

Security Risk Assessment		
Control Objectives	Control Technique	Compliance Procedures
DATA CENTERS		
Controls are in place to ensure that the identification and access rights of users as well as the identity of system and data ownership are established and managed in a unique and central manner to obtain consistency and efficiency of global access control.	Is all the computer and telecommunications equipment in a physically secured data center?	Verify that no computer and telecommunications equipment exist outside a secured data center.
	Has the Data Center been assessed for risk?	Access the data center for risk.
	Is access to riser closets adequately controlled?	Determine whether closets are locked and how keys are secured. Evaluate whether only appropriate, authorized individuals possess keys.
	Are the Riser Closets clean and free of miscellaneous equipment?	Perform walk-through of each closet and determine whether closets are neat and clean.
	If a room contains equipment that will be supported by MORE THAN ONE ORGANIZATIONAL ENTITY, is a recorded CCTV camera used to monitor the person entering the room? One exception to this requirement is to have the approved vendor escorted by a department employee for the full amount of time the vendor is in the room. Also, it is important to ensure via the card key entry system, so that he/she cannot enter alone.	
Physical Access Lists and Visitor Logs to the Data Centers		
Controls are in place to ensure that adequate control measures are imposed to safeguard equipment and facilities	Is there an access list posted at the data center entrance?	Obtain current list of employees and verify that access list is up to date. You may need to obtain a list from HR listing all employees who have transferred or left the area to verify whether the list is current.
	Is there a process to review the access list on a quarterly basis to ensure it is current?	Obtain procedures as well as evidence that review was conducted for the last 2 quarters.
	Do only authorized individuals (including authorized employees, consultants, or vendors) have access to the tech/Comm room or data center and do the names of those authorized match the access list posted on the door?	Obtain a listing from the Card Key System and reconcile against an HR listing of employees who have left the area and current vendor/consultant lists who support equipment in the facility.

Control Objectives	Control Technique	Compliance Procedures
	Do documented procedures exist for the admittance and control over visitors to the tech/communications room or data center? NOTE: If an outsourcing agreement exists, then vendor personnel who require access to perform their job are not considered visitors.	Verify the existence of these procedures..
	Do authorized department personnel while working within the secured Tech/Comm room or data center escort all visitors?	Verify that procedures document this requirement and observe process when visitors are present.
	Does a visitors log exist for all non-authorized personnel to sign-in upon entering the tech/Comm Room or data center?	Select 5 completed pages from the log contains the proper verification items.
	Does it require: date of visit, individual's name, purpose of visit, time-in and time-out and initials of employee authorizing the visit?	Verify the date of visit, individual's name, purpose of visit, time-in and time-out and initials of employee authorizing the visit are present on the samples.
	Is management required to review the visitor logs weekly to ensure that logs are complete and do they evidence their review by signing the log in the appropriate space?	Select a 5-page sample from the logbook and verify entries are complete and that there is evidence of management review.
Physical keys, Card keys and Cipher locks		
Controls are in place to ensure that adequate physical security measures are imposed to safeguard equipment and facilities	Is a recorded Card key system used to enter and exit all legacy and new Installations as specified by Corporate Security?	Verify that a recorded Card key system is used to enter and exit all legacy and new Installations as specified by Corporate Security, by observation.
	Is there a process to periodically inventory the card keys to ensure that none have been lost or stolen?	Obtain evidence of most recent card inventory. Spot check items on the list to ensure inventory is complete.
	Is there a process for management to periodically (i.e., at least semi-annually review card key access listings to ensure that only authorized individuals have access to the facility?	Obtain the results from the last review. Ensure all affected areas of management have an opportunity to review the listing.
	Is there a policy that requires management to obtain card keys from terminated or transferred employees?	Obtain procedures and list of employees who have left the area from HR. verify that cards for employees who have left have either been assigned to other users or are deactivated.

Control Objectives	Control Technique	Compliance Procedures
	Are unused card keys kept in a secured location and kept in a deactivated state?	Meet with security personnel to determine where cards are secured. Review card list or card key system itself to determine whether cards are deactivated. Record observation.
	Does the facility have a fail-safe design or manual override capability if the Card Key Access System fails?	Verify the existence of the fail-safe through observation or documentation from the manufacturer.
	If a cipher lock is used, Compensating controls must be used. Is there a process for management to periodically (i.e., at least semi-annually) review cipher lock access listings to ensure that only authorized individuals have access to the facility?	Obtain the results from the last review. Ensure all affected areas of management have had an opportunity to review the listing.
	Does a procedure exist to change the cipher lock at least quarterly or when an employee leaves the area?	Verify the existence of the procedure stating these controls.
	Is the key to change the cipher lock combination kept in a secured location (i.e., Tele-key box or safe)?	If key is in the Tel-key box, answer facilities – Tele-Key box Section.
	Is a logbook of cipher lock changes kept?	Verify that changes were made quarterly or when an employee left, by reconciling with a HR listing of employees who have left the area. Verify that all log entries are complete.
	Does the facility have a fail-safe design or manual override capability if the cipher lock system fails?	Verify the existence of a fail safe or manual override through observation or documentation from the manufacturer.
	Is the access to the Tech/Comm Room or data center controlled through the use of physical keys?	
	Is there a list of individuals who have keys to the facility and is it appropriate for all those on the list to have these keys?	Verify with management that the appropriate individuals have keys.
	Is a Tel-key box used by the facility to secure keys and/or passwords to sensitive ID's?	If you determine through the course of your review that a Tel-key box is needed, then record this as an issue as well.
	Is the Tel-key box under dual control?	Observe the process to open the box. Obtain a list of individuals who possess these keys and their location. Make sure that one individual cannot dominate the entry process.

Control Objectives	Control Technique	Compliance Procedures
	Is there an inventory of items inside the Tel-key box?	Obtain inventory and sample items in Tel-key box to ensure that the inventory is current.
	Is there a logbook to record what is removed and returned to the Tel-key box? Does the logbook contain Date, Time, Reason for removal including Trouble ticket #, and the initials of both individuals who opened the Tel-key box to remove the item?	Remove 3 completed pages from the log. Verify completeness of columns & entries. Select 6 entries from sampled pages & trace to trouble ticket # or other authorizing paperwork.
	Does management review the Tel-key log monthly to ensure that entries are complete and is there evidence of such a management review?	From 3-page sample, ensure that a management review was performed monthly.
	Is the Tel-key box process documented in a procedure manual?	Verify that the Tel-key Box procedures are documented in the procedure manual.
	If Tech/Comm room is shared among multiple business units and/or vendors, is equipment kept in a locked cabinet? Are keys to these cabinets secured?	Spot check several cabinets and verify that cabinets are locked. Determine controls over cabinet keys.
Passwords		
Passwords, tokens, or other devices are used to identify and authenticate users	Are Password: <ul style="list-style-type: none"> • Unique for specific individuals, not groups; • Controlled by the assigned user and not subject to disclosure; • Changed periodically – every 30 to 90 days; • Not displayed when entered; • At least 6 alphanumeric characters in length; • Prohibited from being shared, and • Prohibited from reuse for at least 6 generations? 	Review pertinent policies and procedures. Interview users. Review security software password parameters. Observe users keying in passwords. Attempt to log on without a valid password; make repeated attempts to guess password. Assess procedures for generating and communicating passwords to users.
	Is the use of names or words prohibited?	Review a system-generated list of current passwords. Search password file using audit software.
	Are vendor-supplied passwords replaced immediately?	Attempt to log on using common vendor supplied passwords. Search password file using audit software.

Control Objectives	Control Technique	Compliance Procedures
	Are generic user Ids and passwords used?	Interview users and security managers. Review a list of IDs and passwords.
	Are password protected screen savers used on all desktop computers?	Verify password protected screen savers are installed and locking out within a specified time period on all desktop computers by sampling them for compliance.
	Are attempts to log on with invalid passwords limited to about three attempts?	Repeatedly attempt to log on using invalid passwords. Review security logs.
	Are personnel files automatically matched with actual system users to remove terminated or transferred employees from the system?	Review pertinent policies and procedures. Review documentation of such comparisons. Interview security managers, Make comparison using audit software.
	Are password files encrypted?	View dump of password files (e.g., hexadecimal printout).
	For other devices, such as tokens or key cards, do users: <ul style="list-style-type: none"> • Maintain possession of their individual tokens, cards, etc, and • Understand that they must not loan or share these with others, and must report lost items immediately? 	Interview users: To evaluate biometrics or other technically sophisticated authentication techniques, the auditor should obtain the assistance of a specialist.
Network Management Systems (NMS)		
Network Management Systems (NMS)	Are all terminal access methods (i.e., dial-in, LAN, hard-wired) for the NMS listed?	Obtain dial-in access list for all NMS in use. Compare list against each NMS configuration.
	Is there a description of each NMS and are the networks they support documented in the procedures?	Each NMS in use must have written procedure for designated network. Operational procedure should be in PCM manual.
	Are all network control and monitoring systems in a physically controlled area?	Ensure that physical security to Network control and monitoring systems approved by manager. Check access list to controlled area against organization chart.

Control Objectives	Control Technique	Compliance Procedures
	If dial-in access is allowed to the NMS, are dial-in access controls in place (e.g., manual log or callback security)?	<p>If the remote dial-in access to NMS is allowed. Operations personnel must have:</p> <ul style="list-style-type: none"> ▪ Ready access to the list of network User ID's, location, and telephone contact number. ▪ The facility to rapidly disable any individual network User ID. Maintain current log for all dial-in access activity. Systems must have unlisted phone numbers.
	Are security administration procedures (i.e., ID creation, review of security, violation monitoring, emergency access, and periodic review of entitlements) in place for each network management system?	Review procedures.
	Is a segregation of duties maintained between the individuals performing the security administration for each NMS and the individuals performing the network management and monitoring functions?	Look at ACL's to determine if security and system administration function is segregated.
	Are the NMS privileges of individuals in the area under review appropriate for their job function?	Review organization chart with roles and responsibilities.
	Are NMS Ids shared by more than one operator or technician?	Look at user ID file to determine if generic Ids exist.
	If shared Ids are used, is it because legacy systems are used where separate Ids are not technologically feasible? Or, are the Ids, which are shared used solely for monitoring purposes, and have read or inquiry access only?	See above
Security Software		
Logical Controls over Data Files and Software Programs	Is security software used to restrict access?	Interview security administrators and system users.
	Is access to security software restricted to security administrators only?	Review security software parameters.
	Are computer terminals automatically logged off after a period of inactivity?	<p>Observe terminals in use.</p> <p>Review security software parameters.</p>

Control Objectives	Control Technique	Compliance Procedures
	Are inactive user accounts monitored and removed when not needed?	Review security software parameters. Review a system generated list of inactive logon IDs, and determine why access for these users has not been terminated.
	Do security administration personnel set parameters of security software to provide access as authorized and restrict access as authorized including access to data files, load libraries, batch operational procedures, source code libraries, security files, and operating system files?	Determine library names for sensitive or critical files and libraries, and obtain security reports of related access rules. Using these reports, determine who has access to critical files and libraries and whether the access matches the level and type of access authorization.
DBMS		
Logical controls over a database	<p>Have database management systems (DBMS) and data dictionary (DD) controls been implemented that :</p> <ul style="list-style-type: none"> • Restrict access to data files at the logical data view, field, or field-value level; • Control access to the DD using security profiles and passwords; • Maintain audit trails that allow monitoring of changes to the DD; • Provide inquiry and update capabilities from application program functions, interfacing DBMS or DD facilities? 	<p>Review pertinent policies and procedures.</p> <p>Interview database administrator.</p> <p>Review DBMS and DD security parameters.</p> <p>Test controls by attempting access to restricted files.</p>
	Is the use of DBMS utilities limited?	Review security system parameters.
	Are access and changes to DBMS software controlled?	Review procedures and change control documentation.
	Is the access to security profiles in the DD and security tables in the DBMS limited?	Review procedures for access.
Network Management Systems (NMS)	Are network topology diagrams current for each network that supports the production environment?	Review each network topology and verify accuracy of the information against the actual network configuration. Use management system data for verification and cross-referencing.
	Are detailed network circuit diagrams current?	Sample 10% of network circuits. Choose several linkages from the topology diagrams and trace diagrams to the physical equipment, Check for Demark ID's, modems, cable switching equipment, label ID's, cabinet ID's, servers, router, etc.

Control Objectives	Control Technique	Compliance Procedures
Remote Access		
Logical controls over telecommunications access	Are dial-in phone numbers published and are they periodically changed?	Review pertinent policies and procedures. Review documentation showing changes to dial-in numbers. Review entity's telephone directory to verify that the numbers are not listed.
Dial Backup (DBU)	Are all Dial Backup lines that are defined to the network listed?	Obtain a list of DBU lines for use by interviewing management.
	Do procedures exist for authorizing, invoking, monitoring and testing dial backup for certain portions of the network?	Obtain procedures and ensure that procedures address all concerns.
Control Objectives	Control Technique	Compliance Procedures
Remote Access	If session level encryption is used (e.g., IRE) and activation is dependent on some type of physical connection, are users prohibited from gaining access via alternate means (i.e., different phone numbers)?	Obtain reports from management system to identify user listing, devices, application names and unauthorized access activity. Check if trouble tickets are opened for illegal connections.
	Is dial-in access to all production resources restricted to authorized personnel via either challenge response, dynamic password exchange, and approved cryptographic techniques, or emergency procedures, which incorporate compensating controls?	All personnel, consultants, and vendor dial-in access should use dynamic password tokens (i.e. SecureID, DESGOLD, etc.) cards for user authentication use.
	Are all Internet gateways to and leased lines interfacing with external networks are protected by a firewall?	Verify that backbone networks and business supported LAN's and WAN's protected by firewalls. Firewalls must be configured to provide; user identification, destination screening, and service restrictions (i.e. Telnet, FTP)
	Does an inventory exist of the dial-in devices, which includes their location?	Access to the network, User ID, location and telephone contact number must be documented.
	Does a formal process exist to request dial-in access, which requires supervisor or business relationship approval?	Procedure must be in place regardless of whether the dial access facilities are owned and operated by the internal organization, or by external service provider. Verify procedures for approved dial-in access.

Control Objectives	Control Technique	Compliance Procedures
	If private or public dial-in access is being used, how is this access tracked and controlled?	Obtain reports to validate dial-in access. Reference to Information Security Admin reports to identify failed attempt and unauthorized access. Obtain violation-logging records for verification.
Encryption and Related Applications		
Cryptographic tools	Have cryptographic tools been implemented to protect the integrity and confidentiality of sensitive and critical data and software programs?	To evaluate cryptographic tools, the auditor should obtain the assistance of a specialist.
Transaction Authorization	Do policies exist to ensure that where appropriate, controls are implemented to provide authenticity of transactions? This requires use of cryptographic techniques for signing and verifying transactions?	Review policies to determine if they exist for authenticity of transactions.
Cryptographic Key Management	Are the physical and logical encryption keys secured under dual control?	Review dual control procedures of logical and physical encryption keys. Some encryption devices have physical keys; others have a module that plugs into the unit to change the logical keys. Key A and B must be separated and maintained by two different party or people. This procedure applies to internal or external controls.
	Are encryption devices properly locked and are physical keys removed from the units?	Select cabinets with encryption devices installed. Each Tag must have, encryption unit #, CKT ID. Unused keys must be Tagged. Verify if encryption devices locks are in locked position and physical keys in Telkey box.
	If encryption keys are automatically changes, are alarms/events in place to notify management when devices are inoperable or set to the bypass mode?	Review encryption devices management system alarms events for unsuccessful DAILY key exchange or BYPASS conditions. Devices that are not connected to management system the above events can be obtained directly from unit. Look into encryption management option. Evidence must be signed and dated by manager. Note: each unit can store up to 99 events, then buffer is over written with new data.

Control Objectives	Control Technique	Compliance Procedures
	Is the organization notified within a designated number of hours whenever a particular device is placed in bypass mode?	Reference: to SLA for user notification process. Memo or trouble ticket should be used for notification if required. Verify if user has requested this type of service.
	Are alarms reviewed in real time? Are procedures in place for performing this review?	Institute procedure to review alarms in real time and develop review process. Manager signature and date must exist. If check off list is utilized, verify if all major alarms are displayed in real time and corrective action taken for each event.
	Does the cryptographic key distribution methodology in place comply with the ANSI X9.17 and X 9.24 standards?	DES is approved standard.
	Is master key encryption keys change procedure documented and in place?	Management must sign logs. Review procedure for MASTER key encryption generation, distribution scheme and records keeping. Reference to vendor manuals for detail process. For manual device key must be changed at least once a year. Devices that utilize management system key can be distributed automatically.
	Do the encryption devices that have manual key exchanging features use tamper proof encryption key transportation and storage device?	Logs must be dated and signed by management. Cryptographic hardware must be tamper proof as specified in Federal Information processing Standards (FIPS) 140-1. Information must be protected from unauthorized access and have automatic erasure,
	Are all data that requires protection encrypted for all systems that process sensitive information?	Standards require encryption over all links that transmit this type of data through which any bank transaction is transmitted. Identify supported business with sensitive information to ensure if restricted and Confidential data is secured. Reference to risk level analysis or SLA documentation if available.
	Do you maintain a list of encrypted and unencrypted circuits and which businesses each circuit supports?	Reference to SLA for encryption requirement and data owner responsibility. Obtain encrypted and unencrypted circuits inventory list. Identify which businesses are not compliant. Verify encrypted circuits supported businesses.

Control Objectives	Control Technique	Compliance Procedures
	Are ALL network data transmissions that leave government property (including cases where government personnel do not occupy contiguous floors of a building) encrypted?	Identify data circuits that transmit through non-government owned property or floors. Contact businesses and obtain approval of exposure.
	Are all default encryption keys changed that are provided by the vendor? Are these keys changed after each new software release?	Examine encryption devices configuration against standards.
	Do policies exist for ensuring that, where appropriate, transactions cannot be denied by either party, and controls are implemented to provide non-repudiation of origin or receipt of transactions? This can be implemented through digital signatures, time stamping and trusted third parties.	Review policies relating to digital signatures.
Monitoring		
Audit trails are maintained	In all activity involving access to and modifications of sensitive or critical files logged?	Review security software settings to identify types of activity logged.
Actual or attempted unauthorized, unusual, or sensitive access is monitored.	Are security violations and activities, including failed logon attempts, and sensitive activity, reported to management and investigated?	Review pertinent policies and procedures. Review security violation reports. Examine documentation showing reviews of questionable activities.
Suspicious access activity is investigated and appropriate action taken	Do security managers investigate security violations and report results to appropriate supervisory and management personnel?	Test a selection of security violations to verify that follow-up investigations were performed and to determine what action were taken against the perpetrator
	Are appropriate disciplinary actions taken?	Review procedures and interview personnel responsible for monitoring of activity.
	Are violations summarized and reported to senior management?	Interview senior management and personnel responsible for summarizing violations. Review any supporting documentation,
	Are access control policies and techniques modified when violations and related risk assessments indicate that such changes are appropriate?	Review policies and procedures and interview appropriate personnel. Review any supporting documentation.

Control Objectives	Control Technique	Compliance Procedures
Security Surveillance	Is all sensitive activity performed by highly privileged accounts monitored for access and maintenance activity?	Verify that there is an appropriate audit trail produced whenever a highly privileged account is used. There should be a traceable trouble ticket opened for each usage and associated audit trail logs outlining the use and appropriate signatures showing concurrence for the use.
Datascope and Sniffers		
Network Monitoring	Is software sniffer technology in use?	Determine local policies. If in violation, record an issue.
	Are there procedures governing the use of hardware sniffers and/or datascope?	Obtain procedures and determine whether controls are included by answer the following several questions.
	Does management on a daily basis to ensure usage is justified review the log or audit trail?	For the samples previously selected, verify that a management review was performed.
Hub Management		
Hub Management	Has a management tool been installed on all Hubs?	Verify that SPEL, HUB management tool has been installed.
	Is "Security" turned "On" for all ports on each HUB's? Configure Hubs with X-disabled ports; X-Send Trap; Define MAC address on all HUB ports?	Ensure that "Security has been turned "On" for all ports on all HUB's. Configuration must have the following settings: X-disabled ports; X-Send trap; X-Lock Ports; Define MAC address on all HUB ports.
	Is a process in place to update HUB inventory?	Verify if HUB inventory process has been developed and implemented.
	Is inventory in place for all physical Hubs and configured ports?	Verify inventory list for all Hubs and check active ports.
Voice Operations		
System-Related	Are maintenance ports configured to prevent direct access from an external line?	Obtain the PBX configuration listing. In addition, try to access the maintenance ports from an outside line. If answer is no, record as comment.
	Are lines that are used for maintenance ports configured through a central office and do they have a different prefix than the regular phone numbers.	Obtain a listing of the maintenance ports modern numbers. If numbers have the same prefix, record as a comment. Review modem technical description and access line information.
	Is invalid access to the maintenance ports tracked and reviewed on a real-time basis? Access to maintenance ports provides the greatest level of access to the system and offers the most potential for abuse.	If system has been outsourced, obtain letter from vendor and vendor's process/ Procedure for performing this function. If system is not outsourced and answer is no, record as a comment. Review PBX maintenance and monitoring procedures.

Control Objectives	Control Technique	Compliance Procedures
	<p>Is there a process to ensure that all systems are backed up at a minimum of every 30 days and does it include:</p> <ul style="list-style-type: none"> ▪ Backup whenever a major system configuration is completed. ▪ (2) copies of backup made with one stored onsite and one offsite? ▪ Backup Tapes are write protected. 	<p>If no, record as comment. Review Copy of process and procedures.</p>
	<p>Is access to the maintenance function limited to administrators on a need to have basis? Unauthorized access to this function can compromise the switch parameters to potential hacking activity.</p>	<p>If outsourced, answer with N/A. If not outsourced, obtain a listing of PBX maintenance users and verify that access is essential. If answer is no, record as a comment. Request a copy of vendor certifications of training,</p>
	<p>Do all PBX administrators have their own maintenance ID's and pass-words and are they certified for access to the switch by the vendor? Untrained/uncertified administrators can provide the potential for unwanted parameters leading to potential incidents of toll fraud.</p>	<p>If answer is no, record as a comment.</p>
	<p>Are all administration/Maintenance terminals providing access to telephone system secured at all times? Are terminals logged off when left attended</p>	
	<p>Is there a process for HR to notify site management of terminated/resigned employees? This is necessary in order to notify the appropriate management of accounts (voice mail and telephone) which need to be terminated.</p>	<p>Check procedure and verify documentation is received of terminated and/or resigned employees. If not, record as comment and obtain procedures of how management is notified. Request listing from HR and sampling of activity for terminated employees.</p>
Trunking Configuration	<p>Is trunking feature "trunk-to-trunk" activated?</p>	<p>If answer is yes, record as a comment. If yes, review the procedures for managing trunk-to-trunk. Review PBX Configuration printout</p>

Control Objectives	Control Technique	Compliance Procedures
	Are trunk access codes (TAC) disabled and only enabled for testing purposes, including TAC access to Tie Trunks (if more than one PBX in complex)?	<p>Allowing TAC access to tie trunks on your switch may give the caller access to the Trunk Verification feature on the switch. If not properly administered, a caller may be able to dial 9 or the TAC's in the other switch. Toll hackers can choose a menu option that allows an extension number that provides access to an outside line.</p> <p>Check the PBX configuration files for the presence of Trunk Access Codes. If answer is no, record as comment.</p>
	Is all Direct Inward System Access (DISA) that allows an external caller to gain access to the PBX system features or trunks, functionality disabled? Remote access to these features may result in toll fraud and system abuse.	Check the Class of Service (COS) to verify that DISA is disabled. If answer is no, record as comment. For Lucent Definity G3 type switches, the COS table will have no reference to DISA, UNLESS it is enabled.
	Is access to any known "pay per call" service restricted (i.e., 900, 976, selected 809)? Access to these numbers may cause unwarranted or fraudulent charges.	Check the ARS Table to verify that the numbers are restricted. If the answer is no, record as comment.
	Does the PBX, except for COB purposes restrict codes used for alternate long distance carriers? If not controlled, hackers can dial out by using carrier codes that bypass touting restrictions placed on primary carrier.	Check the PBX configuration files for long distance carrier restrictions. If answer is no, record as comment.
	Is the PBX set up so that the long distance carrier of choice (e.g. AT&T in the US) is the primary carrier for all long distance calls? And are secondary carriers only used in the event of an outage of the primary carrier.	Obtain telephone bills and verify that no calls are charged except for a MCI 9example) emergency. If answer is no, record as comment.
Class of Service (COS)/Class of Restriction (COR) Configuration	Do semi-annual reviews of the COS levels and CORs take place in light of changing business requirements, improved carrier services, systems usage, and organizational re-engineering? This is necessary to insure that excessive entitlements do not exceed requirements of business, resulting in conditions that may lead to system abuse.	Select a sample of added, changed and deleted subscribers and verify procedures are being followed and executed in a satisfactory and timely manner. Determine date of last review of CORs and COS with business and verify review. If answer is no, record no comment.

Control Objectives	Control Technique	Compliance Procedures
	Is external call forwarding disabled from all COS', including Fax Machine/Modem COS? This prevents a user from forwarding an extension to an outside number.	Check the COS to verify that internal call forwarding is allowed. In addition, test the controls by trying to call forward a phone to an outside number. If answer is no, record as comment.
	Are Privileged Abbreviated Dialing Group Lists present on the PBX? These numbers can be used to bypass any COS restrictions and should be restricted to only authorized business related numbers.	Check the PBX configuration files for the presence of speed dialing numbers. If answer is yes, record as comment.
	Is access to the outside operator (0,00,01,011,411,1411,611,1611, 555-1212 and xxx-555-1212) restricted? This is to prevent an operator from connecting a call through to another number.	Check the Class of Service (COS) tables, Class of Restriction (COR), Automatic Route Selection (ARS) Tables, and the Facility Restriction Levels (FRL's) to verify that operator access is not allowed. If present, record as comment.
	<p>Are publicly-accessible phones restricted as follows:</p> <ul style="list-style-type: none"> ▪ To placing 911 and internal calls ▪ Call-forwarding deactivated? 	If answer is no, record as comment.
	<p>Are publicly-accessible phones used to request admittance into a secured area restricted as follows:</p> <ul style="list-style-type: none"> ▪ To placing 911 and internal calls ▪ Call-forwarding deactivated? 	If answer is no, record as comment.
	Is long distance dialing capability restricted during off-hours? This is a prime time for hackers and other users to abuse the system.	If answer is no, record as comment.
	Are calling cards or authorization codes used after-hours for long distance access if the area in question is not a 24-hour operation?	If answer is no, record as comment.
	Are authorization codes printed in CDR by employee number? If obtained by unauthorized personnel would authorization codes open up those codes to toll fraud?	If listed in CDR by authorization number list as comment.

Control Objectives	Control Technique	Compliance Procedures
	<p>Are group accounts or generic account authorization numbers used for visitors? Generic or group accounts prevent accountability by individuals of toll charges.</p>	<p>If yes, list as comment as the CDR report could not identify individual's long distance charges.</p>
	<p>Are there procedures for managing Authorization (Auth) Codes assigned within system? Do they cover the following:</p> <ul style="list-style-type: none"> ▪ All domestic long distance and international calls require an Auth Code. ▪ Auth Codes are disabled and new code issued when compromise is suspected and/or confirmed. ▪ Auth Codes are disabled and new code issued when employee/temp, etc., leaves the bank or relocates to another location. ▪ Auth Codes must be hand-delivered or sent through registered mail to requesting party, not sent through e-mail, interoffice mail, delivered via telephone, etc. ▪ No "spare" Auth codes are to be activated. 	<p>If no, list as comment.</p>
Call Management System	<p>Is there a process to manage changes to the CMS system that contain:</p> <ul style="list-style-type: none"> ▪ Only system administrator or back-up control all write access to VDN's, vectors, and splits. ▪ CMS system is partitioned to allow this level of control. ▪ Deviations are on file for those areas requiring write access to these features and are renewed yearly. 	<p>If CMS is installed and answer is no, record comment. Review copy of CMS procedures, configuration and identify deviations.</p>
Voice Mail System	<p>Does the Voice Mail system require an 8-digit password/pin? Voice mail accounts must be password protected to prevent unauthorized access to user voice mail system.</p>	<p>Obtain the Voice mail configuration file printout and verify. If answer is no, record as a comment.</p>

Control Objectives	Control Technique	Compliance Procedures
	Does the Voice mail system disconnect a caller attempting to access the system after 3 valid PIN attempts are made (within 1 hour for Octel Voice Mail Systems)? If fraudulent use is suspected, notify vendor and insure SDT is notified when the mailbox is disabled.	Test the feature by trying to log in with 3 successive invalid PIN's. If unauthorized access is suspected, notify vendor and await assurance that box has been disabled.
	Are new Voice mail accounts set up with an initial PIN which is unique and which is not the same as the individuals phone extension.	Review the Voice Mail configuration procedures for PIN initialization procedures. If no procedures exist, as the Voice Mail technician. Test new mailboxes by attempting to access with extension number. If voice mailbox can be accessed, record as comment.
	Does the Voice Mail system prohibit external call capability? This prevents a caller from dialing out through the PBX, thus causing Citibank to pick up the tab for long distance calls. (Except on Octel Voice Mail Systems for Citifax, Pager Notification and Voice Mail System Networking)	Obtain the Voicemail configuration file printout and verify. If answer is no, record as comment.
	Does the Voice mail system detect uninitialized mailboxes? And does the system manager remove them after 45 days?	Review site's procedures for uninitialized mailboxes. If answer is no, record as comment.
	Is there a Call detailing reporting system installed to keep track of length of calls and designation?	If answer is no, record as comment. Review Call detail report & configuration.
	Is the CDR system logging and tracking for adequacy the following: <ul style="list-style-type: none"> ▪ All calls over 15 minutes ▪ Off hour and holiday usage ▪ Calls over certain dollar amounts 	If answer is no, record as comment.
	Are CDR reports reviewed by management every month or whenever an apparent problem occurs (i.e., sudden increase in the number of calls)? Would failure to provide supported businesses with CDR reports disable businesses with a prime management tool to control costs and prevent possible fraud or system abuse?	Obtain copies of old reports and look for signoff. If no, record as comment.

Control Objectives	Control Technique	Compliance Procedures
	Does a Contingency plan exist for the PBX? Does it address the issues outlined in the Continuity of Services and Operations questionnaire?	If no, record as comment. Review copy of site COB Plan
	<p>Are Emergency Bypass Phones installed at site and are they installed as follows:</p> <ul style="list-style-type: none"> ▪ Phones are connected to non-PBX lines, i.e., CO/DOD, 1FB/1MB, or Centrex lines. ▪ Allow full range of out-dial access except for 900, 976 and international calling. 	If no, record as comment. Review copy of Emergency Bypass Phone configuration, including location of all phones, and procedures.
Miscellaneous	<p>Is there a process for producing and reviewing system error reports and logs for:</p> <ul style="list-style-type: none"> ▪ Review on daily basis. ▪ Unauthorized access attempts ▪ Multiple invalid password attempts ▪ High rates of usage 	If no, record as comment.
Policies & Procedures	Is an up-to-date Voice Policy and Procedure Manual (PCM) in place and in use?	Check the Voice PCM and insure policies and required reviews are up to date.