Building the Next Generation Enterprises

PISA

(Planning, Integration, Security and Administration)

An Intelligent Decision Support Environment for IT Managers and Planners

Sample Security Audit Checklist Generated

Note

This is a sample report that has been generated by the PISA environment for a small company. PISA generates many documents as a result of short (15 to 20 minutes) interviews. These documents are produced as html documents that can be easily modified by using MS Word (just open these documents in MS Word and edit them). For display only purposes, this document has been converted to PDF Format.

NGE Solutions, Inc. (www.ngesolutions.com)

AUDIT AND CONTROL CHECKLIST

A comprehensive checklist is essential for information security audits and controls. The following links show you various checklists that you can use to monitor, audit and control the technical as well as management aspects of your security:

The checklist is extracted from the book ("Information Security and Auditing in the Digital Age", A. Umar, NGE Solutions, 2004). It can be customized and expanded/reduced to take into account the following factors: type of company, size of company, specialized situations such as international trade. The checklist is written so that it can be filled out by an auditor. For each item, the answer may be yes, no, or some explanation (e.g., not needed, covered by another category, etc). After reviewing this checklist as part of an audit, the auditor would prepare a risk assessment report to highlight the main risk and suggest future steps.

Color coding

The segments in Customized Checklist are color coded to represent the following:

- If the segment is ***"Black"***, no change needed to this segment
- If the segment is ***"Blue"***, you can reduce this segment or even remove it according to your requirement
- If the segment is ***"Red"***, you may need to expand this segment according to your requirements

1.1. Organizational Controls and Security Administration

These controls are intended for the entire firm and address the organizational structures, policies and procedures.Â

1.1.1. Documentation of the Information Systems Strategic Plan

- Management has developed and implemented long and short term plans that identify and fulfill the organizations strategies _____
- Information systems security is adequately addressed in the organizations long- and short-term plansÂ _____
- The management of the information systems security was established and applied using a structured approach _____Â

1.1.2. Information Security Policies and Procedures

- Information security policies exist _____

- These policies are adequate to address Privacy, Integrity, Authorization, Authentication, and Availability (PIA4) in the following areas (circle the ones that are NOT adequately covered by the policies):
    - Web pages
    - Firewalls
    - Employee Surveillance
    - Electronic Banking
    - Viruses
    - Encryption
    - Digital Signatures/Certificates
    - Contingency Planning
    - Laptops/Portable
    - Logging Controls
    - Internet/Intranet
    - Privacy
    - Emergency Response
    - Micro-computers
    - LAN
    - Passwords
    - E-mail
    - Data Classification
    - Telecommuting
    - User Training
    - Ethics
- Procedures and practices are used by the ISSO to monitor compliance with the above policiesÂ Â _____Â Â
- Ensure the ISSO has been given the positional authority to address policy violations, or reports to an appropriate level of managementÂ Â _____
- Documented actions taken to address recent policy violations _____Â Â

1.1.3. Risk Assessment/Ongoing Analysis

- A framework exists to assess information security risks _____

- A methodology adopted for risk assessmentÂ _____
- Responsibility assigned for periodically performing risk analysis _____
- Risk assessment methodology adequately defines essential elements of risk, provides a qualitative/quantitative measurement of risk, and addresses acceptable risk conclusions _____
- Risk assessment is appropriately reported to senior managementÂ _____
- Action plan allows for the acceptance of the residual risks (risks that cannot be controlled) by the management _____
- Adequate insurance coverage for the residual risks has been obtainedÂ _____Â

1.1.4. Information Security Organizational (ISSO) Structure

- The reporting structure and placement of the ISSO function within the organization is defined _____
- The position is responsible to the appropriate level of management and is appropriately separated from the IS department _____
- Management has defined and implemented security levels related to the sensitivity of specific corporate informationÂ _____Â Â

1.1.5. Information Security Staffing

- Position descriptions exist for the information security position _____Â
- Position descriptions consistent with the ISSO responsibilitiesÂ _____
- Staffing levels adequate in the information security environment _____

1.1.6. Compliance Requirements

- External compliance considerations (e.g., government regulations) documented (crucial for healthcare and government agencies) _____Â
- Impact of external relationships (e.g., partnerships) on compliance requirements, has been assessed _____ Â
- Appropriate and timely corrective actions have been taken for information security deficiencies in compliance examinations, regulatory reviews, and/or audits conducted so farÂ _____

1.2. Physical and Environmental Security

1.2.1. Secure Area

Objective is to prevent unauthorized access, damage and interference to business premises and information.

- Security Perimeters have been established to protect physical and IT assets (i.e., buildings with doors) __________Â

- Protected entry controls, such as the following,Â have been established to ensure that only authorized personnel are allowed access _______________

  - Badges
  - Limited access to buildings
  - Guards on entrance doors
  - Properly secured and tamper proof wiring
  - Alarm doorsÂ

- Suitable intruder detection systems are installed for this area __________Â Â

- Additional controls established for personnel or third parties (i.e., aware of activities in a secure area on a needs to know basis only) ________________ Â Â Â Â Â Â Â Â Â Â Â Â Â Â Â Â Â Â Â Â Â Â Â Â Â Â Â

- Controls are in place for the delivery and loading areas __________

- Access from outside is restricted to formally authorized and identifiedÂ personnel onlyÂ _______

- External door is secured when the internal door is opened ______________Â

- Packages checked for potential hazards before it is moved from the holding area to the point of use ___________

1.2.2. Equipment Security

Objective is to prevent loss, damage or compromise of assets and interruption to business activities.

- Equipment is sited to reduce minimum unnecessary access into work areas _______

- Controls are in place to minimize the risk of theft, fire, explosions, smoke, water, dust, vibration, chemical effects, electrical supply interference and electromagnetic radiation _________

- A policy exists towards drinking, eating and smoking in proximity to information processing facilities _________Â Â Â Â Â Â Â Â Â Â Â Â Â Â Â Â Â Â

- Suitable electrical supplies are available should there be a power failure (i.e backup generator, UPS etc) ____________________ Â Â Â Â Â Â Â

- Controls exist to ensure that power and telecommunications cabling is protected from interception or damageÂ Â ___________

- Equipment maintenance is done periodically ______________

- Only authorized maintenance personnel carry out repairs and serviceÂ _______

- Records kept of all suspected or actual faults _______________
- Adequate insurance in place to protect equipment taken off -site _______________Â
- Controls on authorized equipment exist for off site ___________Â Â
- Sensitive information securely destroyed from retired equipment ______
- Name of the contractors recordedÂ who get the retired equipment ________
- Fixed hard disks checked to ensure that sensitive data and licensed software have been removed or overwritten prior to disposal _________

1.2.3. General Controls

Objective is to prevent compromise or theft of information and information processing facilities.

- A Clear (or Secure) Desk Policy or a Clean screen policy exists ________
- Other measures to reduce the risk of unauthorized access, loss/damage to information during and outside normal working hours __________Â Â Â Â Â Â
- Procedures in place to prevent unauthorized removal of propertyÂ _________
- Spot checks in place ______

1.3. Operation Management

1.3.1. Production procedures and responsibilities

Objective is to ensure the correct and secure operations of information processing facilities.

1.3.1.1. Operating Procedures.

- Documented procedures exist that include instructions for each job _______.
- Procedures include the following:
  - Processing and handling of informationÂ _________
  - Scheduling requirementsÂ ____________
  - Instructions for handling errors or other exceptional conditions ______________
  - Support contactsÂ ________________
  - Special output handling instructions ___________
  - System restarts and recovery procedures.Â Â ________________
  - Close down proceduresÂ ________________

- Back-up proceduresÂ _____
- Computer room safety proceduresÂ _____ Â

1.3.1.2. Production Change Control

Production programs should be subject to strict change control.Â The following items should be considered:

- An audit log containing all relevant information is retainedÂ _____
- Identification and recording of significant changesÂ _____
- Assessment of the potential impact of such changes _____
- Formal approval procedure for proposed changesÂ Â Â _____
- Communication of change details to relevant persons _____
- Identification of responsibilities for aborting and recovering from unsuccessful changesÂ _____ Â

1.3.1.3. Incident Management Procedures

a) Procedures for security incident includingÂ Â

- Procedures for information system failures and loss of serviceÂ _____
- Denial of serviceÂ _____
- Errors resulting from incomplete or inaccurate business data.Â Â _____
- Breaches of confidentiality _____

b) Actions to recover from security breaches and correct system failures that state:Â :

- Only authorized staff are allowed access to live system and data. _____
- All emergency actions are documented in detailÂ _____
- Emergency action is reported to managementÂ _____
- Integrity of business systems and controls is confirmed with minimal delay. _____

1.3.1.4. Segregation of Duties

- Identification of activities which could be basis of fraudÂ and/or crime
- To avoid collusion, duties have been segregated to ensure that 2 or more persons are involvedÂ

1.3.1.5. Separation of Development and Production Facilities.

- Separate facilities for development and productionÂ softwareÂ _____.Â
- Different logon procedures for test and production systems to reduce risk of error and production problemsÂ Â _____Â

1.3.2. System Planning and Acceptance

Â Objective is to minimize the risk of systems failure.

1.3.2.1. Capacity Planning

- A capacity plan exists _____
- Critical components are included in the capacity planÂ _____

1.3.2.2. System Acceptance

- Acceptance criteria for new information systems, upgrades and new versions has been establishedÂ _____
- Tests of the systems specified prior to acceptance _____.Â
- For major new development, the operations function and users consulted at all stages in the developmentÂ _____
- Requirements and criteria for acceptance include the following:
    - Performance and computer capacity requirements _____
    - Error recovery and restart procedures and contingency plansÂ Â _____
    - Testing of operating procedures to defined standardsÂ _____Â
    - Agreed set of security controls for new systems _____
    - Effective manual procedures in case of automation failureÂ Â
    - Business continuity arrangements for new systems
    - Testing to show that the new system will not adversely effect existing systems particularly at peak processing times _____Â
    - Testing of the new system to understand security implications _____Â

1.3.3. Protection Against Malicious Software

Objective is to protect the integrity of software and information

Controls against malicious software should include: Â Â

- Policy prohibiting the use of unauthorized softwareÂ _____

- Policy to protect against obtaining files and software from untrusted sourcesÂ _____.
- Installation and regular update of anti-virus detection and repair of softwareÂ _____
- Regular reviews of the software and data content of systems supporting critical business processes _____
- Procedures for checking files or programs for viruses before useÂ _____Â
- Checking electronic mail attachments and downloads for malicious software before useÂ _____Â Â
- Procedures for virus protection on systems, training in their use, reporting and recovering from virus attacksÂ _____Â
- Business continuity plans for recovering from virus attacksÂ _____
- Procedures to verify all information relating to malicious software before issuing warning bulletins _____Â Â Â Â Â Â Â Â Â

1.3.4. Housekeeping (Traditional, Mainframe Systems)

Objective is to maintain integrity and availability of information processing and communication services.Â Â Â Â

1.3.4.1. Information Back-up

- Back-up arrangement documented in restoration procedures _____
- Back-up information stored in a remote locationÂ _____Â
- At least 3 generation or cycles of back-up information is retained for important business applications _____
- Back-up/restore procedures tested to ensure that they will work in emergency situationsÂ _____Â Â

1.3.4.2. Operator Logs

- Operation logs of the system activities exist _____
- Logs contain critical data (e.g., start finish times, system errors and corrective action taken, name of the person making the log entry) _____Â Â Â Â
- Logs are subject to regular, independent checks against operating procedures _____Â Â

1.3.4.3. Fault Logging

- Fault logs show that all have been satisfactorily resolved _____
- Corrective measures exist to ensure that controls have not been compromisedÂ by personnel _____
- Actions taken to handle faults are fully authorizedÂ _____Â

1.3.5. Media Handling and Security

Objective is to prevent damage to assets and interruptions to business activities. Media should be controlled and physically protected. Â Â Â Â Â Â Â Â Â
Â Â Â Â Â Â Â Â Â Â Â Â Â Â

1.3.5.1. Management of Removable Computer Media

Objective is to protect removable media such as tapes, disks, cassettes and printed reports.

- Contents of any re-usable media with highly sensitive information that are to be removed from the organization areÂ erasedÂ _______________Â
- Authorization is requiredÂ and an audit trail is kept of all highly sensitive removable media ______________Â
- Sensitive media stored in a safe, secureÂ __________________________
- Procedures for disposal of sensitive mediaÂ _______________________ Â

1.3.5.2. Information Handling Procedures

- Procedures in place for handling and storing of sensitive information
- Controls in place for:
    - Handling and labeling of all mediaÂ _________
    - Access restrictions to identify unauthorized personnel _____________
    - Maintenance of a formal record of the authorized recipients of data __________Â Â
    - Ensuring that input, processing, and output is validated and verified for sensitive applications _____________Â
    - Protection of spooled data is at a level consistent with sensitivity _____________Â
    - Storage of media in secure areas ____________Â Â Â
    - Keeping the distribution of data to a minimumÂ ________________
    - Review of distribution lists and lists of authorized recipients at regular intervals.

1.3.5.3. Security of System Documentation

- Systems documentation stored securely ___________________
- The access list for systems documentation kept to a minimumÂ Â ________________
- System documentation not held on a public or unsecure networkÂ ______________

1.4. Enterprise Level Access Controls

1.4.1. Business Requirement for Access Control

Objective is to control access to Information

The access control policy should state:Â

- Security requirements for each application _____
- Standard user profiles for common categories of jobÂ _____
- Management access rights in a network environmentÂ _____Â

1.4.2. User Access Management

Objective is to prevent unauthorized access to information systems.

1.4.2.1. Access Set-up/Removal/Review

- Procedures and standards exist to grant access to new hires, department transfers, vendors, and consultants _____Â Â
- Procedures and standards to remove access from terminated employees, transferred employees, and discontinued vendorsÂ _____ Â Â Â Â Â
- The access lists are reviewed for the sensitive systemsÂ _____Â Â
- Someone has the "ownership" of the user access reviewsÂ _____

1.4.2.2. User Registration

- A formal procedure exists for granting access to all information systems and servicesÂ Â
- UseÂ of unique user ID so they are responsible for actions _____
- Separate approval for access rights from management _____
- Checking that the access given is appropriate for the business purpose giving users a written statement of their access rights _____
- Requiring users to sign the statement so they understand the conditions of their access _____
- Maintaining a register of all persons registered to use the service _____Â
- Periodically checking for removing redundant User Id's from access _____Â
- Ensuring that redundant user IDs are not issued to other users _____

1.4.2.3. Privilege Management

- Controls in place to disallow un-authorized users to override system or application controlsÂ Â _____

- A formal management process in place re the allocation of passwords _____
- Review of user access rights done reviewed on a regular basis ieÂ every 6 months _____

1.4.3. User Responsibilities

Objective is to prevent unauthorized user access.

- Users advised of the security practices to be followed re Passwords (i.e., keep confidential, avoid keeping a paper record, do not share passwords) _____
- Users advised to ensure that unattended equipment has appropriate protection:
    - Terminate active sessions when finishedÂ Â Â Â Â _____Â
    - Logoff mainframe systems when session finishedÂ Â Â _____Â
    - Secure PC's or terminals by a key lock or password access when not in use _____

1.5. System Development and Maintenance

1.5.1. Security Requirements of System

- Organization requires that security is built into the information system _____Â Â Â Â
- Security requirements analyzed and specified at the design state ofÂ new system or enhancement to existing system _____

1.5.2. Cryptographic Controls

Objective to protect the confidentiality, authenticity or integrity of information.

- Policy exists on the use of cryptographic controls (i.e., encryption) for the protection of sensitive information _____
- Digital signatures are used for authentication where needed _____
- Asymmetric encryption used where appropriate _____
- Non-repudiation services used where needed to resolve disputes involving the use of a digital signature on an electronic contract or payment _____
- Proper key management system such as PKI usedÂ Â Â _____

1.5.3. Security of System Files

Objective is to ensure that IT projects and support activities are conducted in a secure manner.

1.5.3.1. Controlof Production software

- Updating of operational program libraries is only performed by the nominated librarianÂ _____
- Operational systems only hold executable code (source code not included for security purposes)Â Â _____
- Executable code is not implemented on operational system without evidence of successful testingÂ _____Â
- An audit log is maintained of all updates to operational program libraries _____
- Previous versions of software is retained as a contingency measure _____
- Vendor supplied software is maintained at the level supported by the supplier _____

1.5.3.2. Protection of System Test Data

The following are put in place to protect production data when used for testing:Â

- The access control procedures, which apply to production application systems, also apply to test application systems _____
- Separate authorization needed each time production information is copied to a test application system _____
- Production information is erased after testing is completedÂ _____Â
- Copying and use of production information is logged for audit trails _____

1.5.3.3. Access Controls to Program Source Library

The following controls are in place to protect potential corruption of computer programs in the source library:

- Program source libraries are not held on the operational systems _____Â
- A program librarian has been be assigned for all sensitive applications _____Â Â
- IT support staff does not have unrestricted access to program source libraries _____
- Programs under development or maintenance are not held in production program source libraries _____
- Updating of program source libraries and issuing of program sources to programmers is only performed by the authorized librarian _____Â
- Program listings are held in a secure environmentÂ _____Â Â

1.5.4. Security in Development and Support Processes

Objective is to maintain the security of application system software and information.

- Change control procedures are in place to ensure security and control procedures are not compromised _____Â Â Â Â Â Â Â Â Â Â Â

- Periodic technical reviews are completed of all operating changesÂ _____Â Â Â Â Â

- Restrictions exist on changes to vendor software packages (e.g., vendor consent before changes, someone who will maintain future maintenance) _____Â Â Â Â Â Â Â Â Â Â Â Â Â Â Â

- Protection in place for backdoors and Trojan codeÂ through careful buying practices (i.e., buying programs from reputable vendors) and inspections of source code before production useÂ _____Â Â

1.6. Business Continuity Management

Objective of business continuity management is to counteract interruptions to business activities and to protect critical business processes from the effects of major failure or disaster.

- A business continuity plan is in place to cover your business _____

- Redundancy and fault tolerance has been built into the systems to minimize the impact of attacksÂ Â Â _____

- The continuity plan contains the following:

    - Identification of attacks (natural, malicious)_____

    - Key personnel responsible for responding to attacks _____

    - System to notify the key personnelÂ _____

    - Offsite location for system backups _____

    - Offsite location for system operation _____

    - Physical arrangements (personnel moved to off-sites, hotel accommodations in the target areas, etc) _____

    - Other considerations (specify) _____

- The plan is reviewed periodically _____

- Plan tested and exercised periodically _____

- Key personnel familiar with the plan and any changes _____

1.7. Compliance

1.7.1. Compliance with Legal Requirements

Objective is to avoid breaches of any criminal and civil law, statutory, regulatory or contractual.

- Intellectual property rights, copyrights, and trademarks are complied with through proceduresÂ _____
- Proprietary software is registered under license agreements that limits the use of the products to specified machinesÂ _____
- Safeguarding of organizational records is in place to ensure their use within regulatory retention periods _____
- Cryptographic keys associated with encrypted archives or digital signatures are kept securelyÂ _____
- Data protection and Privacy Laws are adhered toÂ _____
- A data protection officer has been assignedÂ _____
- Cryptographic controls have been implemented which include:Â Â
    - Import and/or export of computer hardware and software for performing cryptographic functions _____
    - Import and/or export of computer hardware and software which is designed to have cryptographic functions added to it _____
    - Mandatory and discretionary methods of access by the countries to information encrypted by hardware or software to provide confidentiality of contentÂ _____

1.8. Application Controls

Application controls concentrate on individual (usually sensitive and critical) applications and encompass the whole sequence of application processing.

1.8.1. Application Access Controls

Objective is to prevent un-authorized access to information held in application systems.

- Access controls are in place to ensure users are restricted to Read, Write, Execute, Delete based on the organizational information access policyÂ _____
- Organization has a dedicated (isolated) computing environment for hihly sensitive systems _____

1.8.2. Exchanges of Information and Software

Objective is to prevent loss, modification or misuse of information exchanged between organizations.

- Information and software exchange agreements verified before exchange of critical information and software between organizationsÂ _____
- E-commerce security in place to protect from threats such as fraudulent activity, contract dispute, and disclosure or modification of information _____

- Security of sensitive electronic mail is enforced through packages such as PGP, MIME, or others _____
- Security of electronic office systems (e.g., word documents) is enforced through guidelines, policies, and technologiesÂ _____
- Publicly available systems are protectedÂ through policies and technologies _____
- Security of media in transitÂ is enforced through:
    - Reliable transport/courier company used _____
    - Packaging to protect the contents from physical damageÂ _____
    - Special controls to protect sensitive information (i.e., use of locked containers, delivery by hand, tamper evidence packaging, splitting of the consignment to take different routes, use of digital signature and confidential encryption) _____

1.8.3. Input, Output and Processing Controls in Application Systems

Objective is to prevent loss, modification or misuse of user data in application systems.

- Data validation (input edit) is in place to ensure that data input is correct and appropriate before processing _____
- Validation checks are incorporated into systems to detect corruption by processing errors or through deliberate acts _____
- Authorization controls are in place to verify the authority of input providers _____
- Data conversion controls are in place to minimize conversion errors as data is transcribed from one form to another _____
- Checks and controls are in place to reconcile data file balances after transaction updates and software download/upload _____
- Application processing controls are in place to include the following:
    - Matching controls that compare the input data with information held on system files. _____
    - Processing edits to verify for reasonableness or consistency during processing of applications_____Â
    - Control totals during processing to reconcile the input control totals with the totals of items processed _____
- Data produced by an application system is validated to ensure the processing of stored information is correct. This validation may include:
    - Checks to test whether the output data is reasonableÂ _____
    - Reconciliation control counts to ensure processing of all dataÂ _____

- Providing sufficient information for a reader or subsequent processing system to determine the accuracy and completeness of the information _____
- Procedures for responding to output validationÂ testsÂ _____
- Identifying the personnel involved in the data output process _____

- Periodic synching and checking of outputs is done with actuals _____
- Message authentication is implemented in hardware or software for sensitive message exchanges _____
- Message authentication is required where neededÂ _____

1.8.4. Controls for XML-based Applications

This is a new area of work in which the XML document itself but also the DTD are also properly controlled.

- Sensitive XML documents are encryptedÂ by using XML Encryption, XML Signatures or other suitable schemesÂ _____
- DTDs of sensitive XML documents are properly controlled so that only authorized personnel can update them _____

1.8.5. Application and Shared Data Security Controls

- Additional sets of passwords and security restrictions are in place for sensitive applications _____
- Additional sets of passwords and security restrictions are in place for sensitive applications _____
- Security profiles have been created to allow different people different access (e.g., online users, medical record processing, etc) _____:
- These profiles are established and maintained by a data security system _____.

1.8.6. Controls on Mobile and Web Services Applications

The objective is to properly control the mobile client, Web tier, and the back-end transaction control issues for mobile applications.Â

- Mobile clients are authenticated before they can invoke applicationsÂ _____
- Security checks are done at the wireless gateway (e.g., WAP Gateway) _____
- Transactions have proper controls for remote invocationsÂ _____
- Proper controls for Web Services applications are in place:
  - Services defined with WSDL have been properly checked _____
  - Services advertised through UDDI are properly checked _____

1.9. Network Security Controls

Objective is to ensure the safeguarding of information in networks and the prevention of the supporting infrastructure.

1.9.1. Network Access Controls

Objective is protection of networked services:

- There is a security policy concerning the network and network services in the enterpriseÂ _____
- Policy indicates the network and network services allowed to be accessed,Â authorization procedures for determining who is allowed access to which networks and networked services _____
- Only restricted paths (e.g., dedicated and/orÂ encrypted lines, security firewalls, limited menu and submenu options for users)Â allowed to sensitive databases and programs _____
- User authentication for remote users for external connections _____
- Segregation of networks (separate logical network domains, firewalls)Â is in place _____
- Network connection controls exist for electronic mail, file transfers, interactive access, etc. _____
- Network routing controls exist for isolating networks and preventing routes to propagate from the network of one organization into the network of another _____
- Public Internet access used to access corporate resourcesÂ _____
- VPN used for external network accessÂ _____
- A warning message is initiated for users accessing the proprietary network.Â The wordings may be "You have connected to a proprietary system. Only authorized users may access this system. Access by unauthorizedÂ individuals is prohibited and will be prosecuted to the full extent of the law. This system is monitored for unauthorized usage."Â _____

1.9.2. Network FirewallsÂ and Controls

- A firewall policy is in place _____
- Firewall does the following type of filtering:
    - Packet filtering _____
    - Application filtering_____
    - File transfer filtering _____
    - Other filters (specify) _____

- Firewall rules are kept in a secure area and can only be modified by authorized personnel _____

- Responsibility for network firewall security is separated from computer operations where appropriate _____Â

- Responsibilities and procedures for the management of remote equipment has been established _____Â Â Â

- Special controls have been established for confidentiality and integrity of data passing over public networksÂ _____Â

1.9.3. Remote Access Service (RAS) Controls

- Remote Access Services (RAS) is installed on the server being reviewedÂ _____Â

- Remote access authorization is granted based on corporate standardsÂ _____Â

- Remote access is granted within the job functionÂ _____Â

- Encryption has been set on all RAS logon and authentication informationÂ _____Â

- Remote access users are monitored and reviewed _____Â

1.10. ServerÂ Platforms Controls

1.10.1. Overview

Most organizations at present have servers that are dispersed to different organizational units. Some of these servers are used for departmental or regional computing. For example, a regional office in Atlanta may have a server that handles all the applications and databases at Atlanta.Â Some servers are used for specialized purposes such as email servers, portal servers, database servers, etc. Although the overall administrative controls discussed previously apply to these servers, the following checklists are intended to assure that these servers are also under proper controls. Some checklists will appear to be redundant with previous lists but they have a different purpose ? controls on servers and their compliance to the corporate standards and policies. This is a general procedure that can be and should be customized for different types of server platforms such as Windows NT, XP, 200x,Â Linux, Unix, and others.Â

1.10.2. Server Security Administration

- Someone is responsible for operating system administration and maintenance for the platformsÂ _____

- Administrators are made aware of system standards and Information Security Standards _____Â

- System and security administration procedures have been formally documented and up-to-date _____Â Â

- The following standards are being followed:Â
    - A standard naming convention is being usedÂ _____
    - Each user is assigned a unique user idÂ _____.
    - Group IDs and shared/generic account should not be used _____.
    - The system has been configured to authenticate all users through a valid ID and password
- Procedures are in place to review server configuration using commercially availableÂ tools _____Â Â
- Procedures are in place to ensure that system level accounts are disabled and/or removed for terminated employees _____Â
- Procedures are in place to ensure that user system access rights are appropriately modified for transferred employees _____Â
- Human Resources department provides security administration personnel with periodic reports of terminated and transferred employeesÂ _____
- Global password rules have been established by setting appropriate account policies. Examples of the rules are:Â
    - Minimum Password Age (allow changes in 1 day)
    - Maximum Password Age(60 days)
    - Minimum password length (6 characters)
    - Account Lockout (allow 3 bad attempts)
    - Account Lockout (reset count in 1440 minutes)
    - Lockout Duration (Forever)
    - Password History (Remember 3 passwords)Â

1.10.3. Monitoring System Access and Use

Objective is to detect unauthorized activities.

- Audit logs of event logging is being kept for an agreed period _____Â
- Audit logs contain User Id's. dates & times for logon, logoff, terminal identification or location if possible, records of successful and rejected systems, data, and other resource access attemptsÂ _____Â
- Procedures are set for monitoring the use of information processing facilities _____
- Results of the monitoring are reviewed regularly to assess risk factors _____
- System clocks are reviewed to ensure accuracy (correct setting of computer clocks is important to ensure the accuracy of audit logs)Â _____

1.10.4. Operating System Access Controls

Objective is to prevent unauthorized computer access.

- Automatic terminal identification in place to authenticate connections to specific locations and to portable equipment _____
- Logon procedure not display system or application identification until logon successfully completed _____
- A general notice is displayed that the computer should only be accessed by authorized usersÂ _____
- Number of unsuccessful logon attempts is limited to 3Â _____
- Unsuccessful attempts are recorded rigorouslyÂ _____
- The password management system:
    - Enforces the use of individual passwords to maintain accountability _____
    - Allow users to select and change their own passwords _____
    - Enforces a choice of quality passwords _____
    - Enforces password changes periodically (e.g., passwords expire once a month or twice a year)Â _____
    - Stores password files separately to application system data _____Â Â
    - Stores passwords in encrypted formÂ _____
    - Alters default vendor passwords following installation of software _____

1.10.5. User Accounts

- Guest account has been disabledÂ _____Â
- Administrator account has been renamed to stop intruders from accessing this account _____Â
- Strong password has been set for the administrator accountsÂ _____
- Administrator has his unique account assigned to only him, and not shared by other administratorsÂ _____Â
- Logon scripts are secured with restricted access permissionÂ _____Â
- User is required to change the password at the time of initial logon _____
- Length of time restrictions are placed on system accounts provided to contractors and temporary workersÂ _____Â

1.10.6. Groups

- A structure exists to group user IDs by department or job functions in order to be efficiently administered by securityÂ _____Â
- The rights have been assigned to the global groups and the group membership and privileges are appropriateÂ _____Â
- The rights have been assigned to the local groups. Verify that group membership and privileges are appropriate _____
- There is a business purpose for each globalÂ group _____
- There is a business purpose for each local group _____Â
- The number of users with privileged access is limited _____

1.10.7. User Rights

- Standard user access rights (read, write, execute) specifiedÂ Â Â _____Â
- Any user given rights outside standard require special authorizationÂ _____
- Periodic review of user access rights in place to ensure that access rights remain commensurate with user job responsibilitiesÂ _____
- Audit software is used as part of the regular reviewsÂ _____

1.10.8. System Registry Security

- File and directory permissions are appropriate for groups with accessÂ _____
- Permissions set for the critical Registry keys are configured to recommended standardsÂ _____Â Â

1.10.9. Operating System Configuration

- Formal procedures are in place over the installation of new servers to ensure the consistency of operating system configuration settings throughout the processing environmentÂ _____Â
- Formal standards and procedures are inÂ place over the implementation of operating system upgradesÂ _____Â
- Operating system installations/upgrades are thoroughly tested and hardened before being loaded into the production environmentÂ _____Â
- Fallback procedures are in place for operating system upgradesÂ _____Â
- Controls are in place to ensure that operating system security configuration changes are authorized and approvedÂ _____
- Records are maintained to document all modifications and fixes to operating system securityÂ _____Â

- Secure passwords for predefined system accounts (i.e., Administrator, Guest, etc.) are assigned immediately upon installation or upgradeÂ _____Â
- Powerful system utilities that assist system administrators (i.e., disk management, system registry editing, etc) are appropriately restricted to authorized system personnel only _____Â
- Appropriate trust relationships have been established based on corporate standards _____
- Formal standards and procedures exist over the configuration of security at the directory and file levelÂ _____Â
- Key system directories are secured _____
- Access to key system directories is restricted to system administration personnelÂ _____Â
- Permissions assigned to shared resources within the environment have been restricted _____Â

1.10.10. File and Directory Protection

- Critical production application directories, subdirectories, and files have been identifiedÂ _____Â
- Critical directory and file permissions are set based onÂ corporate standardsÂ _____Â
- Users are not granted access to modify key system programsÂ _____Â Â

1.10.11. Monitoring/Auditing/Reporting

- Systems have beenÂ configured to log audit events such as:
    - Log-on and log-off activity (failure)Â Â _____
    - Security policy changes (failure)Â Â _____
    - Restart and Shutdown (failure)Â Â _____Â
- System audit log files are securedÂ _____Â Â
- Audit logs are backed up on a regular basisÂ Â _____
- Audit logs are reviewed by appropriate security/system administration personnel on a regular basisÂ _____Â
- Escalation procedures are in place to ensure that detected security events are appropriately investigated in a timely mannerÂ _____Â
- Reports are produced to evaluate trends in the audit log informationÂ _____
- Procedures established to prevent, detect, and recover from computer virusesÂ _____

- Invalid attempts to exercise administrative rights are trackedÂ _____Â

1.10.12. Server Backup Recovery

- Backup and recovery procedures are in placeÂ _____Â

1.10.13. Server Physical Security

- Critical servers are physically secured from unauthorized access.

1.11. Additional IT Infrastructure Controls

These controls are overall controls governing the organization's information technology infrastructure. The following starter checklist can be extended considerably. :

- Database management system resources, such as Oracle and SQL Server dictionaries are properly protectedÂ _____
- IDEs (Integrated Development Environments) such as IBM's Websphere Studio and Microsoft's .NET Visual Studio are properly protected from potential attacks and failures _____.Â
- Middleware services are placed in protected areas with proper authentication and authorization controlsÂ Â _____Â Â
- The integrity of application serversÂ is protected against compromised. _____
- Controls in place to ensure that computer hardware is physically secure and can be accessed only by authorized individuals _____