PREPARED BY:	AUDIT PROGRAM	Author: Lance M. Turcato
APPROVED BY:	Logical Security Operating Systems - Generic	Audit Date:_____

Assigned	Sec.	Sub-Sec.	Audit Step	Date	Ref.	Initials
	A		**SYSTEMS UNDERSTANDING**			
	A	1.0	**Organization** **Objective: To ensure that the audit team has a clear understanding of the delineation of responsibilities for system administration and maintenance.**			
	A	1.1	Determine who is responsible for systems administration and maintenance. Obtain a current organization chart if available.			
	A	2.0	**Hardware Platforms** **Objective: To ensure that the audit team has a clear understanding of the hardware platforms subject to review and to obtain the necessary information for identifying critical systems throughout the processing environment.**			
	A	2.1	Obtain an understanding of the server infrastructure at the site under review: • Request a complete server inventory. If an inventory is not available, obtain an understanding of the server environment through discussions with the system administrator(s). • If a server inventory is unavailable, meet with systems administration personnel and tour the facility to identify all servers and collect information regarding each server. • At a minimum, obtain the following information for each server included in the scope of the review: ▪ Server name ▪ Manufacturer and model ▪ Purpose / function of each server ▪ Owner ▪ Enterprise supported ▪ Responsible systems administrator • Identify the key servers that support business applications.			
	A	2.2	Obtain an understanding of the peripherals in the environment (i.e., printers, shared disks, etc.).			
	A	2.3	Determine if there are known problems with servers in the environment.			
	A	3.0	**Operating System** **Objective: To ensure that the audit team has a clear understanding of the operating system included in the scope of the review. Furthermore, to ensure that known vulnerabilities associated with specific operating system versions are considered during the audit to ensure that all exposures are identified.**			
	A	3.1	Ascertain which version(s) of the operating system are running on the servers included in the scope of the audit.			
	A	3.2	Determine if the most current version of the operating system is installed. If not, evaluate the justification for why the most current version is not installed.			
	A	3.3	Ascertain whether all known operating system fixes have been installed. If not, evaluate the justification for why available fixes have not been installed.			
	A	3.4	Determine if procedures are in place to ensure that system administration personnel are informed of available operating system fixes in a timely manner.			
	A	3.5	Determine if third-party security software is running on the servers.			
	A	4.0	**Network Overview** **Objective: To ensure that the audit team has a clear understanding of network components and interfaces which may impact the logical security of specific servers and workstations.**			

PREPARED BY:			AUDIT PROGRAM	Author: Lance M. Turcato		
APPROVED BY:			Logical Security Operating Systems - Generic	Audit Date:_____		
Assigned	Sec.	Sub-Sec.	Audit Step	Date	Ref.	Initials
	A	4.1	Obtain an understanding of the network environment at the site under review. (NOTE: Determine if audit professionals responsible for network security have documentation regarding the network environment before initiating discussions with system administrators).			
	B		**SECURITY MANAGMENT**			
	B	1.0	**Roles & Responsibilities** **Objective: To ensure that roles and responsibilities for security management have been clearly and appropriately defined.**			
	B	1.1	Determine who is responsible for ensuring that the processing environment is in compliance with applicable corporate security policies and standards.			
	B	1.2	Determine whether or not appropriate systems and security administration personnel are involved in defining corporate security policies and standards to ensure the applicability of the policies and standards throughout the processing environment.			
	B	2.0	**Corporate Security Policies & Standards** **Objective: To ensure that existing corporate security policies and standards have been communicated. Furthermore, to ensure that existing policies and standards are applicable throughout the processing environment and that all systems are in compliance with appropriate policies and standards.**			
	B	2.1	Determine if existing corporate security policies and standards are applicable to the environment under review.			
	B	2.2	Determine if security administration personnel are aware of relevant corporate security policies and standards for the operating environment under review.			
	B	2.3	Identify the procedures in place to ensure compliance with relevant corporate security policies and standards.			
	B	3.0	**Security Awareness & Training** **Objective: To ensure that end-users are aware of appropriate corporate security policies and standards and are informed of their individual responsibilities relative to ensuring a secure processing environment.**			
	B	3.1	Determine if a process is in place to ensure that all systems and security administration personnel are informed of all relevant corporate security policies and standards.			
	B	3.2	Determine if a process is in place to ensure that all new employees are informed of corporate security policies and standards.			
	B	3.3	Determine if a security awareness program is in place to ensure that end-users are periodically informed of corporate security policies and standards to ensure that they are aware of their individual responsibilities relative to security. .			
	B	3.4	Determine if processes are in place to ensure that individuals with security administration responsibilities are kept informed of key security advisories (i.e., CERT, CIAC, etc.) and issues related to installed operating systems.			
	C		**SECURITY ADMINISTRATION**			
	C	1.0	**Roles & Responsibilities** **Objective: To ensure that roles and responsibilities for security administration have been clearly and appropriately defined.**			
	C	1.1	Determine if the role and responsibilities of Security Administrator have been formally defined and documented.			

PREPARED BY:			AUDIT PROGRAM	Author: Lance M. Turcato		
APPROVED BY:			Logical Security Operating Systems - Generic	Audit Date:_____		
Assigned	Sec.	Sub-Sec.	Audit Step	Date	Ref.	Initials
	C	1.2	Determine if individuals with security administration responsibilities are dedicated to security administration on a full-time basis? If security administration is a part-time responsibility, determine if the individuals with security administration responsibilities have other responsibilities that are incompatible with the security administration function.			
	C	2.0	**Staffing** **Objective: To ensure that appropriate processes are in place to ensure that individuals with security administration responsibilities are qualified to complete defined security administration tasks.**			
	C	2.1	Evaluate the hiring process for system and security administration personnel. Specifically, determine if: • written job descriptions exist for system and security administrators, • a process is in place to ensure that prospective employee are appropriately qualified, and • prospective employee skills are adequately assessed prior to employment.			
	C	2.2	Determine if security administration personnel have been adequately trained to support the technology that they are responsible for.			
	C	2.3	Ascertain if backup system and security administration personnel have been identified to provide systems support in the event that the primary administrator(s) are unavailable.			
	C	2.4	Determine if vendors / contractors have security administration responsibilities.			
	C	3.0	**Security Administration Procedures** **Objective: To ensure that security administration responsibilities and activities have been adequately defined and documented to support the security administration function and to ensure that appropriate documentation is available to facilitate training processes for new administrators.**			
	C	3.1	Determine if documented procedures exist to support the security administration function and to facilitate the training process for new employees.			
	C	3.2	If documented procedures exist, ascertain if the documentation is up to date.			
	C	3.3	If documented procedures exist, evaluate the documentation and determine whether the documentation is adequate to provide guidance in the event that primary security administration personnel become unavailable.			
	C	3.4	Evaluate the use of third-party tools to complete security administration activities.			
	C	3.5	Determine if in-house developed automated processes (e.g., scripts) are used to complete security administration activities. Ensure that: • Script files are secured. • Documentation has been prepared to support these processes.			
	D		**SYSTEM CONFIGURATION**			
	D	1.0	**Servers** **Objective: To ensure that adequate controls are in place over the installation and configuration of server hardware.**			
	D	1.1	Determine if formal policies and standards exist for the installation and configuration of server hardware.			
	D	1.2	Determine if documented procedures / checklists exist to support the server installation process.			
	D	1.3	Determine if processes are in place to ensure that server installations are in compliance with applicable policies and standards.			

PREPARED BY:			AUDIT PROGRAM	Author: Lance M. Turcato		
APPROVED BY:			Logical Security Operating Systems - Generic	Audit Date:_____		
Assigned	Sec.	Sub-Sec.	Audit Step	Date	Ref.	Initials
NOTE: If reliance is placed on third-party security systems (e.g., TopSecret) to control system level security, refer to sections D 6.0 through D 8.0.						
	D	**2.0**	**Operating System Configuration - Policies & Standards** **Objective: To ensure that operating system installations and upgrades are configured in compliance with appropriate security and configuration policies and standards.**			
	D	**2.1**	Determine if formal policies and standards exist for the configuration of the operating system under review.			
	D	**2.2**	If policies and standards exist, identify which of these policies and standards are applicable to the environment under review.			
	D	**2.3**	Determine if procedures are in place to ensure compliance with applicable policies and standards throughout the configuration process for operating system installations and upgrades.			
	D	**3.0**	**Operating System Configuration - Configuration Process** **Objective: To ensure that adequate controls are in place over the configuration of operating system installations and upgrades.**			
	D	**3.1**	Ensure that the operating system installation / upgrade process is subject to corporate change management guidelines. No further testing of controls over systems software maintenance is necessary as these controls are addressed in the change management audit programs.			
	D	**3.2**	Determine if documented procedures / checklists exist to support the configuration of system *security* parameters during the operating system installation / upgrade process.			
	D	**3.3**	Determine if standard operating system configuration images are maintained to ensure the consistency of all operating system configuration efforts.			
	D	**3.4**	Determine if all operating system *security* configurations are appropriately authorized as well as adequately reviewed and approved by appropriate management prior to being introduced into the production environment.			
	D	**3.5**	Determine if adequate records are maintained to document all modifications and fixes to operating system security.			
	D	**3.6**	Ensure that operating system configuration procedures include steps to ensure compliance with all relevant corporate policies and standards.			
	D	**3.7**	Ensure that appropriate records are maintained to document all deviations from relevant corporate policies and standards.			
	D	**3.8**	Determine if operating system configuration policies and standards require that • all vendor supplied default passwords for predefined system accounts are changed immediately upon installation or upgrade, • all unneeded vendor supplied system accounts are disabled or deleted, and • all passwords for privileged system accounts are assigned to appropriate system / security administration personnel.			
	D	**4.0**	**Operating System Configuration - System Security Parameters** **Objective: To ensure that existing operating system security parameters are configured to secure settings and are in compliance with best practices and relevant corporate policies and standards.**			
	D	**4.1**	Review relevant corporate policies and standards for the operating system under review. Tailor this audit program to ensure that audit procedures are designed to ensure that operating system configuration settings are in compliance with those policies and standards.			
	D	**4.2**	Evaluate existing best practices for the configuration of operating system security parameters. Tailor this audit program to ensure that applicable best practices are considered in the audit approach.			

Assigned	Sec.	Sub-Sec.	Audit Step	Date	Ref.	Initials
	D	4.3	Evaluate current operating system configuration settings to ensure that the settings are in compliance with relevant corporate policies and standards and conform to best practices.			
	D	4.3.1	Ensure that all default passwords for predefined system accounts have been changed.			
	D	4.3.2	Determine if the configurations for predefined system account profiles have been changed from the vendor settings. If so, determine why and evaluate the effect of the changes on system security.			
	D	4.3.3	Determine if the configurations for predefined group profiles have been changed from the vendor settings. If so, determine why and evaluate the effect of the changes on system security.			
	D	4.3.4	Ensure that all guest accounts have been disabled or removed from the system.			
	D	4.3.5	Ensure that the assigned passwords for super-user accounts are known by appropriate system / security administration personnel only.			
	D	4.3.6	Ensure that all defined system services have been approved and are in compliance with relevant configuration policies and standards.			
	D	4.3.7	Ensure that all systems services are configured to appropriate system ports.			
	D	4.3.8	Ensure that processes are in place to prevent the operating system from being booted with unauthorized configuration settings.			
	D	5.0	**System Utilities** **Objective: To ensure that adequate controls are in place over the use of sensitive system utilities.**			
	D	5.1	Evaluate procedures in place to restrict access to powerful and sensitive system utilities.			
	D	5.2	Identify those installed utilities that have the ability to bypass system level security.			
	D	5.3	Determine if any scripts, command procedures, or applications have been developed which have the ability to bypass system security.			
	D	5.4	Identify the accounts and groups with access to system utilities. Ensure that the number of users with access to these utilities is reasonable and appropriate based upon the user's job function.			
NOTE: Sections D 6.0 through D 8.0 are only applicable if third-party security systems are installed and relied upon my management to control system level access (e.g., TopSecret).						
	D	6.0	**Security System Configuration - Policies & Standards** **Objective: To ensure that third-party security system installations and upgrades are configured in compliance with appropriate security and configuration policies and standards.**			
	D	6.1	Determine if formal policies and standards exist for the configuration of the third-party security system under review.			
	D	6.2	If policies and standards exist, identify which of these policies and standards are applicable to the environment under review.			
	D	6.3	Determine if procedures are in place to ensure compliance with applicable policies and standards throughout the configuration process for security system installations and upgrades.			
	D	7.0	**Security System Configuration - Configuration Process** **Objective: To ensure that adequate controls are in place over the configuration of third-party security system installations and upgrades.**			

PREPARED BY:			AUDIT PROGRAM	Author: Lance M. Turcato		
APPROVED BY:			Logical Security Operating Systems - Generic	Audit Date:_____		
Assigned	Sec.	Sub-Sec.	Audit Step	Date	Ref.	Initials
	D	7.1	Ensure that the security system installation / upgrade process is subject to corporate change management guidelines. No further testing of controls over systems software maintenance is necessary as these controls are addressed in the change management audit programs.			
	D	7.2	Determine if documented procedures / checklists exist to support the configuration of the security system parameters during the installation / upgrade process.			
	D	7.3	Determine if standard configuration images are maintained to ensure the consistency of all configuration efforts for the security system under review.			
	D	7.4	Determine if all security system configurations are appropriately authorized as well as adequately reviewed and approved by appropriate management prior to being introduced into the production environment.			
	D	7.5	Determine if adequate records are maintained to document all modifications and fixes to third-party security systems.			
	D	7.6	Ensure that configuration procedures include steps to ensure compliance with all relevant corporate policies and standards.			
	D	7.7	Ensure that appropriate records are maintained to document all deviations from relevant corporate policies and standards.			
	D	7.8	Determine if security system configuration policies and standards require that • all vendor supplied default passwords for predefined system accounts are changed immediately upon installation or upgrade, • all unneeded vendor supplied system accounts are disabled or deleted, and • all passwords for privileged system accounts are assigned to appropriate system / security administration personnel.			
	D	**8.0**	**Security System Configuration - System Security Parameters** **Objective: To ensure that existing parameters for third-party security systems are configured to secure settings and are in compliance with best practices and relevant corporate policies and standards.**			
	D	8.1	Review relevant corporate policies and standards for the security system under review. Tailor this audit program to ensure that audit procedures are designed to ensure that third-party security system configuration settings are in compliance with those policies and standards.			
	D	8.2	Evaluate existing best practices for the logical system security. Tailor this audit program to ensure that applicable best practices are considered in the audit approach.			
	D	8.3	Evaluate current third-party security system configuration settings to ensure that the settings are in compliance with relevant corporate policies and standards and conform to best practices.			
	D	8.3.1	Ensure that all default passwords for predefined accounts have been changed.			
	D	8.3.2	Ensure that ownership of all predefined accounts is documented.			
	D	8.3.3	Determine if the configurations for predefined system account profiles have been changed from the vendor settings. If so, determine why and evaluate the effect of the changes on system security.			
	D	8.3.4	Determine if the configurations for predefined group profiles have been changed from the vendor settings. If so, determine why and evaluate the effect of the changes on system security.			
	D	8.3.5	Ensure that the assigned passwords for super-user accounts are known by appropriate system / security administration personnel only.			
	D	8.3.6	Ensure that all defined system services have been approved and are in compliance with relevant configuration policies and standards.			
	D	8.3.7	Ensure that all systems services are appropriately configured.			
	D	8.3.8	Ensure that processes are in place to prevent the system from being booted / IPLed with unauthorized security system configuration settings.			

PREPARED BY:			AUDIT PROGRAM	Author: Lance M. Turcato		
APPROVED BY:			Logical Security Operating Systems - Generic	Audit Date:_____		
Assigned	Sec.	Sub-Sec.	Audit Step	Date	Ref.	Initials
	E		**ACCESS CONTROLS**			
	E	1.0	**Account Management** **Objective: To ensure that appropriate controls are in place over the system level account management process.**			
	E	1.1	Meet with security administration personnel to obtain an understanding of the account management process. Consider: • Are system / security administrators aware of relevant corporate policies and standards regarding user account management? • Have formal account management procedures been developed? ⇒ Are formal procedures in place over the creation of new user accounts? ⇒ Are formal procedures in place over the modification of existing accounts? ⇒ Are formal procedures in place to ensure that system level accounts are disabled and/or removed promptly for terminated employees? ⇒ Are formal procedures in place to ensure that user access rights are appropriately reviewed and modified for transferred employees? • Are third-party automated tools utilized? • Are in-house developed scripts utilized? • Are all new system level accounts authorized by appropriate management before creation? • Is appropriate documentation maintained to support the authorization of all system level accounts? • Are user account templates used to set-up new accounts or does the security / system administrator set-up each account from scratch? • Do all system level IDs follow a consistent naming convention? • Are all account IDs unique? • Does the Human Resources department provide security administration personnel with periodic reports of terminated and transferred employees? • Are periodic reviews of user access rights completed by appropriate management to ensure that access rights remain commensurate with user job responsibilities? • Have the systems been configured to automatically disable accounts that have been inactive for an excessive time period (*e.g.*, 90 days)?			
	E	1.2	If available, review documented procedures in place to support user account management activities.			
	E	1.3	Request a listing of all system accounts from the responsible security / systems administrator.			
	E	1.3.1	Review the system account listing and determine if all IDs follow a consistent naming convention and comply with existing standards.			
	E	1.3.2	Determine if any accounts exist which have been inactive for over 90 days and have not been disabled.			
	E	1.4	Request a report that summarizes all terminations that have occurred with the last three months. Verify that the accounts for all terminated employees have been disabled or removed from the systems.			

Assigned	Sec.	Sub-Sec.	Audit Step	Date	Ref.	Initials
	E	1.5	Judgmentally select a sample of accounts from the account listing requested in step **E 1.3** and review the following: • Are all account IDs unique and in compliance with existing naming conventions? • Is appropriate documentation available to support the authorization of each account and the approval of all access rights and privileges granted to each account? • Is documentation available which supports periodic reviews of user access rights?			
	E	2.0	**Password Management** **Objective: To ensure that the system has been configured to facilitate the use of secure passwords to prevent unauthorized access to critical applications, data and system resources.**			
	E	2.1	Meet with security administration personnel to obtain an understanding of the password management controls. Consider: • Are security / system administration personnel aware of relevant policies and standards in place over the configuration of password management controls? • Have the systems been configured to authenticate **all** users through a valid ID and password? • Is a unique initial password assigned to all new accounts upon creation? • Are the initial passwords assigned to all new accounts set as pre-expired, requiring the user to change the password upon the initial logon? • Have the systems been configured to enforce restrictions on password syntax and use? • Are password dictionaries used? • Are passwords hard-coded within scripts, batch files, or applications?			

		2.2	Request appropriate reports from the security / system administrator which display current password management configurations and ensure the following:
			• Current configurations are in compliance with relevant corporate policies and standards.
			• Appropriate restrictions are in place over password syntax as required by relevant corporate policies and standards:
			  ■ Minimum password length (*e.g.*, 6 characters end users; 8 characters systems personnel and privileged accounts).
			  ■ Restrictions on password syntax (i.e., limit repeating characters, restrict special characters, etc.).
			  ■ Password lifetimes (*e.g.*, 30 days for privileged accounts; 60 days for end user accounts).
			  ■ Restrictions on the ability to re-use passwords (i.e., password histories maintained).
			• Appropriate controls are in place to limit the number of invalid access attempts allowed before an account is locked or disabled (*e.g.*, 3 invalid attempts allowed prior to the system taking evasive action).			

	E	3.0	**User Profile Configurations** **Objective: To ensure that adequate controls are in place over the configuration of user profiles to ensure that user access rights are commensurate with users' job responsibilities.**			

Assigned	Sec.	Sub-Sec.	Audit Step	Date	Ref.	Initials
	E	3.1	Meet with security administration personnel to obtain an understanding of the controls over the configuration of user profiles. Consider: • Are standards in place over the configuration of user profiles? • Are privileges and access rights granted to individual user accounts or are they granted to groups and then allocated to users by assigning users to those groups? • Have standard access definitions been established by job function or service (product)? • How are user profiles established? ⇒ Are user profile templates used to create new user profiles? ⇒ Are existing profiles copied and modified to create a new profile? ⇒ Are all new user profiles created from scratch? • Are user profiles configured to ensure that users are restricted to appropriate applications and menus? • Are users restricted from accessing the operating system command line in the production environment? • Are time restrictions placed on the use of the accounts? • Are station restrictions placed on the use of the accounts?			
	E	3.2	Select a sample of accounts from the system account listing requested in step **E 1.3**.			
	E	3.2.1	Review the current configurations of user profiles for each of the accounts included in the sample: • Ensure that the user profiles are configured securely and comply with applicable corporate policies and standards. • Ensure that the access rights and privileges assigned to each user are commensurate with the user's job responsibilities. • If login scripts are used, ensure that the login scripts are appropriately secured. • Ensure that the home directory for each account is properly referenced and secured. • Ensure that the account has not been inactive for an unreasonable time period (*e.g.,* greater than 90 days).			
	E	4.0	**Group Profile Configurations** **Objective: To ensure that adequate controls are in place over the configuration of group profiles to ensure that access rights for users assigned to the group profiles are commensurate with users' job responsibilities.**			
	E	4.1	Meet with security administration personnel to obtain an understanding of the controls over the configuration of group profiles. Consider: • Are standards in place over the configuration of group profiles? • Have standard group access definitions been established by job function or service (product)? • How are group profiles established? • Are default vendor supplied group profiles used? • Are group profiles configured to ensure that users are restricted to appropriate applications and menus? • Are the access rights assigned to group profiles reviewed and approved by appropriate management?			
	E	4.2	Request a report from the security / systems administrator which lists all group profiles existing on the systems.			
		4.2.1	Select a sample of group profiles for review.			

	E	4.2.2	Review the current configurations of each group profile included in the sample: • Obtain an understanding of the purpose of each group profile. • Ensure that the group profiles are configured securely and comply with applicable corporate policies and standards. • Review the access rights and privileges provided by the group profiles and ensure that the access rights and privileges are reasonable based upon the purpose of the profile (i.e., is there an issue regarding segregation of functions, etc.). • Ensure that the user accounts assigned to each group profile are appropriate? Are the access rights and privileges provided to the user by the group profile commensurate with each user's job responsibilities?			
	E	5.0	**Privileged Accounts** **Objective: To ensure that adequate controls are in place over the authorization, ownership, and use of sensitive super-user accounts.**			
	E	5.1	Meet with security administration personnel to obtain an understanding of the controls in place over privileged system level accounts. Consider: • Are standards in place over the assignment and use of privileged accounts? • Have superuser IDs been established to provide technical support staff with a means to address immediate, emergency platform problems? • Is the number of users with privileged access appropriately limited? • Are the passwords for super-user accounts (i.e., *root* - UNIX; *Administrator* - NT; etc.) unique to each server? • Do administrators login directly to super-user accounts (i.e., *root* - UNIX; *Administrator* - NT; etc.) or are administrators assigned the necessary privileges to complete system and security administration tasks utilizing their own unique accounts? • Do administrators login to their own unique accounts with administrative rights only when necessary to perform actions requiring those rights. At all other times do the administrators log on with unique accounts that have been granted fewer rights? • Are privileged user access rights reviewed on a regular basis by user management (*e.g.,* minimum quarterly review)?			
	E	5.2	Request a report from the systems / security administrator that lists all privileged accounts existing on the systems.			
	E	5.2.1	Review the report of privileged accounts: • Is the number of privileged accounts reasonable based upon the size of the environment? • Do the privileges assigned to these accounts appear appropriate? • Does documentation exist to support the authorization of each account and the approval of all privileges assigned to each account? • Are appropriate controls in place over the use of privileged predefined accounts supplied by the vendor (i.e., *Administrator* - NT; *root* - UNIX)? Is the use of these accounts appropriately monitored? • Do generic account IDs exist for any of the privileged accounts? If so, determine how management ensures accountability over the use of these generic accounts. • Ensure that all privileged accounts are active and are not associated with a terminated employee.			
	E	5.3	Request a report from the systems / security administrator that lists all privileged groups and the accounts assigned to those groups.			

Assigned	Sec.	Sub-Sec.	Audit Step	Date	Ref.	Initials
	E	5.3.1	Review the report of privileged groups: • Evaluate the purpose of each privileged group. • Based upon the purpose of each group, determine if the number of accounts assigned to each group appears reasonable. • Does documentation exist to support the authorization of each account assigned to each privileged group? • Ensure that all accounts assigned to each privileged group are active and are not associated with a terminated employee.			
	E	6.0	**Special User Accounts** **Objective: To ensure that appropriate controls are in place over the authorization, ownership, and use of unique special user accounts.**			
	E	6.1	Meet with security administration personnel to obtain an understanding of the controls in place over special user accounts: • Are standards in place over the assignment and use of special user accounts? • Are restrictions placed on accounts provided to contractors and temporary workers (i.e., time restrictions, etc.)? • Are special developer accounts provided to developers to diagnose application problems in the production environment? Is access to production environment read only? • Are emergency IDs created to perform emergency systems maintenance?			
	E	6.2	Evaluate the controls in place over the establishment and use of special user accounts.			
	E	7.0	**Logon / Logoff Processes** **Objective: To ensure that appropriate controls are in place over the logon and logoff processes.**			
	E	7.1	Determine if the systems have been configured to lock accounts after a specified number of invalid logon attempts (*e.g.*, 3 invalid attempts allowed prior to the system taking evasive action)?			
	E	7.2	Determine if system banners are displayed on the systems during the login process to provide a warning against unauthorized access.			
	E	7.3	Ensure that Organization specific information is not included in the system banner displays.			
	E	7.4	Determine if user names and / or passwords are hardcoded in logon scripts or command procedures.			
	E	7.5	Determine if the systems have been configured to automatically logoff or lock a terminal / workstation after a specified period of inactivity (*e.g.*, greater than 15 minutes of inactivity)?			
	E	7.6	Determine if the systems have been configured to limit concurrent logins to a single account.			
	E	7.7	Determine if system consoles have been appropriately secured to prevent unauthorized access?			
	E	8.0	**Generic / Shared Accounts** **Objective: To ensure that the use of generic and shared accounts is limited and justified by business need and to ensure that appropriate controls are in place over the use of these accounts.**			

Assigned	Sec.	Sub-Sec.	Audit Step	Date	Ref.	Initials
	E	8.1	Meet with security administration personnel to obtain an understanding of the controls in place over generic / shared accounts: • Are generic / shared accounts used (i.e., OPERATOR, etc.)? If so, on what basis? • Are system / security administrators aware of standards in place over the assignment and use of these accounts?			
	E	8.2	Review the list of accounts acquired in step **E 1.3** and identify all generic accounts and accounts that appear to be shared accounts.			
	E	8.3	If generic or shared accounts are identified, discuss these accounts with appropriate management to determine if the use of these accounts is reasonable and based upon business requirements.			
	E	8.4	Determine if policies and standards regarding generic / shared accounts are being met.			
	E	9.0	**Remote Access** **Objective: To ensure that appropriate controls are in place to control access to the internal network and systems from a remote system.**			
	E	9.1	Meet with security / systems administration personnel to obtain an understanding of the controls in place over access to the organization's systems via modems and other forms of remote access. • Are system / security administrators aware of standards regarding remote access? • Are authentication devices utilized to control remote access? • Are modem phone numbers kept confidential?			
	E	10.0	**System Boot Process** **Objective: To ensure that appropriate controls are in place to ensure that only authorized security settings and system services are initiated during the system boot / IPL process.**			
	E	10.1	Meet with security / systems administration personnel to obtain an understanding of the controls in place over system boots / IPLs.			
	E	10.2	Ensure that boot command procedures are appropriately secured.			
	F		**FILE & DIRECTORY PROTECTION**			
	F	1.0	**System Directories & Files** **Objective: To ensure that system level security has been configured to appropriately protect critical system directories and files.**			
	F	1.1	Meet with security / systems administration personnel to obtain an understanding of the controls in place over system directories and files. • Are system / security administrators aware of relevant standards regarding the configuration of security over system directories and files? • Are procedures in place over the configuration of security for system directories and files? • How are access rights for system directories and files determined and assigned? • Who approves access rights for system directories and files?			
	F	1.2	Determine if corporate policies and standards exist regarding the configuration of security over system directories and files for the operating platform under review.			
	F	1.3	Request reports from security / systems administration personnel which detail the current security settings for critical system directories and files.			
	F	1.3.1	Determine which accounts and groups have been assigned access to the system directories and files.			

Assigned	Sec.	Sub-Sec.	Audit Step	Date	Ref.	Initials
	F	1.3.2	Evaluate the appropriateness of the access rights assigned to the identified accounts and groups.			
	F	1.3.3	Determine if universal access (i.e., world, everyone) has been granted to any of the system directories or files.			
	F	1.4	Determine if appropriate system files have been encrypted (i.e., password files).			
	F	1.5	Determine if any scripts, command procedures, or applications have been developed which have the ability to alter directory or file security.			
	F	2.0	**Application Directories & Files** **Objective: To ensure that system level security has been configured to appropriately protect critical application directories and files.**			
	F	2.1	Meet with security / systems administration personnel to obtain an understanding of the controls in place over application directories and files. • Are system / security administrators aware of relevant standards regarding the configuration of security over application directories and files? • Are procedures in place over the configuration of security for application directories and files? • How are access rights for application directories and files determined and assigned? • Who approves access rights for application directories and files?			
	F	2.2	Determine if corporate policies and standards exist regarding the configuration of security over application directories and files.			
	F	2.3	Request reports from security / systems administration personnel which detail the current security settings for critical application directories and files.			
	F	2.3.1	Determine which accounts and groups have been assigned access to the application directories and files.			
	F	2.3.2	Evaluate the appropriateness of the access rights assigned to the identified accounts and groups.			
	F	2.3.3	Determine if universal access (i.e., world, everyone) has been granted to any of the application directories or files.			
	F	3.0	**Production Data Directories & Files** **Objective: To ensure that system level security has been configured to appropriately protect critical production data directories and files.**			
	F	3.1	Meet with security / systems administration personnel to obtain an understanding of the controls in place over production data directories and files. • Are system / security administrators aware of relevant standards regarding the configuration of security over production data directories and files? • Are procedures in place over the configuration of security for production data directories and files? • How are access rights for production data directories and files determined and assigned? • Who approves access rights for application directories and files?			
	F	3.2	Determine if corporate policies and standards exist regarding the configuration of security over production data directories and files.			
	F	3.3	Request reports from security / systems administration personnel which detail the current security settings for critical production data directories and files.			
	F	3.3.1	Determine which accounts and groups have been assigned access to the production data directories and files.			
	F	3.3.2	Evaluate the appropriateness of the access rights assigned to the identified accounts and groups.			
	F	3.3.3	Determine if universal access (i.e., world, everyone) has been granted to any of the production data directories or files.			

PREPARED BY:			AUDIT PROGRAM	Author: Lance M. Turcato		
APPROVED BY:			Logical Security Operating Systems - Generic	Audit Date:_____		
Assigned	Sec.	Sub-Sec.	Audit Step	Date	Ref.	Initials
	G		**REPORTING & AUDITING**			
	G	1.0	**Logging** **Objective: To ensure that appropriate security events are logged to provide security administration personnel with the ability to appropriately monitor system security.**			
	G	1.1	Determine if security / systems administration personnel are aware of corporate standards which exist for the configuration of system audit log facilities.			
	G	1.2	Evaluate the current configuration of the system audit log facilities: • Are appropriate events being logged? ▪ Failed logon attempts ▪ Failed file and object access attempts ▪ Account and group profile additions, changes and deletions ▪ Changes to system security configurations ▪ System shutdown and restarts ▪ Privileged operations ▪ Use of sensitive utilities ▪ Access to critical data files • Are audit entries written to appropriate log files / databases? • Are system audit facilities configured to start automatically during the boot / IPL process? • Are current configurations in compliance with relevant policies and standards?			
	G	1.3	Determine if audit log files are appropriately secured.			
	G	1.4	Determine if audit log files are backed up on a regular basis.			
	G	1.5	Determine if audit log files are archived on a regular basis.			
	G	2.0	**Reporting** **Objective: To ensure that appropriate reports are produced to summarize data recorded in audit logs so that security events may be efficiently monitored on a timely basis.**			
	G	2.0	Determine if security / systems administration personnel are aware of corporate standards regarding security reporting.			
	G	2.1	Evaluate current security reporting processes and procedures: • Are security reports generated on a regular basis? • Are filters utilized to select data from audit log files to generate meaningful and useful security reports? • Are automated reporting facilities active: ▪ Alerts posted to system consoles ▪ Automatic pages for specific security events ▪ Automatic email messages generated for specific security events • Are current security reporting processes and procedures in compliance with relevant policies and standards?			
	G	3.0	**Monitoring** **Objective: To ensure that appropriate processes and procedures are in place to monitor security reports in order to detect security violations and unauthorized changes to system security configurations in a timely manner.**			
	G	3.1	Determine if security / systems administration personnel are aware of corporate standards regarding the review of security audit logs.			

PREPARED BY:			AUDIT PROGRAM	Author: Lance M. Turcato		
APPROVED BY:			Logical Security Operating Systems - Generic	Audit Date:_____		
Assigned	Sec.	Sub-Sec.	Audit Step	Date	Ref.	Initials
	G	3.2	Evaluate current monitoring procedures: • Are generated security reports regularly reviewed by appropriate security / system administration personnel. • Are automated processes in place to monitor security events? • Are procedures in place to analyze trends in security events? • Are current monitoring processes and procedures in compliance with relevant policies and standards?			

Administration & Sign-off Reference

Program Prepared By:_____

Signed:_____

Program Approved By:_____

Signed:_____

Engagement Team (print):	Initials
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____