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.
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.

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 plans
- The management of the information systems security was established and applied using a structured approach

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):
  o Web pages
  o Firewalls
  o Employee Surveillance
  o Electronic Banking
  o Viruses
  o Encryption
  o Digital Signatures/Certificates
  o Contingency Planning
  o Laptops/Portable
  o Logging Controls
  o Internet/Intranet
  o Privacy
  o Emergency Response
  o Micro-computers
  o LAN
  o Passwords
  o E-mail
  o Data Classification
  o Telecommuting
  o User Training
  o Ethics

• Procedures and practices are used by the ISSO to monitor compliance with the above policies

• Ensure the ISSO has been given the positional authority to address policy violations, or reports to an appropriate level of management

• Documented actions taken to address recent policy violations

1.1.3. Risk Assessment/Ongoing Analysis
• A framework exists to assess information security risks
• A methodology adopted for risk assessment
• 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 management
• 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 obtained

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 information

1.1.5. **Information Security Staffing**

• Position descriptions exist for the information security position
• Position descriptions consistent with the ISSO responsibilities
• 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)
• Impact of external relationships (e.g., partnerships) on compliance requirements, has been assessed
• Appropriate and timely corrective actions have been taken for information security deficiencies in compliance examinations, regulatory reviews, and/or audits conducted so far

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)

• Protected entry controls, such as the following, have been established to ensure that only authorized personnel are allowed access
  o Badges
  o Limited access to buildings
  o Guards on entrance doors
  o Properly secured and tamper proof wiring
  o Alarm doors

• Suitable intruder detection systems are installed for this area

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

• Controls are in place for the delivery and loading areas

• Access from outside is restricted to formally authorized and identified personnel

• External door is secured when the internal door is opened

• 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

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

• Controls exist to ensure that power and telecommunications cabling is protected from interception or damage

• Equipment maintenance is done periodically

• Only authorized maintenance personnel carry out repairs and service
• Records kept of all suspected or actual faults ________________
• Adequate insurance in place to protect equipment taken off-site ________________
• Controls on authorized equipment exist for off-site ____________
• Sensitive information securely destroyed from retired equipment _________
• Name of the contractors recorded 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 ____________
• Procedures in place to prevent unauthorized removal of property _________
• 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:
  o Processing and handling of information _________
  o Scheduling requirements _________
  o Instructions for handling errors or other exceptional conditions ________________
  o Support contacts _________
  o Special output handling instructions ________________
  o System restarts and recovery procedures _________
  o Close down procedures _________
1.3.1.2. Production Change Control

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

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

1.3.1.3. Incident Management Procedures

a) Procedures for security incident including

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

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

- Only authorized staff are allowed access to live system and data.
- All emergency actions are documented in detail
- Emergency action is reported to management
- 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 fraud and/or crime
- To avoid collusion, duties have been segregated to ensure that 2 or more persons are involved
1.3.1.5. Separation of Development and Production Facilities.

- Separate facilities for development and production software.
- Different logon procedures for test and production systems to reduce risk of error and production problems.

1.3.2. System Planning and Acceptance

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 plan.

1.3.2.2. System Acceptance

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

1.3.3. Protection Against Malicious Software

Objective is to protect the integrity of software and information.

Controls against malicious software should include:

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

1.3.4. Housekeeping (Traditional, Mainframe Systems)

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

1.3.4.1. Information Back-up

• Back-up arrangement documented in restoration procedures.
• Back-up information stored in a remote location.
• 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 situations.

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).
• Logs are subject to regular, independent checks against operating procedures.

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 compromised by personnel.
• Actions taken to handle faults are fully authorized.
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.

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 are erased.
- Authorization is required and an audit trail is kept of all highly sensitive removable media.
- Sensitive media stored in a safe, secure location.
- Procedures for disposal of sensitive media.

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 media.
  - Access restrictions to identify unauthorized personnel.
  - Maintenance of a formal record of the authorized recipients of data.
  - Ensuring that input, processing, and output is validated and verified for sensitive applications.
  - Protection of spooled data is at a level consistent with sensitivity.
  - Storage of media in secure areas.
  - Keeping the distribution of data to a minimum.
  - 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 minimum.
- System documentation not held on a public or unsecure network.
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:

- Security requirements for each application
- Standard user profiles for common categories of job
- Management access rights in a network environment

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
- Procedures and standards to remove access from terminated employees, transferred employees, and discontinued vendors
- The access lists are reviewed for the sensitive systems
- Someone has the "ownership" of the user access reviews

1.4.2.2. User Registration

- A formal procedure exists for granting access to all information systems and services
- Use 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
- Periodically checking for removing redundant User Id's from access
- 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 controls
• A formal management process in place re the allocation of passwords

• Review of user access rights done reviewed on a regular basis ie 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:
  o Terminate active sessions when finished
  o Logoff mainframe systems when session finished
  o 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

• Security requirements analyzed and specified at the design state of 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

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. Control of Production Software

- Updating of operational program libraries is only performed by the nominated librarian.
- Operational systems only hold executable code (source code not included for security purposes).
- Executable code is not implemented on operational system without evidence of successful testing.
- 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:

- 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 completed.
- 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.
- A program librarian has been assigned for all sensitive applications.
- 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.
- Program listings are held in a secure environment.

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.

• Periodic technical reviews are completed of all operating changes.

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

• Protection in place for backdoors and Trojan code through careful buying practices (i.e., buying programs from reputable vendors) and inspections of source code before production use.

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 attacks.

• The continuity plan contains the following:
  o Identification of attacks (natural, malicious)
  o Key personnel responsible for responding to attacks
  o System to notify the key personnel
  o Offsite location for system backups
  o Offsite location for system operation
  o Physical arrangements (personnel moved to off-sites, hotel accommodations in the target areas, etc)
  o 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 procedures.
• Proprietary software is registered under license agreements that limits the use of the products to specified machines.
• 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 securely.
• Data protection and Privacy Laws are adhered to.
• A data protection officer has been assigned. Cryptographic controls have been implemented which include:
  o Import and/or export of computer hardware and software for performing cryptographic functions.
  o Import and/or export of computer hardware and software which is designed to have cryptographic functions added to it.
  o Mandatory and discretionary methods of access by the countries to information encrypted by hardware or software to provide confidentiality of content.

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 policy.
• Organization has a dedicated (isolated) computing environment for highly 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 organizations.
• 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 technologies ______

• Publicly available systems are protected through policies and technologies ______

• Security of media in transit is enforced through:
  o Reliable transport/courier company used _______________
  o Packaging to protect the contents from physical damage ___________
  o 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:
  o Matching controls that compare the input data with information held on system files. _______________
  o Processing edits to verify for reasonableness or consistency during processing of applications _______
  o 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:
  o Checks to test whether the output data is reasonable _______________
  o Reconciliation control counts to ensure processing of all data _______________
Providing sufficient information for a reader or subsequent processing system to
determine the accuracy and completeness of the information

Procedures for responding to output validation tests

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 needed

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 encrypted by using XML Encryption, XML Signatures
  or other suitable schemes
- 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.

- Mobile clients are authenticated before they can invoke applications
- Security checks are done at the wireless gateway (e.g., WAP Gateway)
- Transactions have proper controls for remote invocations
- 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 enterprise
- Policy indicates the network and network services allowed to be accessed, authorization procedures for determining who is allowed access to which networks and networked services
- Only restricted paths (e.g., dedicated and/or encrypted lines, security firewalls, limited menu and submenu options for users) allowed to sensitive databases and programs
- User authentication for remote users for external connections
- Segregation of networks (separate logical network domains, firewalls) 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 resources
- VPN used for external network access
- A warning message is initiated for users accessing the proprietary network. The wordings may be "You have connected to a proprietary system. Only authorized users may access this system. Access by unauthorized individuals is prohibited and will be prosecuted to the full extent of the law. This system is monitored for unauthorized usage."

1.9.2. Network Firewalls 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.

• Responsibilities and procedures for the management of remote equipment has been established.

• Special controls have been established for confidentiality and integrity of data passing over public networks.

1.9.3. Remote Access Service (RAS) Controls

• Remote Access Services (RAS) is installed on the server being reviewed.

• Remote access authorization is granted based on corporate standards.

• Remote access is granted within the job function.

• Encryption has been set on all RAS logon and authentication information.

• Remote access users are monitored and reviewed.

1.10. Server 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. 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, Linux, Unix, and others.

1.10.2. Server Security Administration

• Someone is responsible for operating system administration and maintenance for the platforms.

• Administrators are made aware of system standards and Information Security Standards.

• System and security administration procedures have been formally documented and up-to-date.
• The following standards are being followed:
  o A standard naming convention is being used
  o Each user is assigned a unique user id
  o Group IDs and shared/generic account should not be used
  o 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 available tools

• Procedures are in place to ensure that system level accounts are disabled and/or removed for terminated employees

• Procedures are in place to ensure that user system access rights are appropriately modified for transferred employees

• Human Resources department provides security administration personnel with periodic reports of terminated and transferred employees

• Global password rules have been established by setting appropriate account policies. Examples of the rules are:
  o Minimum Password Age (allow changes in 1 day)
  o Maximum Password Age (60 days)
  o Minimum password length (6 characters)
  o Account Lockout (allow 3 bad attempts)
  o Account Lockout (reset count in 1440 minutes)
  o Lockout Duration (Forever)
  o Password History (Remember 3 passwords)

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

• 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 attempts

• 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)
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 users
- Number of unsuccessful logon attempts is limited to 3
- Unsuccessful attempts are recorded rigorously
- 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)
  - Stores password files separately to application system data
  - Stores passwords in encrypted form
  - Alters default vendor passwords following installation of software

1.10.5. User Accounts

- Guest account has been disabled
- Administrator account has been renamed to stop intruders from accessing this account
- Strong password has been set for the administrator accounts
- Administrator has his unique account assigned to only him, and not shared by other administrators
- Logon scripts are secured with restricted access permission
- 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 workers
1.10.6. Groups

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

1.10.7. User Rights

- Standard user access rights (read, write, execute) specified.
- Any user given rights outside standard require special authorization.
- Periodic review of user access rights in place to ensure that access rights remain commensurate with user job responsibilities.
- Audit software is used as part of the regular reviews.

1.10.8. System Registry Security

- File and directory permissions are appropriate for groups with access.
- Permissions set for the critical Registry keys are configured to recommended standards.

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 environment.
- Formal standards and procedures are in place over the implementation of operating system upgrades.
- Operating system installations/upgrades are thoroughly tested and hardened before being loaded into the production environment.
- Fallback procedures are in place for operating system upgrades.
- Controls are in place to ensure that operating system security configuration changes are authorized and approved.
- Records are maintained to document all modifications and fixes to operating system security.
• Secure passwords for predefined system accounts (i.e., Administrator, Guest, etc.) are assigned immediately upon installation or upgrade.

• Powerful system utilities that assist system administrators (i.e., disk management, system registry editing, etc.) are appropriately restricted to authorized system personnel only.

• 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 level.

• Key system directories are secured.

• Access to key system directories is restricted to system administration personnel.

• Permissions assigned to shared resources within the environment have been restricted.

1.10.10. File and Directory Protection

• Critical production application directories, subdirectories, and files have been identified.

• Critical directory and file permissions are set based on corporate standards.

• Users are not granted access to modify key system programs.

1.10.11. Monitoring/Auditing/Reporting

• Systems have been configured to log audit events such as:
  o Log-on and log-off activity (failure)
  o Security policy changes (failure)
  o Restart and Shutdown (failure)

• System audit log files are secured.

• Audit logs are backed up on a regular basis.

• Audit logs are reviewed by appropriate security/system administration personnel on a regular basis.

• Escalation procedures are in place to ensure that detected security events are appropriately investigated in a timely manner.

• Reports are produced to evaluate trends in the audit log information.

• Procedures established to prevent, detect, and recover from computer viruses.
• Invalid attempts to exercise administrative rights are tracked.

1.10.12. Server Backup Recovery
• Backup and recovery procedures are in place.

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 protected.

• IDEs (Integrated Development Environments) such as IBM's Websphere Studio and Microsoft's .NET Visual Studio are properly protected from potential attacks and failures.

• Middleware services are placed in protected areas with proper authentication and authorization controls.

• The integrity of application servers is protected against compromised.

• Controls in place to ensure that computer hardware is physically secure and can be accessed only by authorized individuals.