RISK AREAS OF IT AUDIT

Area of Risk	Actual Risks	Control Procedures to Minimize Risk	Audit procedures
1.Overall (General)	• Break-in to facilities where computer is housed and destruction of data • Theft of data as it is transmitted • Virus infection of system • Computer breakdown	• Developing an information security/protection plan. • Restricting physical and logical access. • Encrypting data. • Protecting against viruses. • Implementing firewalls. • Instituting data transmission controls. • Preventing and recovering from system failures or disasters, including: • Designing fault-tolerant systems. • Preventive maintenance. • Backup and recovery procedures. • Disaster recovery plans.	• **Systems Review:** Inspecting computer sites. Interviewing personnel. Reviewing policies and procedures. Examining access logs, insurance policies, and the disaster recovery plan. **Test Controls:** Auditors test security controls by: Observing procedures. Verifying that controls are in place and work as intended.
2. System development, acquisition and (*X)	• Two things can go wrong in program development: ○ Inadvertent errors due to careless programming or misunderstanding specifications; or ○ Deliberate insertion of unauthorized instructions into the programs	• The preceding problems can be controlled by requiring: • Management and user authorization and approval • Thorough testing • Proper documentation • Thorough step-by-step documentation in acquisition of canned software systems	• The auditor's role in systems development should be limited to an independent review of system development activities. • To maintain necessary objectivity for performing an independent evaluation, the auditor should not be involved in system development. • During the systems review, the auditor should gain an understanding of development procedures and controls therein by discussing them with management, users, and IS personnel.

Area of Risk	Actual Risks	Control Procedures to Minimize Risk	Audit procedures
3. Modification (*X)	• program change implemented incorrectly • program change introduces new errors into existing system • program change not implemented • program change not documented	• When a program change is submitted for approval, a list of all required updates should be compiled by management and program users. • Changes should be thoroughly tested and documented. • During the change process, the developmental version of the program must be kept separate from the production version. • When the amended program has received final approval, it should replace the production version.	• An important part of these tests is to verify that program changes were identified, listed, approved, tested, and documented. • Test for Unauthorized changes: To test for unauthorized program changes, auditors can use a source code comparison program to compare the current version of the program with the original source code.
4. The working of the programs in the system (processing) (*X)	• Types of errors and fraud • During computer processing, the system may: • Fail to detect erroneous input. • Improperly correct input errors. • Process erroneous input. • Improperly distribute or disclose output.	• Computer data editing routines. • Reconciliation of batch totals. • Effective error correction procedures. • Effective handling of data input and output by data control personnel.. • Maintenance of proper environmental conditions in computer facility.	• Processing test data
5. The capture and input of data into the system (source data) (*X)	• Inaccurate source data • Unauthorized source data	• Effective handling of source data [input documents] input by data entry dept personnel • User authorization of source data input • Logging of the receipt, movement, and disposition of source data input • Effective procedures for correcting and resubmitting erroneous data	• Auditors should test source data controls on a regular basis to see if these controls are working, because the strictness with which they are applied may vacillate

Area of Risk	Actual Risks	Control Procedures to Minimize Risk	Audit procedures
6. The storage of data that has been input (data files)	• concerns the accuracy, integrity, and security of data stored in machine-readable files (including relational tables in a database) after this data has been entered • Data storage risks include: • Unauthorized modification of data • Destruction of data • Disclosure of data • If file controls are seriously deficient, especially with respect to access or backup and recovery, the auditor should strongly recommend they be rectified.	• Destruction of stored data due to: • Inadvertent errors • Hardware or software malfunctions • Intentional acts of sabotage or vandalism • Unauthorized modification or disclosure of stored data • restrictions on physical access to data files • Logical access (access by program) controls using passwords • Encryption of highly confidential data • Use of virus protection software • Maintenance of backup copies of all data files in an off-site location	• Review logical access policies and procedures. • Review operating documentation to determine prescribed standards for: • Use of write-protection mechanisms. • Use of virus protection software. • Use of backup storage. • System recovery, including checkpoint and rollback procedures. • Review systems documentation to examine prescribed procedures for: • Use of data encryption • Control of file conversions • Reconciling master file totals with independent control totals • Examine disaster recovery plan. • Discuss data file control procedures with systems managers and operators.