, and determine if stakeholders and users find them to be relevant to risks and organizational practices."

• Ask executive management about any recent or planned changes to the organization (e.g., business unit acquisitions/dispositions, new systems, changes in regulatory environment), and determine if the IT security plan is properly aligned.

• Determine if security processes have been implemented to uniquely identify and control the actions of all users and processes through review of system (development, test and production systems) and application accounts, job queues and services, and security software mode settings.

• Through a sample of access control lists (ACLs), determine whether the security provisioning process appropriately considers the following:

- Sensitivity of the information and applications involved (data classification)
- Policies for information protection and dissemination (legal, regulatory and contractual requirements)
- The 'need-to-have' of the function
- Standard user access profiles for common job roles in the organization
- The need for segregation for the access rights involved
- Data owner and management's authorization for access
- The documentation of identity and access rights in a central repository
- Creation, communication and change of initial passwords

• Through inquiry and review of sampled ACLs, determine if a process exists for resolving access provisioning requests that are not commensurate with established security authentication practices and roles.

• Determine if a risk assessment process was utilized to identify possible segregation of duties and if an escalation process was utilized to obtain added levels of management authorization.

• Determine if authentication and authorization mechanisms exist to enforce access rights according to the sensitivity and criticality of information (e.g., password, token, digital signature).

- Determine if trust relationships enforce comparable security levels and maintain user and process identities.
- Select a sample of user and system accounts and a sample ACL to determine existence of the following:
- Clearly defined requested role and/or privileges
- Business justification for assignment
- Data owner and management authorization
- Business/risk justification and management approval for non-standard requests
- Access requested commensurate with job function/role and required segregation of duties

- Documentation evidencing adherence to and completion of the provisioning process

• Select a sample of critical network devices and system services, and determine if access control mechanisms have been routinely evaluated and tested to confirm their operational effectiveness.

• Select a sample of critical network devices and system services, and determine if they have been routinely monitored for existence of security incidents.

• Sample security baselines and determine if they are appropriately aligned to the organization's risk profile and levels of accepted risk and if they take into account common risks and vulnerabilities (i.e., conform to leading practices).

• Select a sample of IT devices and determine their compliance with established security baselines. For deviations from baselines, determine if a risk assessment was performed and if management approved the deviation from the baseline.

• Determine if a security review process has been integrated into the organization's acquisition and implementation processes (AI) and delivery and support processes (DS), requiring security management's involvement and approval of any IT changes that would impact the design or operation systems security. The review process should consider:

- Overall technology architecture
- Database access and security design
- Protocol, port and socket usage
- Required services
- User remote access and modem requirements
- Server-to-server authentication and encryption
- Scalability, availability and redundancy
- Session management and cookie usage
- Administrative capabilities
- User ID and password management
- Audit trails and logging/reporting

• Determine if security audit trails capture user identification (ID), type of event, date and time, success or failure indication, origination of event, and the identity or the name of the affected object. Logged events should include accesses to sensitive data, actions by administrative and privileged accounts, initialization of audit logs, and modification of system-level objects.

• Inspect and review documents supporting the recording, analysis and resolution of potential security incidents, and perform the following steps:

- Understand the methods used to categorize incidents and identify actionable threats.

- Identify specific logged security incidents, and inquire as to the nature and disposition of the incident.

• Inspect documentation evidencing the process used to match the organization's network device inventory to published vulnerabilities for the purpose of verifying that all devices are at current release and security patch levels.

• Determine if formal management responsibilities and procedures exist throughout the key management life cycle, including changes to encryption equipment, software and operating procedures.

• Assess whether the data/system protection software is centrally distributed throughout the network environment.

• Assess the control features for filtering incoming traffic against unsolicited information.

• Select a sample of critical network devices, and confirm that the devices are properly secured with special mechanisms and tools (e.g., authentication for device management, secure communications, and strong authentication mechanisms) and that active monitoring and pattern recognition are in place to protect devices from attack.

• Select a sample of network devices, and determine if the devices have been configured with minimal features enabled (e.g., features that are necessary for functionality and hardened for security applications); all unnecessary services, functionalities and interfaces have been removed; and all relevant security patches and major updates are applied to the system in a timely manner before going to production.

• Select a sample of new network devices or changes to existing network devices and determine that the organization's Acquire and Implement (AI) process controls and Deliver and Support (DS) process controls have been followed.

- Select a sample of firewall devices, and review ACLs for the following:
- Access rules effectively segregating trusted and non-trusted network segments
- Documentation evidencing the business purpose and management's approval of rules
- Configurations following management-approved baselines
- Devices that are current on version and patch release levels

• Determine if encryption is utilized for all non-console administrative access, such as SSH, VPN or SSL/TLS.

• Assess whether automated controls safeguard the data and systems, such that data are transmitted through reliable sources.

• Determine if user management periodically reviews user profiles and access rights to ensure the adequacy of access rights and requirements for segregation of duties.

- Verify that direct access to data is prevented or, where required, controlled and documented accordingly.
- Verify that the quality requirements for passwords are defined and enforced by systems.

• Determine the level of security consciousness within the organization by reviewing functional and operational documentation for the existence of security considerations (e.g., involvement of the security management function within the SDLC).

• Benchmark the information security organization (e.g., size, lines of reporting) against similar organizations, and benchmark formalized policies, standards and procedures to international standards/recognized industry best practices.

• Determine if the security management function is commensurate with the size and complexity of the IT landscape. Consider the following:

- Size, complexity and diversity of the IT landscape
- Use of security administration tools and technology

- Alignment of security management to business lines (e.g., do organization segments have competing security functions?)

- Skills and training of security management personnel

• Determine if members of executive management communicate the importance and their support of the security management organization. Consideration should be given to executive management or security steering committee approval of formalized security policies.

• Determine the existence of a management-approved security charter and policies, standards and procedures that address logical security for all relevant aspects of the organization's IT landscape.

• Determine if the IT security plan has adequately considered the security profile of the organization, including any regulatory and compliance requirements.

• Assess the ability of the security management organization to execute and monitor compliance with the plan. Consideration should be given to the size of the organization, use of security assessment and administration technology and tools, and required experience levels and ongoing training received by security personnel.

• Select policy, standards and procedural documentation from various financial, operational and compliance areas within the organization, and determine if key provisions of the IT security plan have been appropriately reflected in the documentation.

• Determine if a security review process has been integrated into the organization's AI and DS processes, requiring security management's involvement and approval of any IT changes that would impact the design or operation systems security.

• Identify the existence and reasonableness of anonymous and group accounts (e.g., nobody, web user, everybody), remote processes and started tasks. Consideration should be given to the nature and scope of transaction authorities, the risk of possible escalation of privileges, the process origin (e.g., trusted, non-trusted), or if a security design review was performed for system and application initiated jobs and processes.

• Determine if security software, applications and supporting systems software has been configured to enforce user authentication or propagate user and process identities. Determine if default accounts exist to authenticate anonymous users or processes.

• Determine sources of non-trusted access (e.g., business partners, vendors), and determine how access has been assigned to provide uniquely identifiable account holders and appropriate protection of information.

• Through the use of audit software tools or scripts, identify the existence of inactive or unused accounts and determine the existence of a business justification.

• Identify active vendor or contractor accounts, and determine if access is commensurate with the terms and duration of the contract.

• Determine if vendor-supplied accounts have been appropriately safeguarded (e.g., default passwords changed, accounts revoked).

• Assess the reasonableness of the nature and frequency of verification and vulnerability assessment processes utilized, considering the organization's risk profile, size, complexity and diversity.

• Determine if security scripts and tools are utilized to test the existence of common vulnerabilities, the effectiveness of security mechanisms and the effectiveness of user access administration processes (e.g., existence of inactive or never used accounts, terminated user accounts, accounts without passwords or forced password changes).

• Identify and select a sample of organization-critical network devices (hardware and application systems) and atrisk perimeter network devices. Determine the existence of security sensors or use of host logging to capture incidents, and ensure that security incidents are included in the daily review process.

• Obtain a sample of security-related incident work order tickets, and determine if the issue has been appropriately resolved and closed in a timely manner.

• Determine if security tool deployment appropriately addresses all principal technologies utilized by the organization and if personnel possess the required skills to appropriately operate the security tools and technologies.

• Determine if security personnel are required to attend annual training and if security tools receive routine updates to threat and vulnerability engines and supporting database/signatures.

• Determine whether the security controls have been implemented to prevent exposure from malicious attacks and vulnerabilities.

• Determine if portable code (e.g., Java, JavaScript) and downloaded binaries and executables are scanned before being allowed into the network or blocked from entering the network.

• Determine that the organization's network documentation accurately reflects the current network environment, including wireless devices, and examine the network design to determine if security barriers are strategically placed at the network's perimeter, between the organization's trusted internal network and non-trusted public (i.e., Internet), vendor (i.e., service organization) or business partner (i.e., extranet) segments.

• Verify that changes to security-relevant parameters follow the organization's change management processes and are authorized and tested accordingly.

COBiT4.01 to NIST Mappings for the Areas being Assessed

DS5 Ensure Systems Security

DS5.7 Protection of security technology states: 'Make security-related technology resistant to tampering, and do not disclose security documentation unnecessarily'.

This was mapped with:

• PE-4 Access Control for Transmission Medium, which requires the organization to control physical access to information system distribution and transmission lines within organizational facilities to prevent accidental damage, eavesdropping, intransit modifications, disruption, or physical tampering

• SA-5 Information System Documentation, which requires the organization to ensure that adequate documentation for the information

system is available, protected when required, and distributed to authorized personnel

• SC-3 Security Function Isolation, which requires the information system to isolate security functions from non-security functions

The COBIT control seems to imply a broader non-tampering requirement. The US federal perspective does not require any particular

level of tamper resistance.

DS5.9 Malicious software prevention, detection and correction states: 'Put preventive, detective and corrective measures in place (especially up-to-date security patches and virus control) across the organization to protect information systems and technology from malware (e.g., viruses, worms, spyware, spam)'.

This was mapped with:

• SC-18 Mobile Code, which requires the organization to:

- Establish usage restrictions and implementation guidance for mobile code technologies based on the potential to cause damage to the information system if used maliciously

– Document, monitor, and control the use of mobile code within the information system. Appropriate organizational officials authorize the use of mobile code.

• SI-3 Malicious Code Protection, which requires the information system to implement malicious code protection

• SI-7 Software and Information Integrity, which requires the information system to detect and protect against unauthorized changes to software and information

• SI-8 Spam Protection, which requires the information system to implement spam protection

DS5.10 *Network security* states: 'Use security techniques and related management procedures (e.g., firewalls, security appliances, network segmentation and intrusion detection) to authorize access and control information flows from and to networks'.

This was mapped with:

• <u>AC-4 Information Flow Enforcement</u>, which requires the information system to enforce assigned authorizations for controlling the flow of information within the system and amongst interconnected systems in accordance with applicable policy

• <u>SC-7 Boundary Protection</u>, which requires the information system to monitor and control communications at the external boundary of the information system and at key internal boundaries within the system

• <u>SI-4 Information System Monitoring Tools and Techniques</u>, which requires the organization to employ tools and techniques to monitor events on the information system, detect attacks and provide identification of unauthorized use of the system

DS5.11 Exchange of sensitive data states: 'Exchange sensitive transaction data only over a trusted path or medium with controls to provide authenticity of content, proof of submission, proof of receipt and non-repudiation of origin'.

This was mapped with:

• AU-10 Nonrepudiation, which requires the information system to provide the capability to determine whether a given individual took a particular action (e.g., created information, sent a message, approved information [e.g., to indicate concurrence or sign a contract] or received a message)

• SC-9 Transmission Confidentiality, which requires the information system to protect the confidentiality of transmitted information

• SC-11 Trusted Path, which requires the information system to establish a trusted communications path between the user and the following security functions of the system: based on organization-defined security functions to include at a minimum, information system authentication and reauthentication

• SC-16 Transmission of Security Parameters, which requires the information system to reliably associate security parameters with information exchanged amongst information systems

• SC-23 Session Authenticity, which requires the information system to provide mechanisms to protect the authenticity of communications sessions

COBiT 4.01 Criteria for Programs

DS5.01-11: Ensure Systems Security

Summary:

The need to maintain the integrity of information and protect IT assets requires a security management process. This process includes establishing and maintaining IT security roles and responsibilities, policies, standards, and procedures. Security management also includes performing security monitoring and periodic testing and implementing corrective

actions for identified security weaknesses or incidents. Effective security management protects all IT assets to minimize the business impact of security vulnerabilities and incidents.

Objective / Criteria:

Management of the process of Ensure Systems Security that satisfies the business requirements for IT of maintaining the integrity of information and processing infrastructure and minimizing the impact of security vulnerabilities and incidents is ...

0 Non-existent when The organization does not recognize the need for IT security. Responsibilities and accountabilities are not assigned for ensuring security. Measures supporting the management of IT security are not implemented. There is no IT security reporting and no response process for IT security breaches. There is a complete lack of a recognizable system security administration process.

1 Initial/Ad Hoc when The organization recognizes the need for IT security. Awareness of the need for security depends primarily on the individual. IT security is addressed on a reactive basis. IT security is not measured. Detected IT security breaches invoke finger-pointing responses, because responsibilities are unclear. Responses to IT security breaches are unpredictable.

2 Repeatable but Intuitive when Responsibilities and accountabilities for IT security are assigned to an IT security coordinator, although the management authority of the coordinator is limited. Awareness of the need for security is fragmented and limited. Although security-relevant information is produced by systems, it is not analyzed. Services from third parties may not address the specific security needs of the organization. Security policies are being developed, but skills and tools are inadequate. IT security reporting is incomplete, misleading or not pertinent. Security training is available but is undertaken primarily at the initiative of the individual. IT security is seen primarily as the responsibility and domain of IT and the business does not see that IT security is within its domain.

3 Defined Process when Security awareness exists and is promoted by management. IT security procedures are defined and aligned with IT security policy. Responsibilities for IT security are assigned and understood, but not consistently enforced. An IT security plan and security solutions exist as driven by risk analysis. Reporting on security does not contain a clear business focus. Ad hoc security testing (e.g., intrusion testing) is performed. Security training is available for IT and the business but is only informally scheduled and managed.

4 Managed and Measurable when Responsibilities for IT security are clearly assigned, managed and enforced. IT security risk and impact analysis is consistently performed. Security policies and practices are completed with specific security baselines. Exposure to methods for promoting security awareness is mandatory. User identification, authentication and authorization are standardized. Security certification is pursued for staff who are responsible for the audit and management of security testing is done using standard and formalized processes leading to improvements of security levels. IT security processes are coordinated with an overall organization security function. IT security reporting is linked to business objectives. IT security training is conducted in both the business and IT. IT security training is planned and managed in a manner that responds to business needs and defined security risk profiles. KGIs and KPIs for security management have been defined but are not yet measured.

5 Optimized when IT security is a joint responsibility of business and IT management and is integrated with corporate security business objectives. IT security requirements are clearly defined, optimized and included in an approved security plan. Users and customers are increasingly accountable for defining security requirements, and security functions are integrated with applications at the design stage. Security incidents are promptly addressed with formalized incident response procedures supported by automated tools. Periodic security assessments are conducted to evaluate the effectiveness of implementation of the security plan. Information on threats and vulnerabilities is systematically collected and analyzed. Adequate controls to mitigate risks are promptly communicated and implemented. Security testing, root cause analysis of security incidents and proactive identification of risk are used for continuous process improvements. Security processes and technologies are integrated organization-wide. KGIs and KPIs for security management are collected and communicated. Management uses KGIs and KPIs to adjust the security plan in a continuous improvement process.

Scope:

Control over the IT Process of Ensure Systems Security that satisfies the business requirement for IT of maintaining the integrity of information and processing infrastructure and minimizing the impact of security vulnerabilities and incidents **by focusing on** defining IT security policies, procedures and standards, and monitoring, detecting, reporting and resolving security vulnerabilities and incidents

is achieved by

- Understanding security requirements, vulnerabilities and threats
- Managing user identities and authorizations in a standardized manner
- Testing security regularly

and is measured by

- Number of incidents damaging reputation with the public
- Number of systems where security requirements are not met
- Number of violations in segregation of duties

Procedure Step: DS5.07 - Protection of Security Technology

Determine and analyze

• whether and confirm that policies and procedures have been established to address security breach consequences (specifically to address controls to configuration management, application access, data security and physical security requirements).

- the control records granting and approving access and logging unsuccessful attempts, lockouts, authorized access to sensitive files and/or data, and physical access to facilities.
- whether and confirm that the security design features facilitate password rules (e.g., maximum length, characters, expiration, reuse).
- whether and confirm that the control requires annual management reviews of security features for physical and logical access to files and data.
- that access is authorized and appropriately approved.
- security reports generated from system tools preventing network penetration vulnerability attacks.

Additional Tasks:

Purpose:

Make security-related technology resistant to tampering, and do not disclose security documentation unnecessarily.

Risk / Effect:

DS5.7 Value Drivers

- Corporate security technology protected
- Reliable information secured
- Corporate assets protected

DS5.7 Risk Drivers

- Exposure of information
- Breach of trust with other organizations
- Violations of legal and regulatory requirements

DS5.7 Practical Controls for Protection of Technology

- Ensure that all hardware, software and facilities related to the security function and controls, e.g., security tokens and encryptors, are tamperproof.
- Secure security documentation and specifications to prevent unauthorized access. However, do not make security of systems reliant solely on secrecy of security specifications.
- Make the security design of dedicated security technology (e.g., encryption algorithms) strong enough to resist exposure, even if the security design is made available to unauthorized individuals.
- Evaluate the protection mechanisms on a regular basis (at least annually) and perform updates to the protection of the security technology, if necessary.

DS5.7 **Test for the Controls** for the Design of Protection of Technology Perimeter and Network Security Program, 7/30/2012 8:41:14 PM version 1.3

- Enquire whether and confirm that policies and procedures have been established to address security breach consequences (specifically to address controls to configuration management, application access, data security and physical security requirements).
- Inspect the control records granting and approving access and logging unsuccessful attempts, lockouts, authorized access to sensitive files and/or data, and physical access to facilities.
- Enquire whether and confirm that the security design features facilitate password rules (e.g., maximum length, characters, expiration, reuse).
- Enquire whether and confirm that the control requires annual management reviews of security features for physical and logical access to files and data.
- Verify that access is authorized and appropriately approved.
- Inspect security reports generated from system tools preventing network penetration vulnerability attacks.

Procedure Step: DS5.09 - Malicious Software Prevention, Detection and Correction

Determine and analyze

- whether and confirm that a malicious software prevention policy is established, documented and communicated throughout the organization.
- that automated controls have been implemented to provide virus protection and that violations are appropriately communicated.
- of key staff members whether they are aware of the malicious software prevention policy and their responsibility for ensuring compliance.
- a sample of user workstations, observe whether a virus protection tool has been installed and includes virus definition files and the last time the definitions were updated.
- whether and confirm that the protection software is centrally distributed (version and patch-level) using a centralized configuration and change management process.
- the distribution process to determine the operating effectiveness.
- whether and confirm that information on new potential threats is regularly reviewed and evaluated and, as necessary, manually updated to the virus definition files.
- the review and evaluation process to determine operating effectiveness.
- whether and confirm that incoming e-mail is filtered appropriately against unsolicited information.
- the filtering process to determine operating effectiveness, or review the automated process established for filtering purposes.

Additional Tasks:

Purpose:

Put preventive, detective and corrective measures in place (especially up-to-date security patches and virus control) across the organization to protect information systems and technology from malware (e.g., viruses, worms, spyware, spam).

Risk / Effect:

DS5.9 Value Drivers

- System security ensured by proactive malware protection
- Ensured system integrity
- Timely detection of security threats

DS5.9 Risk Drivers

- Exposure of information
- Violations of legal and regulatory requirements

- Systems and data that are prone to virus attacks
- Ineffective countermeasures

DS5.9 Practical Controls for Malicious Software Prevention, Detection and Correction

- Establish, document, communicate and enforce a malicious software prevention policy in the organization. Ensure that people in the organization are aware of the need for protection against malicious software, and their responsibilities relative to same.
- Install and activate malicious software protection tools on all processing facilities, with malicious software definition files that are updated as required (automatically or semi-automatically).
- Distribute all protection software centrally (version and patch-level) using centralized configuration and change management.
- Regularly review and evaluate information on new potential threats.
- Filter incoming traffic, such as e-mail and downloads, to protect against unsolicited information (e.g., spyware, phishing e-mails).

DS5.9 Test the Control Design for Malicious Software Prevention, Detection and Correction

- Enquire whether and confirm that a malicious software prevention policy is established, documented and communicated throughout the organization.
- Ensure that automated controls have been implemented to provide virus protection and that violations are appropriately communicated.
- Enquire of key staff members whether they are aware of the malicious software prevention policy and their responsibility for ensuring compliance.
- From a sample of user workstations, observe whether a virus protection tool has been installed and includes virus definition files and the last time the definitions were updated.
- Enquire whether and confirm that the protection software is centrally distributed (version and patch-level) using a centralized configuration and change management process.
- Review the distribution process to determine the operating effectiveness.
- Enquire whether and confirm that information on new potential threats is regularly reviewed and evaluated and, as necessary, manually updated to the virus definition files.
- Review the review and evaluation process to determine operating effectiveness.
- Enquire whether and confirm that incoming e-mail is filtered appropriately against unsolicited information.
- Review the filtering process to determine operating effectiveness, or review the automated process established for filtering purposes.

Procedure Step: DS5.10 - Network Security

Determine and analyze

• whether and confirm that a network security policy (e.g., provided services, allowed traffic, types of connections permitted) has been established and is maintained.

• whether and confirm that procedures and guidelines for administering all critical networking components (e.g., core routers, DMZ, VPN switches) are established and updated regularly by the key administration personnel, and changes to the documentation are tracked in the document history.

Additional Tasks:

Purpose:

Use security techniques and related management procedures (e.g., firewalls, security appliances, network segmentation, intrusion detection) to authorize access and control information flows from and to networks.

Risk / Effect:

DS5.10 Value Drivers

- Corporate security technology protected
- Reliable information secured
- Corporate assets protected
- Network security managed in a consistent manner

DS5.10 Risk Drivers

- Failure of firewall rules to reflect the organization's security policy
- Undetected unauthorized modifications to firewall rules
- Compromised overall security architecture
- Security breaches not detected in a timely manner

DS5.10 Practical Controls for Network Security

- Establish, maintain, communicate and enforce a network security policy (e.g., provided services, allowed traffic, types of connections permitted) that is reviewed and updated on a regular basis (at least annually).
- Establish and regularly update the standards and procedures for administering all networking components (e.g., core routers, DMZ, VPN switches, wireless).
- Properly secure network devices with special mechanisms and tools (e.g., authentication for device management, secure communications, and strong authentication mechanisms). Implement active monitoring and pattern recognition to protect devices from attack.

Configure operating systems with minimal features enabled (e.g., features that are necessary for functionality and are hardened for security applications). Remove all unnecessary services, functionalities and interfaces (e.g., graphical user interface [GUI]). Apply all relevant security patches and major updates to the system in a timely manner.

- Plan the network security architecture (e.g., DMZ architectures, internal and external network, IDS placement and wireless) to address processing and security requirements. Ensure that documentation contains information on how traffic is exchanged through systems and how the structure of the organization's internal network is hidden from the outside world.
- 6. Subject devices to reviews by experts who are independent of the implementation or maintenance of the devices.

DS5.10 Test the Control Design for Network Security

- Enquire whether and confirm that a network security policy (e.g., provided services, allowed traffic, types of connections permitted) has been established and is maintained.
- Enquire whether and confirm that procedures and guidelines for administering all critical networking components (e.g., core routers, DMZ, VPN switches) are established and updated regularly by the key administration personnel, and changes to the documentation are tracked in the document history.

Procedure Step: DS5.11 - Exchange of Sensitive Data

Determine and analyze

- whether and confirm that data transmissions outside the organization require encrypted format prior to transmission.
- whether and confirm that corporate data are classified according to exposure level and classification scheme Perimeter and Network Security Program, 7/30/2012 8:41:14 PM version 1.3 Page 16

(e.g., confidential, sensitive).

- whether and confirm that sensitive data processing is controlled through application controls that validate the transaction prior to transmission.
- that the application logs or halts processing for invalid or incomplete transactions.

Additional Tasks:

Purpose:

Exchange sensitive transaction data only over a trusted path or medium with controls to provide authenticity of content, proof of submission, proof of receipt and non-repudiation of origin.

Risk / Effect:

DS5.11 Value Drivers

- Trusted ways of communications
- Reliable information exchange
- System and data integrity safeguarded

DS5.11 Risk Drivers

- Sensitive information exposed
- Inadequate physical security measures
- Unauthorized external connections to remote sites
- Disclosure of corporate assets and sensitive information accessible for unauthorized parties

DS5.11 Practical Controls for Exchange of Sensitive Data

- Determine by using the established information classification scheme how the data should be protected when exchanged.
- Apply appropriate application controls to protect the data exchange.
- Apply appropriate infrastructure controls, based on information classification and technology in use, to protect the data exchange.

DS5.11 Test the Control Design for Exchange of Sensitive Data

- Enquire whether and confirm that data transmissions outside the organization require encrypted format prior to transmission.
- Enquire whether and confirm that corporate data are classified according to exposure level and classification scheme (e.g., confidential, sensitive).
- Enquire whether and confirm that sensitive data processing is controlled through application controls that validate the transaction prior to transmission.
- Review that the application logs or halts processing for invalid or incomplete transactions.