Audit Area and Objective	Test Procedure	Test Result	Work Paper Reference	Gap Analysis
1. Organization and Management Policies Objective: Organizational policies and management procedures should be in place to enable the IT function to be controlled properly.	1.1 Determine if the overall responsibility for the IT function has been allocated to a board director or senior manager.			
	1.2 Determine if there is a formal IT structure with reporting hierarchy and job responsibility descriptions.			
	1.3 Determine if there is an IT Steering Committee. If so determine how often they meet and what documentation exists.			
	1.4 Determine if there is a formal IT strategy covering the next 1-3 years. If so determine what documentation exists.			
	1.5 Determine if there is a formal IT budget showing planned hardware, software, and development costs. If so determine what documentation exists.			
	1.6 Assess whether adequate procedures exist to evaluate significant IT investments. If so determine what documentation exists.			
	1.7 Determine that current versions of operating and application systems software are installed.			
	1.8 Determine if a formal Information Security policy exists and is enforced.			

Audit Area and Objective	Test Procedure	Test Result	Work Paper Reference	Gap Analysis
	1.9 Determine if the security policy is supported by documented standards and procedures. Consider: o Security hardware and software implementation o Responsibility for monitoring or updating o Internal Audit involvement o Areas covered o Distribution to technical staff o End-user agreement distribution			
	1.10 Determine whether there is a security committee, or similar body, responsible for establishing, maintaining and reviewing security standards and guidelines.			
	1.11 Determine if there is a security administration function. Consider: o Organization chart o Duties and responsibilities o Training or experience o Segregation of administration and monitoring roles			
	1.12 Determine if documentation of any end-user computing policies exists.			
	1.13 Assess whether a data ownership policy has been established and issued to management and staff.			
	1.14 Determine what formally documented standards and procedures exist covering all IT functions. Consider: o Scope and coverage o Dates when documents were issued or last updated o Policy regarding hardware and software			
	1.15 Determine if the organization is complying with the IT aspects of statutory and			

Audit Area and Objective	Test Procedure	Test Result	Work Paper Reference	Gap Analysis
	regulatory requirements.			
	1.16 Determine the extent to which there is an Internal Audit department. Determine if there is an internal audit policy document.			
	1.17 Determine if there is an internal computer audit function. Assess whether IT issues are subject to independent review by the Internal Audit function.			
	1.18 Determine how the organization identifies its present and future IT manpower and skills requirements.			
	1.19 Determine if there are training and development plans to ensure that staff are suitably skilled in the use and control of IT and that IT staff are aware of the business activities and systems. Determine if IT staff has performance appraisals.			
	1.20 Determine what requirements exist for the hiring of appropriately skilled IT staff.			
	1.21Determine if background checks are required for all employees.			
	1.22 Determine if there are any consultants or contractors working long term at the site.			
	1.23 Determine if confidentiality agreements are required for all employees, consultants, and contractors.			
	1.24 Determine if there is a disciplinary process for employees that violate policies.			
	1.25 Determine if formal dismissal procedures exist.			
	1.26 Determine if a hardware and software inventory exists.			

2. Segregation of Duties <u>Objective:</u> Segregation of duties for staff, both within the IT Department and user functions, should be adequate to prevent and/or detect error or irregularities.	2.1 From the organization chart and job descriptions assess whether segregation of duties within the IT Department is appropriate for the size of the organization. Consider: o Number of IT staff o Systems administrators o Systems developers/programmers o Database administrators o Data Center Operations o Network security o Reliance on key personnel o Reliance on contract staff			
	2.2 Determine if IT staff only has responsibilities for functions within the IT Department. Consider: o Responsibility for initiating or authorizing transactions o Custody of valuable or moveable assets o Amendments to master files o Correction of input errors.			
	2.3 Assess whether staff with programming expertise are segregated from the users who are controlling the systems. Determine if developers have access to production environments.			
	2.4 Determine if a data classification scheme is in place. Assess whether Owners, Custodians, and Users of Information Systems are defined in the supplier's organization with clear-cut roles and responsibilities.			
	2.5 Assess whether data owners are responsible for data classification based on its sensitivity and predetermined protection priorities.			
	2.6 Assess whether sensitive information in all of its forms is labeled as to its sensitivity.			

Audit Area and Objective	Test Procedure	Test Result	Work Paper Reference	Gap Analysis
3. Logical Access Controls Objective: Data files, application programs and/or operating systems should be accessed and/or amended with appropriate authority.	3.1 Determine if sensitive data and applications have been identified.			
	3.2 Determine if appropriate security measures have been implemented to restrict users' access to data and programs.			
	3.3 Determine if development staff are prevented from accessing data and software in the production environment.			
	3.4 Determine if unique user IDs and passwords are assigned to each user. Determine if any accounts are shared.			
	3.5 Determine if strong password controls are in place. Consider: o Password requirement o Password maximum age o Password minimum age o Password minimum length o Password history o Password lockout on incorrect entry o Password lockout duration o Password complexity requirement			
	3.6 Determine if Root, Domain Administrator, Local Administrator, and System Administrator passwords are changed on a regular basis.	o		
	3.7 Determine if the allocation, authorization, and use of powerful user ids or passwords are controlled and monitored. Determine to whom these ids/passwords are assigned.			
	3.8 Determine if there is a documented procedure to ensure passwords are issued			

Audit Area and Objective	Test Procedure	Test Result	Work Paper Reference	Gap Analysis
	and changed in a controlled manner.			
	3.9 Determine if documented procedures exist for the creating and disabling/deleting of user accounts.			
	3.10 Determine if user access rights are reviewed periodically. Assess if employee access rights are changed when they are relocated internally.			
	3.11 Determine if password files are encrypted and access to copies of the password files are highly restricted (backup tapes, recovery disks).			
	3.12 Determine if dial-up modems are properly controlled and restricted. Assess if passwords and logging are enabled.			
	3.13 Determine if logging, monitoring, and alerting are in place at network, operating system, database, and application levels. Determine if security events, especially failures are captured and reviewed.			
	3.14 Determine if idle terminal timeouts are locking screen savers are mandatory or voluntary.			
	3.15 Determine if logon banners are in place at network, operating system, database, and application levels.			
	3.16 Determine if encryption is in use for data transfer (i.e., data in motion). Determine if encryption is in use for data storage (i.e., data files or database columns, data at rest). If so determine the version, key size, and algorithm in use.	○		
	3.17 Determine if supported versions of hardware and software are in use at network, operating system, database, and application levels.			
	3.18 Determine if patch maintenance procedures exist and are enforced at network, operating system, database, and application levels.			
	3.19 Determine if hardening procedures exist and are enforced at network, operating system, database, and application levels.	○		
	3.20 Determine if end users are restricted from gaining access to sensitive or customer data. Determine if end users are restricted from			

Audit Area and Objective	Test Procedure	Test Result	Work Paper Reference	Gap Analysis
	gaining inappropriate access through file permissions, access control lists, or role based access controls.			
	3.21 Determine if end users are restricted from using utility programs capable of amending or deleting live data. If allowed determined if the use of utilities on live data is authorized and documented.			
4. Physical Access Controls Objective: The risk of accidental or malicious damage to, or theft of, computer equipment and removable media should be adequately controlled.	4.1 Determine if the site has a perimeter fence erected.			
	4.2 Determine if access to the site is controlled and monitored. Consider: o Security gatehouse o 24-hour security guards o Regular patrols o Security cameras and how long they store information before overwriting o Use of identity and access badges o Alarm systems			
	4.3 Determine if IT infrastructure (i.e., data center, wiring closets, circuit feeds, wireless access points) is concentrated near the exterior or interior of the facility.	o		
	4.4 Assess whether the security of the building is appropriate to the activities of the organization.			

Audit Area and Objective	Test Procedure	Test Result	Work Paper Reference	Gap Analysis
	4.5 Determine if control measures are in place to ensure that only members of staff or authorized visitors are on the premises. Consider: o Visible identity and access badges o Issue of passes or badges to visitors o Visitors are accompanied by a permanent staff member o Security awareness of staff; i.e., to challenge unescorted visitors o Record maintained of all visitors o After-hours access			
	4.6 Determine if there are any unattended access points, and what procedures are in place to restrict access from such points.			
	4.7 Assess whether specific authority is required for staff to remove computer equipment or media from the building.			
	4.8 Determine if access to the computer room is restricted to authorized persons. Consider: o Record of visitors o Use of access-control devices o Controls to prevent misuse of the access system o Logging and alerting for access control adherence and violation o Access restrictions to different areas o Requirement for visitors to be accompanied			
	4.9 Determine if access to particularly sensitive areas (e.g., telecommunications area) is further restricted.			
	4.10 Determine if master system consoles and other critical terminals are located in the computer area.			
	4.11 Determine if the main power supply in the building is restricted to authorized personnel only. Determine if alternative power supplies are available (i.e., UPS, generator). If so determine how long they will last in a contiguous power outage.			

Audit Area and Objective	Test Procedure	Test Result	Work Paper Reference	Gap Analysis
	4.12 Determine what controls exist to prevent the loss or disruption of communications (e.g., secure cable pits, locked PBX room, etc.). Verify access to cable risers, distribution boards, PBX rooms, etc., is controlled.			
	4.13 Determine if service maintenance visits are scheduled, authorized and, as far as possible, monitored. Determine if cleaners and service staff are required to sign in/out of the building and computer areas. Determine if cleaners are accompanied when in computer areas.			
	4.14 Determine if person traps are in place at the entrances to the computer areas to reduce the likelihood of unauthorized access.			
	4.15 Determine if appropriate environmental controls have been implemented both within the building and within the computer areas. Consider: ○ Fire prevention or detection systems (what type) ○ Air conditioning ○ Humidity controls ○ Raised floor ○ Power conditioning and UPS	○		
	4.16 Determine if adequate environmental monitoring and alerting are in place. Consider: ○ Fire/smoke alarms ○ Temperature/humidity alarms ○ Water leak detection and alerting ○ Power outage detection and alerting ○ Motion detectors ○ Video cameras with significant recording times	○		
	4.17 Determine if backup tapes are properly secured and stored in fire rated data safes.			
	4.18 Determine if computer data, media, and documentation are adequately secured. Determine if such items are loose or in locked cabinets or data safes.			

Audit Area and Objective	Test Procedure	Test Result	Work Paper Reference	Gap Analysis
	4.19 Determine if writeable storage media is disposed of securely and safely when no longer functional or required. Determine if media, including defective hard disk drives, are allowed to leave the firm without being properly destroyed.			
	4.20 Determine if paper shredders are available at this location. Determine if office paper that is removed in bulk is shredded by a third party before disposal or recycling.			
	4.21 Determine if fire precautions and instructions on what to do in the event of a fire are posted in all departments. Determine if fire drills are held regularly.			
	4.22 Determine if fire-fighting equipment is regularly serviced. Determine if the staff is trained on how to use the equipment.			
5. Systems Development and Change Management Controls Objective: System development and program changes should be authorized, tested and/or documented, and should operate as designed.	5.1 Determine if there is a System Development Life Cycle methodology for all systems development work.			
	5.2 Determine if a feasibility study is carried out and approved when developing new systems. Consider: o Cost justification o Strengths and weakness comparison between existing systems and proposed new ones o Data requirements o Hardware, software and processing requirements o Security and control requirements of			

Audit Area and Objective	Test Procedure	Test Result	Work Paper Reference	Gap Analysis
	new system o System interface requirements			
	5.3 Assess whether users are appropriately involved in the systems development process. Consider: o Specification of requirements o User sign-offs o User acceptance testing o Training o Formal approval before implementation o Development of user manuals o Cost control			
	5.4 Determine if comprehensive systems and program documentation are produced. Consider: o System specifications o Program specifications o Data-flow diagrams o Logical data structures o Operations instructions o Functional business model or entity model			
	5.5 Determine if automated tools such as CASE are used.			
	5.6 Determine if the business is dependent on externally supplied and maintained application systems. If so assess whether a well-established supplier is used. Consider: o Whether comprehensive documentation is provided o If control requirements have been evaluated (system controls, management reports, and audit trails) o Whether adequate training and technical support is provided o If the source code is provided o If the software is owned by the supplier, and if there is an escrow agreement. o If procedures exist to ensure the			

Audit Area and Objective	Test Procedure	Test Result	Work Paper Reference	Gap Analysis
	software version is up to date			
	5.7 Determine if changes and upgrades are planned to minimize disruption. Assess if changes and upgrades are checked and tested before installation.			
	5.8 Determine if there are controls to restrict access by supplier staff to data and programs.			
	5.9 Assess whether adequate internal controls and audit trails are specified for the system. Consider: o Access controls o Application controls o User controls o System controls o Management reports o Audit trails			
	5.10 Determine if computer operations is made aware of any new or updated system. Consider: o Capacity planning o Resource planning o Recovery or restart procedures o Technical documentation o Processing requirements o Control requirements			
	5.11 Assess whether comprehensive systems documentation is produced for any updates or changes.			
	5.12 Determine if adequate project control and management is practiced. Consider: o Stated objectives o Plans developed o Responsibilities of team members o Milestones o Budget and costs monitored o Adequacy of resources o Consultants managed or controlled in effective and efficient way			
	5.13 Determine if a quality assurance activity exists for system installs and updates.			

Audit Area and Objective	Test Procedure	Test Result	Work Paper Reference	Gap Analysis
	5.14 Determine if formal change management procedure exist. Consider: o Program changes o System software changes o Hardware changes o Use of program change form o Authorizing body for proposed changes			
	5.15 Determine if requests for program changes are normally approved by authorized users. Assess whether users are involved in the change process. Determine if users approve program changes before revised versions of a program are implemented into the production environment.			
	5.16 Determine if major program change requests have been approved by the IT Steering Committee.			
	5.17 Determine if program code is subject to review.			
	5.18 Determine if development staff is prevented from implementing new program versions into the production environment.			
	5.19 Is there a facility to determine if unauthorized changes have occurred to operational programs. Consider: o Object compare software o Management review o Logging of changes			
	5.20 Determine if automated change control software such as CA-ENDEVOR is used.			
	5.21 Determine if there is a procedure to ensure previous versions of software are made inactive and only current version are operative.			
	5.22 Determine if the established procedures for controlling any emergency changes made by systems development staff are adequate.			
	5.23 Determine if program test procedures are adequate. Determine if all programs are tested together in a simulated live environment to ensure that the system performs as planned. Consider:			

Audit Area and Objective	Test Procedure	Test Result	Work Paper Reference	Gap Analysis
	○ System testing ○ Unit testing ○ Volume testing ○ Sequence testing ○ User involvement ○ System interfaces ○ Result-checking			
	5.24 Determine whether separate libraries are assigned for test and production activities.			
	5.25 Determine whether regression testing is carried out when failures have been rectified.			
	5.26 Determine if a formal sign-off is required after system testing, and who is required to sign off.			
	5.27 Determine if a post-implementation review is carried out to ensure the system has achieved its objectives.			
	5.28 Determine if users receive training on the features of the new systems before implementation.			
	5.29 Determine whether systems documentation is maintained up-to-date and is secured. Determine if user manuals are maintained up-to-date and are secured. Consider: ○ User and IT Department responsibilities ○ Objectives and description of system ○ Offsite storage ○ Readability and references Determine if operating manuals are maintained up-to-date and are secured. Consider: ○ Flow charts ○ Job control language (JCL) statements ○ Rerun, checkpoint, backup, and restart/recovery procedures ○ Offsite storage			

Audit Area and Objective	Test Procedure	Test Result	Work Paper Reference	Gap Analysis
6. Incident Response Objective: Security events should be responded to in a prompt, organized, and repeatable manner.	6.1 Determine if an Incident Response policy exists. Determine if an Incident Response team exists.			
	6.2 Determine if incident information is kept in a logbook. Determine if all response actions are logged.			
	6.3 Determine if problem identification/ clarification procedures exist.			
	6.4 Determine if an incident contact list exists. Verify the release of incident information is addressed in the response policy.			
	6.5 Determine if attempts are made to identify responsible parties.			
	6.6 Determine if proper chain of custody procedures are documented and followed.			
	6.7 Determine if recovery efforts includes information on system snapshots, lockout, and restoration procedures.			

Audit Area and Objective	Test Procedure	Test Result	Work Paper Reference	Gap Analysis
7. Business Continuity Objective: The ability of the business to resume effective operations in the event that its existing primary site and processing facilities were not available should be reasonably assured.	7.1 Determine if a Business Continuity Plan exists for the firm and verify it has approved policies, standards and procedures in place. Determine if a BCP Coordinator exists to maintain the plan.			
	7.2 Determine if BCP goals and objectives are in place and communicated throughout the organization.			
	7.3 Determine if firm management has reviewed, approved, and signed-off on the BCP.			
	7.4 Determine if effective communication procedures and documentation exist for firm-wide command centers in the event of a disaster.			
	7.5 Determine if the firm performs a Business Impact Analysis to prioritize critical systems, resources, and processes. Determine that the BCP office performs a Business Impact Analysis to identify any potential financial impacts of a disaster.			
	7.6 Determine if documented procedures detail how emergency funds are to be acquired in a disaster or other emergency event.			
	7.7 Determine if the firm has purchased adequate insurance policies to cover all appropriate risks associated with a disaster.			
	7.8 Determine if adequate inventories exist for production hardware and software, especially licenses, for insurance and recovery purposes.			

Audit Area and Objective	Test Procedure	Test Result	Work Paper Reference	Gap Analysis
	7.9 Determine if an adequate contingency facility exists for the firm.			
	7.10 Determine if Service Level Agreements with the external recovery provider address priority access to the designated contingency facilities.			
	7.11 Determine that adequate redundant infrastructure exists at a designated back up location to ensure processing capabilities. These items include: o Application software o Hardware o Telecommunications o Supplies o Vital Record Information o Utilities			
	7.12 Determine if adequate preventative measures are in place at the production site to reduce the need to declare disasters over small incidents (i.e., power outage).			
	7.13 Determine if essential personnel and training requirements have been defined and included in the recovery plan.			
	7.14 Determine that documented procedures exist defining the criteria for declaring a disaster.			
	7.15 Determine if call trees and contact lists are included in the recovery plan. Verify that external as well as internal parties will be notified in the event of a disaster.			
	7.16 Determine if Recovery Time Objectives (RTOs) are stated in the BCP documentation and are known by key business unit contacts, support vendors, and customers.			
	7.17 Determine if the contingency plan is documented. Verify the latest version is available to appropriate users and at the recovery site. Verify hard and soft copies of the contingency plan have been created and are regularly maintained and updated.			
	7.18 Determine if manual processes are known and can be implemented to perform transactions in place of systems for designated operations.			

Audit Area and Objective	Test Procedure	Test Result	Work Paper Reference	Gap Analysis
	7.19 Determine that the recovery plan is tested and a documented test plan exists and is approved to ensure completeness of testing including test objectives, criteria, reporting methods, and regularity.			
	7.20 Determine if the updated BCP is distributed to appropriate parties, including the recovery site, in a controlled manner.			
	7.21 Determine if cross training is performed for all critical staff involved in the disaster recovery process.			
	7.22 Determine if a regular backup schedule exists and where the tapes are kept when on-site. Determine if tapes are stored in a fire rated data safe. Verify access to backup tapes is highly restricted.			
	7.23 Determine if backup tapes are kept in secure off-site storage. Determine the frequency of tape removal and how long those tapes are stored. Verify there is an inventory of the back up tapes as well as a backup tape numbering scheme.			
	7.24 Determine if a test restore from backup tape been conducted to ensure it works properly and all necessary information is available. Determine if there is a periodic test restore schedule.			
	7.25Determine if an inventory of hardware and software backup tapes are kept in secure off-site storage. Determine the frequency of tape removal and how long those tapes are stored. Verify there is an inventory of the back up tapes as well as a backup tape numbering scheme.			
	7.26 Determine if IT restoration procedures have been documented and sent offsite as part of the continuity plan.			
	7.27 Determine if business processes (i.e., how people do what they do and when it needs to be done) have been documented and sent offsite as part of the continuity plan.			

Audit Area and Objective	Test Procedure	Test Result	Work Paper Reference	Gap Analysis
8. Data Center Computer Operations Objective: Computer operations should be controlled properly to ensure appropriate working practices and processing.	8.1 Determine if computer operations personnel can initiate or change input transactions for application systems. Consider: o Data access o Ad hoc jobs o Emergency changes o Job overrides o Job scheduling o Record of reruns			
	8.2 Determine whether computer processing logs are generated and reviewed regularly to detect unauthorized or unusual actions. Consider: o Availability of system logs o Details of information received o Use of software to identify specific actions o Identification of sensitive utilities o Use of access control software			
	8.3 Determine the degree to which capacity planning and performance monitoring are carried out. Consider: o System downtime o CPU usage o Availability of disk space o Identification of processing bottlenecks o CPU, memory, and bandwidth availability or future growth requirements o Reliability of disks, tapes or other media o Software problems o System reliability			
	8.4 Determine if job schedules and system updates/changes are well controlled, documented, and consider customer needs.			

Audit Area and Objective	Test Procedure	Test Result	Work Paper Reference	Gap Analysis
	8.5 Determine if procedures to control the issue and maintenance of backup tapes exist. Consider: o Tape management systems o Physical inventory of tapes o Testing of backup tapes to ensure they work o Identification of tapes o Record maintained of tape location. o Secure storage of tapes (i.e., fire rated data safe)			
	8.6 Determine if operating procedures are documented. Consider: o Shift procedures o Shift diaries o Incident reporting o Statistics o Follow up and review of problems			
	8.7 Determine if operations documentation is regularly reviewed and updated.			
	8.8 Determine if any output is generated from customer data. Assess if the data is kept or disposed of in a secure manner.			
	8.9 Determine if preventative maintenance is carried out in accordance with manufacturers' recommendations.			
	8.10 Determine if any third party services are involved in maintaining or monitoring customer machines. Determine if there is a hardware maintenance contract and will others have access to customer machines.	o		
	8.11 Determine if Service Level Agreements exist with all third party service providers including hardware, software, and telecommunications circuits.			

Audit Area and Objective	Test Procedure	Test Result	Work Paper Reference	Gap Analysis
9. Network Communications Objective: Security over network communications (e.g., data confidentiality, integrity and availability) should be controlled properly.	9.1 Assess the overall network plan. Consider: ○ Local area network (LAN) including servers, desktops, printers, and switches ○ Wide area network (WAN) including servers, routers, and switches ○ Modem use ○ Wireless networking ○ Firewalls ○ Intrusion Detection Systems ○ Remote Access (RAS) ○ Virtual Private Networks ○ Authentication			
	9.2 Determine whether responsibility is assigned for management and control of the network, and who the person is. Consider: ○ Integration of network planning and development with the IT plan ○ Network control and monitoring of utilization, performance and security			
	9.3 Determine the number of Internet access points and how they are protected. Determine if firewalls and Intrusion Detection Systems are used.			
	9.4 Determine if security reviews and penetration tests have been performed and if so how recently.			
	9.5 Determine if any incidents have occurred at the production or backup location.			
	9.6 Determine if email monitoring and alerting applications are in use to block unauthorized information dissemination.			
	9.7 Determine if web access monitoring and alerting applications are in use to block unauthorized information dissemination.			
	9.8 Determine if external instant messaging is allowed at this facility. If so how is it secured. Determine if PDAs are allowed at this facility. If so how are they secured.			

Audit Area and Objective	Test Procedure	Test Result	Work Paper Reference	Gap Analysis
	9.9 Determine if wireless networking is allowed at this facility. If so how is it secured. Consider: o MAC address filtering o Vendor specific authentication o SSID/Network ID o Wired Equivalent Privacy (WEP) o VLANs o Firewalled WLANs with at network touch-points with VPNs for authentication, authorization and encryption			
	9.10 Determine the adequacy of recovery procedures for a loss of communications links.			
	9.11 Determine if important data are encrypted, when being transmitted over communication links, to ensure their integrity and confidentiality. Consider: o Type of encryption (i.e., algorithm and key length) o Authentication of the sender as genuine (i.e., digital signatures, digital certificates) o Protecting the data from unauthorized access and browsing o Who has access and why o Error detection (i.e., message digests) o Management of the keys used for encryption			
	9.12 Determine if modems are in use. If so determine if security facilities are installed, such as encryption, authentication, or dial-back to verify callers' locations.			
	9.13 Determine is the PBX has a modem attached for maintenance. If so determine who has dial up access. Verify that all administrative accounts have had their passwords changed from defaults. Verify adequate voicemail and toll fraud security settings are in place. Verify the number of analog lines in place on the PBX and stand-alone POTS lines.			

Audit Area and Objective	Test Procedure	Test Result	Work Paper Reference	Gap Analysis
	9.14 Determine is Remote Access via modem or network connection is in use. If so determine if VPNs with strong authentication are in use to mitigate security concerns.			
	9.15 Assess the adequacy of access controls over user access to the network.			
	9.16 Assess the controls for access by external parties. Consider: o Communications circuit vendors o Third party information feed vendors o Telecommunications (PBX) vendors o Customers	o		
	9.17 Determine if single points of failure have been eliminated or mitigated through other means.			
10. Operating Systems Software Objective: The operating system should be secured and protected from unauthorized amendments.	10.1 Determine if there is a specialist function responsible for maintaining operating system software.			
	10.2 Determine if security requirements are clearly defined. Consider: o IT security policy o Classification of sensitive systems and data o Quality assurance o Independent review			
	10.3 Determine if the need for protecting various types of resources, such as critical files and transactions, has been identified and specified. Determine the sensitive operating system software features have			

Audit Area and Objective	Test Procedure	Test Result	Work Paper Reference	Gap Analysis
	been identified.			
	10.4 Determine if system software is protected against unauthorized access and modification. Verify that adequate access controls are in place.			
	10.5 Determine if access to administrative level accounts is restricted. Verify all users have an individual account that is password protected.			
	10.6 Determine if anti-virus is installed on the machines and up to date.			
	10.7 Determine if a local firewall, hardware or software, is installed on the machines.			
	10.8 Determine if Host-based Intrusion Detection Systems or Host-based Intrusion Prevention Systems are installed on the machines.			
	10.9 Determine if a system software maintenance plan exists. Verify all operating systems are currently supported and patches are up to date. Verify the existence of a patch maintenance process.			
	10.10 Determine whether a record is maintained of all system software upgrades, including both supplier upgrades and in-house upgrades. Verify this information is documented and kept current.			
	10.11 Determine whether all system software upgrades are properly authorized.			
	10.12 Determine if hardening policies and procedures are in place for operating systems.			
	10.13 Determine if file encryption is in use at an operating system level. Consider: o Type of encryption (i.e., algorithm and key length) o Protecting the data from unauthorized access and browsing o Who has access and why			

Audit Area and Objective	Test Procedure	Test Result	Work Paper Reference	Gap Analysis
	○ Management of the keys used for encryption			
	10.14 Determine if all programs and data files (compilers, assemblers, link editors, macro libraries, source libraries, etc.) used to construct and maintain system software are adequately protected. Consider: ○ Identification of protected data sets ○ Use of access control software ○ Updated authorization procedures			
	10.15 Verify a record is maintained of: ○ All system software installed ○ All internally-generated modifications or extensions ○ All system software problems encountered			
	10.16 Determine that use is made of system logging facilities. Verify the logs are kept for a significantly long period of time before overwriting or deletion. Determine if log files are backed up or sent to a log server. Determine if automated log monitoring and alerting capabilities are in use to detect unauthorized behavior.			
	10.17 Determine if backup files of the system software are created. Consider: ○ Frequency ○ Completeness ○ Offsite storage ○ Test restores			
	10.18 Determine if operating system monitoring reviews are carried out to ensure system resources are being used most effectively.			

Audit Area and Objective	Test Procedure	Test Result	Work Paper Reference	Gap Analysis
11. Database Systems Objective: Databases should be maintained in order to ensure data confidentiality, integrity and availability.	11.1 Verify there is a database administration (DBA) function. Determine if the DBA function is segregated from application programming.			
	11.2 Determine if the duties and responsibilities of the DBA are defined in writing and include: o Control and security issues o Backup and recovery facilities o Maintenance and control of the database definitions using a database dictionary o Control over or review of usage of programs that amend data in the database o Review and approval of modifications to applications programs that access the database o Responsibility for maintenance of the database management software in conjunction with systems programming personnel			
	11.3 Determine if database software is protected against unauthorized access and modification. Verify that adequate access controls are in place.			
	11.4 Determine if access to administrative level accounts is restricted. Verify all users have an individual account that is password protected.			
	11.5 Determine if a database software maintenance plan exists. Verify all database systems are currently supported and patches are up to date. Verify the existence of a patch maintenance process.			

Audit Area and Objective	Test Procedure	Test Result	Work Paper Reference	Gap Analysis
	11.6 Determine whether a record is maintained of all database software upgrades, including both supplier upgrades and in-house upgrades. Verify this information is documented and kept current.			
	11.7 Determine whether all database software upgrades are properly authorized.			
	11.8 Determine if the DBA is responsible for the security classification of individual data elements. Determine if the DBA regularly reviews the dictionary to ensure that only required data items are accessed by application programs.			
	11.9 Find out if access to application program functions is restricted, e.g., by the use of menus specific to user ids or groups. Determine if the use of inherent database access control software is effective in restricting access to the database.			
	11.10 Determine if access control software is used to restrict access to the database, note whether it is implemented effectively. Determine if violation reports being produced? If so verify by obtaining such a report that is reviewed by the DBA or security administrator.			
	11.11 Determine whether the database area containing passwords is restricted to only the DBA.			
	11.12 Determine if hardening policies and procedures are in place for database systems.			
	11.13 Determine if record integrity and data integrity software is in use and its frequency of use.			
	11.14 Determine if column encryption is in use at a database system level. Consider: o Type of encryption (i.e., algorithm and key length) o Protecting the data from unauthorized access and browsing o Who has access and why o Management of the keys used for			

Audit Area and Objective	Test Procedure	Test Result	Work Paper Reference	Gap Analysis
	encryption			
	11.15 Determine if all programs and data files (compilers, assemblers, link editors, macro libraries, source libraries, etc.) used to construct and maintain system software are adequately protected. Consider: o Identification of protected data sets o Use of access control software o Updated authorization procedures			
	11.16 Verify a record is maintained of: o All database software installed o All internally-generated modifications or extensions o All database software problems encountered			
	11.17 Determine that use is made of database logging facilities. Verify the logs are kept for a significantly long period of time before overwriting or deletion. Determine if log files are backed up or sent to a log server. Determine if automated log monitoring and alerting capabilities are in use to detect unauthorized behavior.			
	11.18 Determine if backup files of the database are created. Consider: o Frequency o Completeness o Offsite storage o Test restores with documented restore procedures			
	11.19 Determine if database system monitoring reviews are carried out to ensure system resources are being used most effectively.			

Audit Area and Objective	Test Procedure	Test Result	Work Paper Reference	Gap Analysis
12. Application Systems Objective: The completeness and accuracy of input, processing and output of data in applications systems should be controlled properly.	12.1 Determine if there is a specialist function responsible for maintaining application system software.			
	12.2 Determine if security requirements are clearly defined. Consider: o IT security policy o Classification of sensitive systems and data o Quality assurance o Independent review			
	12.3 Determine if the need for protecting various types of resources, such as critical files and transactions, has been identified and specified. Determine the sensitive application software features have been identified.			
	12.4 Determine if application software is protected against unauthorized access and modification. Verify that adequate access controls are in place.			
	12.5 Determine if access to administrative level accounts is restricted. Verify all users have an individual account that is password protected.			
	12.6 Determine if an application software maintenance plan exists. Verify all applications are currently supported and patches are up to date. Verify the existence of a patch maintenance process.			
	12.7 Determine whether a record is maintained of all application software upgrades, including both supplier upgrades and in-house upgrades. Verify this information is documented and kept current.			

Audit Area and Objective	Test Procedure	Test Result	Work Paper Reference	Gap Analysis
	12.8 Determine whether all application software upgrades are properly authorized.			
	12.9 Determine if file encryption is in use at an application system level. Consider: o Type of encryption (i.e., algorithm and key length) o Protecting the data from unauthorized access and browsing o Who has access and why o Management of the keys used for encryption			
	12.10 Verify a record is maintained of: o All application software installed o All internally-generated modifications or extensions o All application software problems encountered			
	12.11 Determine that use is made of application logging facilities. Verify the logs are kept for a significantly long period of time before overwriting or deletion. Determine if log files are backed up or sent to a log server. Determine if automated log monitoring and alerting capabilities are in use to detect unauthorized behavior.			
	12.12 Determine if backup files of the application software are created. Consider: o Frequency o Completeness o Offsite storage o Test restores			
	12.13 Determine if application monitoring reviews are carried out to ensure system resources are being used most effectively.			

Audit Area and Objective	Test Procedure	Test Result	Work Paper Reference	Gap Analysis
13. End-User Computing Objective: Information available through end-user use of microcomputers, terminals or workstations should be protected properly.	13.1 Determine if end-user computing is a concern with this firm. Determine if end-user computing policies exist.			
	13.2 Determine if client side requirements exist for the applications to be used. Consider: o Security requirements o Connectivity requirements o Required software o Software patches o Required hardware o Programming requirements o Testing o Documentation o Anti-virus o Monitoring and alerting o Backup o Training			
	13.3 Determine if employees, customers, and service vendors are aware of firm end-user policies and the consequences of not following them.			
	13.4 Determine if programming languages and tools can be used to circumvent normal end-user controls. Determine if users have the ability to make changes to production applications or data files.			
	13.5 Determine if there is access control software in place to prevent unauthorized access to any workstation or terminal.			

Audit Area and Objective	Test Procedure	Test Result	Work Paper Reference	Gap Analysis
	13.6 Determine if data is uploaded to central computer systems. Consider: o Are file controls in place to ensure that access to production programs, data and files cannot occur in an unauthorized manner o Are file controls in place to prohibit update of production files and programs except under controlled, authorized conditions.			
	13.7 Inquire whether customer users are satisfied with the critical systems. Consider: o Management information o Timeliness of reporting o On-line help facilities o User-friendly facilities o Response times o Reliability and up-time			
	13.8 Assess whether users are satisfied with the service from the IT Department. Consider: o Help desk o Program change o Ad hoc requests o Turnaround time on user requests			