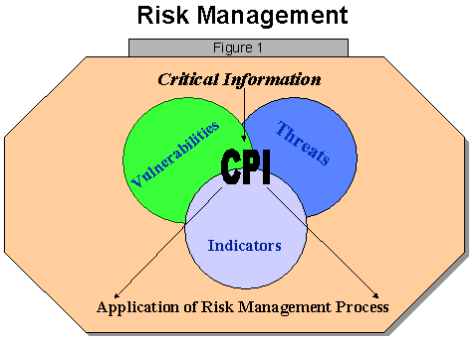
Audit Program Steps for Identity Management and Access Control

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 Critical Process Information 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)?

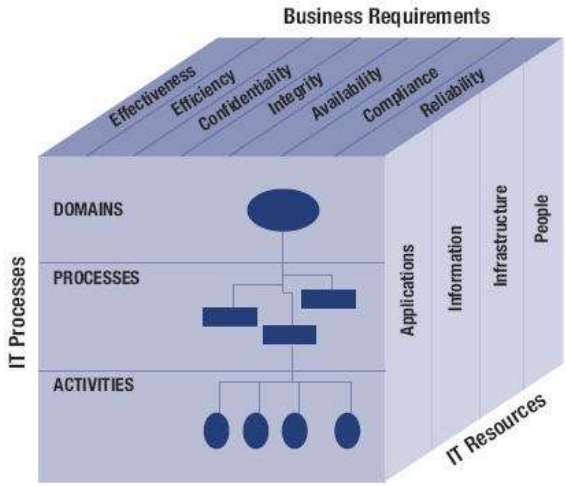


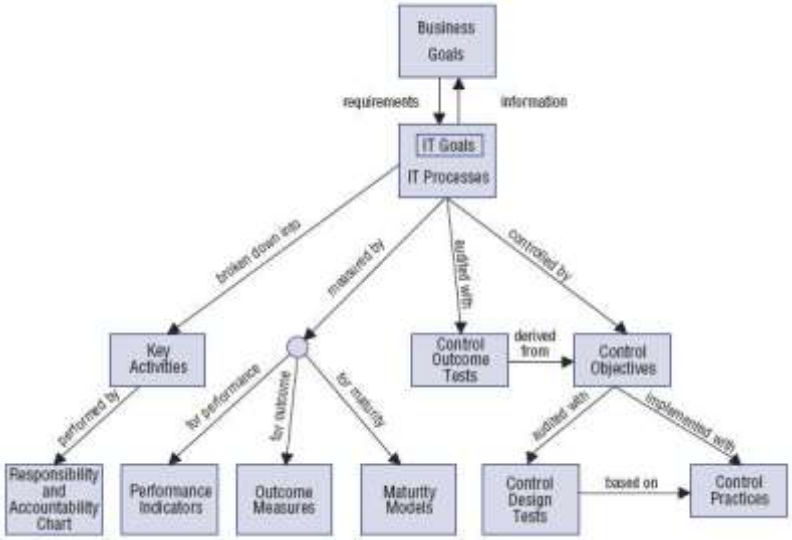
Pre-Audit considerations

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, services, and data 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 *Audited Institution or entity name* on *date of onsite audit* to validate that appropriate controls and procedures exist to mitigate the potential threat of the inappropriate access and utilization of campus information system services or data resources.

III Execution (Operational Requirements):

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. Identity Management (50%) _____ (auditor name)
      ii. Access Control (50%) _____ (auditor name)
2. Key Characteristics and Operational Environment
   a. Policy on Identification and Authentication
   b. User access management, e.g., user registration process, provisioning and privilege measurement, user password management, review of user rights
   c. User responsibilities, e.g., password use, unattended user equipment, clear desk and clear screen policy, etc.
   d. Access enforcement
   e. Segregation of duties

f. Least privilege
g. Policy on use of network services available to users
h. User authentication for external connections
    i. Secure login procedures e.g., Physical access is control so intruder cannot by-pass controls
    ii. Unsuccessful Login attempts, session locks, termination, supervision review, etc.,
    iii. System use notification notice on login
i. Operating Systems and Applications providing services
    i. Access is controlled - User identification and authentication for local and external connections
    ii. Password management system is in place and automates key processes
    iii. Limitations of connection time
    iv. Information access restrictions
    v. Sensitive systems isolated
j. HR has processes in place for:
    i. Personnel Security Policy and Procedures
    ii. Position Categorization
    iii. Personnel Screening
    iv. Personnel Termination
    v. Personnel Transfer
    vi. Third Party Personnel Security
    vii. Personnel Sanctions
    viii. Access Agreements
k. Other business owner responsibilities?
l. Key system to be evaluated are the major network support systems associated with user use or access:
    i. Banner
    ii. PeopleSoft
    iii. Other database systems
    iv. Directory services (NDS, AD, LDAP, etc.)
    v. Email
    vi. One Card system
    vii. User access to 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
m. Checklist listed for Systems evaluated?
    i. Internal Control Checklist Questionnaire for IAM.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. 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 /	**Start**	End

		Hours		

IV Command, Control, & Communication:

1. 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
    a. Key shareholders – regular situational audit updates to the audited entity
    b. 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
    c. 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 Identity Management and Access Control (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.

• 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

• Obtain from HR a sample of employee transfers and terminations and, through review of system account profiles and/or ACLs, determine if access has been appropriately altered and/or revoked in a timely manner with the following criteria (as applicable):

- Personnel Security Policy and Procedures: The organization develops, disseminates, and periodically reviews / updates;
  - A formal, documented, personnel security policy that addresses purpose, scope, roles, responsibilities, and compliance; and
  - formal, documented procedures to facilitate the implementation of the personnel security policy and associated personnel security controls
- Position Categorization: The organization assigns a risk designation to all positions and establishes screening criteria for individuals' filling those positions. The organization reviews and revises position risk designations
- Personnel Screening: The organization screens individuals requiring access to organizational information and information systems before authorizing access
- Personnel termination: When employment is terminated, the organization terminates information system access, conducts exit interviews, ensures the return of all organizational information system related property (e.g., keys, ID cards, building passes, etc.), and ensures that appropriate personnel have access to official records created by the terminated employee that are stored on organizational information systems
- Personnel Transfer: The organization reviews information systems/facilities access authorizations, when individuals are reassigned or transferred to other positions within the organization and initiates appropriate actions …
  - Reissuing keys, ID cards, and building passes
  - Closes old accounts access
  - Establishes new account access
  - Changing system access authorizations
- Access Agreements: The organization completes appropriate access agreements (e.g., non-disclosure agreements, acceptable use agreements, rules of behavior, conflict-of-interest agreements) for individuals requiring access to organizational information and information systems before authorizing access
- Third-Party Personnel Security: The organization establishes personnel security requirements for third-party providers (e.g., service bureaus, contractors, and other organizations providing information systems development, information technology services, outsourced application, network and security management) and monitors provider compliance to ensure adequate security
- Personnel Sanctions: The organization employs a formal sanctions process for personnel failing to comply with established information security policies and procedures

• 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.

• 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).

• 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.

• 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).

• Select a sample of business-critical or sensitive data, and determine if data have been secured in accordance with the organization's encryption standards.

• Verify that the cryptographic system used to protect stored data effectively renders data unreadable, and determine if any method can be utilized to access erased data through forensic techniques.

• 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.

• Confirm that sensitive information is not disclosed or exposed to unauthorized parties.

COBiT4.01 to NIST Mappings for the Areas being Assessed

DS5 Ensure Systems Security

DS5.3 ***Identity management*** states: 'Ensure that all users (internal, external and temporary) and their activity on IT systems (business application, IT environment, system operations, development and maintenance) are uniquely identifiable. Enable user identities via authentication mechanisms. Confirm that user access rights to systems and data are in line with defined and documented business needs and that job requirements are attached to user identities. Ensure that user access rights are requested by user management, approved by system owners and implemented by the security-responsible person. Maintain user identities and access rights in a central repository. Deploy cost-effective technical and procedural measures, and keep them current to establish user identification, implement authentication and enforce access rights'.

This was mapped with:

• IA-1 Identification and Authentication Policy and Procedures, which requires the organization to develop, disseminate and periodically review/update:

– A formal, documented identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, co-ordination amongst organizational entities and compliance

– Formal, documented procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls

• IA-2 User Identification and Authentication, which requires the information system to uniquely identify and authenticate users (or processes acting on behalf of users)

• IA-4 Identifier Management, which requires the organization to manage user identifiers by:

– Uniquely identifying each user

– Verifying the identity of each user

– Receiving authorization to issue a user identifier from an appropriate organization official

– Ensuring that the user identifier is issued to the intended party

– Disabling the user identifier after the organization-defined time period of inactivity

– Archiving user identifiers Centralization of user identities and access rights (mentioned in the CobiT control objectives) is not required by NIST guidance, but is usually implemented as a matter of efficiency. In addition, US Homeland Security Presidential Directive/HSPD-12, *Policy for a Common Identification Standard for Federal Employees and Contractors*, mandates that all US federal agencies use a government wide standard form of identification for the federal government's employees and contractors. This policy is intended to enhance security, increase government efficiency, reduce identity fraud and protect personal privacy. It requires the use of this identification for gaining physical access to federally controlled facilities and logical access to federally controlled information systems.

DS5.4 ***User account management*** states: 'Address requesting, establishing, issuing, suspending, modifying and closing user accounts and related user privileges with a set of user account management procedures. Include an approval procedure outlining the data or system owner granting the access privileges. These procedures should apply for all users, including administrators (privileged users) and internal and external users, for normal and emergency cases. Rights and obligations relative to access to enterprise systems and information should be contractually arranged for all types of users. Perform regular management review of all accounts and related privileges'.

This was mapped with:

• AC-2 Account Management, which requires the organization to manage information systems accounts, including establishing, activating, modifying, reviewing, disabling and removing accounts. The organization reviews information systems accounts based on the organization-defined frequency, at least annually.

• IA-4 Identifier Management, which requires the organization to manage user identifiers by:
– Uniquely identifying each user
– Verifying the identity of each user
– Receiving authorization to issue a user identifier from an appropriate organization official
– Ensuring that the user identifier is issued to the intended party
– Disabling user identifier after the organization-defined time period of inactivity
– Archiving user identifiers

• PS-6 Access Agreements, which requires the organization to complete appropriate access agreements for individuals requiring access to organizational information and information systems, before authorizing access, and review/update the agreements

DS5.5 ***Security testing, surveillance and monitoring*** states: 'Test and monitor the IT security implementation in a proactive way. IT security should be reaccredited in a timely manner to ensure that the approved enterprise's information security baseline is maintained. A logging and monitoring function will enable the early prevention and/or detection and subsequent timely reporting of unusual and/or abnormal activities that may need to be addressed'.

This was mapped with:
• AU-6 Audit Monitoring, Analysis, and Reporting, which requires the organization to regularly review/analyze information system audit records for indications of inappropriate or unusual activity, investigate suspicious activity or suspected violations, report findings to appropriate officials, and take necessary actions.

• CA-2 Security Assessments, which requires the organization to conduct an assessment of the security controls in the information system based on the organization-defined frequency, at least annually, to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting the security requirements for the system.

• CA-6 Security Accreditation, which requires the organization to authorize (i.e., accredit) the information system for processing before operations and update the authorization based on the organization-defined frequency, at least every three years or when there is a significant change to the system. A senior organizational official signs and approves the security accreditation.

• CA-7 Continuous Monitoring, which requires the organization to monitor the security controls in the information system on an ongoing basis.

• CM-4 Monitoring Configuration Changes, which requires the organization to monitor changes to the information system, conducting security impact analyses to determine the effects of the changes.

• RA-5 Vulnerability Scanning, which requires the organization to scan for vulnerabilities in the information system based on the organization-defined frequency or when significant new vulnerabilities potentially affecting the system are identified and reported. This is also part of the FIPS 199 risk calculation.

• SI-4 Information System Monitoring Tools and Techniques, 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.

COBiT 4.01 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. 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: DS5.03 - Identity Management

Determine and analyze

• if security practices require users and system processes to be uniquely identifiable and systems to be configured to enforce authentication before access is granted.
• if predetermined and preapproved roles are utilized to grant access, then determine if the roles clearly delineate responsibilities based on least privileges and ensure that the establishment and modification of roles are approved by process owner management.
• if access provisioning and authentication control mechanisms are utilized for controlling logical access across all users, system processes and IT resources, for in-house and remotely managed users, processes and systems.

Additional Tasks:

Purpose:

Ensure that all users (internal, external and temporary) and their activity on IT systems (business application, IT environment, system operations, development and maintenance) are uniquely identifiable. Enable user identities via authentication mechanisms. Confirm that user access rights to systems and data are in line with defined and documented business needs and that job requirements are attached to user identities. Ensure that user access rights are requested by user management, approved by system owners and implemented by the security-responsible person. Maintain user identities and access rights in a central repository. Deploy cost-effective technical and procedural measures, and keep them current to establish user identification, implement authentication and enforce access rights.

Risk / Effect:

DS5.3 Value Drivers

• Effective implementation of changes
• Proper investigation of improper access activity
• Secure communication ensuring approved business transactions

DS5.3 Risk Drivers

• Unauthorized changes to hardware and software
• Access management failing business requirements and compromising the security of business-critical systems
• Unspecified security requirements for all systems
• Segregation-of-duty violations
• Compromised system information

DS5.3 **Practical Controls** for Identity Management

- Establish and communicate policies and procedures to uniquely identify, authenticate and authorize access mechanisms and access rights for all users on a need-to-know/need-to-have basis, based on predetermined and preapproved roles. Clearly state accountability of any user for any action on any of the systems and/or applications involved.
- Ensure that roles and access authorization criteria for assigning user access rights take into account:
    - Sensitivity of information and applications involved (data classification)
    - Policies for information protection and dissemination (legal, regulatory, internal policies and contractual requirements)
    - Roles and responsibilities as defined within the enterprise
    - The need-to-have access rights associated with the function
    - Standard but individual user access profiles for common job roles in the organization
    - Requirements to guarantee appropriate segregation of duties
- Establish a method for authenticating and authorizing users to establish responsibility and enforce access rights in line with sensitivity of information and functional application requirements and infrastructure components, and in compliance with applicable laws, regulations, internal policies and contractual agreements.

- Define and implement a procedure for identifying new users and recording, approving and maintaining access rights. This needs to be requested by user management, approved by the system owner and implemented by the responsible security person.
- Ensure that a timely information flow is in place that reports changes in jobs (i.e., people in, people out, people change). Grant, revoke and adapt user access rights in co-ordination with human resources and user departments for users who are new, who have left the organization, or who have changed roles or jobs.

DS5.3 **Test for the Controls** for Identity Management

- Determine if security practices require users and system processes to be uniquely identifiable and systems to be configured to enforce authentication before access is granted.
- If predetermined and preapproved roles are utilized to grant access, determine if the roles clearly delineate responsibilities based on least privileges and ensure that the establishment and modification of roles are approved by process owner management.
- Determine if access provisioning and authentication control mechanisms are utilized for controlling logical access across all users, system processes and IT resources, for in-house and remotely managed users, processes and systems.

Procedure Step: DS5.04 - User Account Management

Determine and analyze

• if procedures exist to periodically assess and recertify system and application access and authorities.
• if access control procedures exist to control and manage system and application rights and privileges according to the organization's security policies and compliance and regulatory requirements.
• if systems, applications and data have been classified by levels of importance and risk, and if process owners have been identified and assigned.
• if user provisioning policies, standards and procedures extend to all system users and processes, including vendors, service providers and business partners.

Additional Tasks:

Purpose:

Address requesting, establishing, issuing, suspending, modifying and closing user accounts and related user privileges with a set of user account management procedures. Include an approval procedure outlining the data or system owner granting the access privileges. These procedures should apply for all users, including administrators (privileged users) and internal and external users, for normal and emergency cases. Rights and obligations relative to access to enterprise systems and information should be contractually arranged for all types of users. Perform regular management review of all accounts and related privileges.

Risk / Effect:

DS5.4 Value Drivers

• Consistently managed and administered user accounts
• Rules and regulations for all kinds of users
• Timely discovery of security incidents
• Protection of IT systems and confidential data from unauthorized users

DS5.4 Risk Drivers

• Security breaches
• Users failing to comply with security policy
• Incidents not solved in a timely manner
• Failure to terminate unused accounts in a timely manner, thus impacting corporate security

DS5.4 **Practical Controls** for User Account Management

- Ensure that access control procedures include but are not limited to:
    - Using unique user IDs to enable users to be linked to and held accountable for their actions

- Awareness that the use of group IDs results in the loss of individual accountability and are permitted only when justified for business or operational reasons and compensated by mitigating controls. Group IDs must be approved and documented
- Checking that the user has authorization from the system owner for the use of the information system or service, and the level of access granted is appropriate to the business purpose and consistent with the organizational security policy
- A procedure to require users to understand and acknowledge their access rights and the conditions of such access
- Ensuring that internal and external service providers do not provide access until authorization procedures have been completed
- Maintaining a formal record, including access levels, of all persons registered to use the service
- A timely and regular review of user IDs and access rights

- Ensure that management reviews or reallocates user access rights at regular intervals using a formal process. User access rights should be reviewed or reallocated after any job changes, such as transfer, promotion, demotion or termination of employment. Authorizations for special privileged access rights should be reviewed independently at more frequent intervals.

DS5.4 **Test for the Controls** for User Account Management

- Determine if procedures exist to periodically assess and recertify system and application access and authorities.
- Determine if access control procedures exist to control and manage system and application rights and privileges according to the organization's security policies and compliance and regulatory requirements.
- Determine if systems, applications and data have been classified by levels of importance and risk, and if process owners have been identified and assigned.
- Determine if user provisioning policies, standards and procedures extend to all system users and processes, including vendors, service providers and business partners.

Procedure Step: DS5.05 - Security Testing, Surveillance and Monitoring

Determine and analyze

• whether and confirm that an inventory of all network devices, services and applications exists and that each component has been assigned a security risk rating.
• if security baselines exist for all IT utilized by the organization.
• if all organization-critical, higher-risk network assets are routinely monitored for security events.
• if the IT security management function has been integrated within the organization's project management initiatives to ensure that security is considered in development, design and testing requirements, to minimize the risk of new or existing systems introducing security vulnerabilities.

Additional Tasks:

Purpose:

Test and monitor the IT security implementation in a proactive way. IT security should be reaccredited in a timely manner to ensure that the approved enterprise's information security baseline is maintained. A logging and monitoring function will enable the early prevention and/or detection and subsequent timely reporting of unusual and/or abnormal activities that may need to be addressed.

Risk / Effect:

DS5.5 Value Drivers

• Staff experienced in security testing and monitoring of IT systems
• Regularly reviewed security level
• Deviations from business requirements highlighted
• Security breaches detected proactively

DS5.5 Risk Drivers

- Misuse of users' accounts, compromising organizational security
- Undetected security breaches
- Unreliable security logs

DS5.5 **Practical Controls** for Security Testing, Surveillance and Monitoring

- Implement monitoring, testing, reviews and other controls to:
  - Promptly prevent/detect errors in the results of processing
  - Promptly identify attempted, successful and unsuccessful security breaches and incidents
  - Detect security events and thereby prevent security incidents by using detection and prevention technologies
  - Determine whether the actions taken to resolve a breach of security are effective
- Conduct effective and efficient security testing procedures at regular intervals to:
  - Verify that identity management procedures are effective
  - Verify that user account management is effective
  - Validate that security-relevant system parameter settings are defined correctly and are in compliance with the information security baseline
  - Validate that network security controls/settings are configured properly and are in compliance with the information security baseline
  - Validate that security monitoring procedures are working properly
- Consider, where necessary, obtaining expert reviews of the security perimeter

DS5.5 **Test for the Controls** for Security Testing, Surveillance and Monitoring

- Enquire whether and confirm that an inventory of all network devices, services and applications exists and that each component has been assigned a security risk rating.
- Determine if security baselines exist for all IT utilized by the organization.
- Determine if all organization-critical, higher-risk network assets are routinely monitored for security events.
- Determine if the IT security management function has been integrated within the organization's project management initiatives to ensure that security is considered in development, design and testing requirements, to minimize the risk of new or existing systems introducing security vulnerabilities.