IT Operations Review Questions

IT operations controls are associated with the day-to-day operation of computer programs and systems. These controls are designed to ensure that IT systems are operating efficiently and that effectiveness targets are being met.

Procedures detailing instructions for operational tasks and procedures coupled with appropriate IT management oversight are necessary parts of the IT control environment. This documentation should include details based on/for:

- Operating instructions and job flows for computer and peripheral equipment
- Monitoring systems and applications
- Detecting systems and applications errors and problems
- Handling information services problems and escalation of unresolved issues
- Backup and recovery

Click the links below to review questions for each of the following areas of IT Operations:

IT personnel (observation)

Operator access

Operator manuals

Access to the library

Contents and location of offline storage

File-handling procedures

Data entry

Lights-out operations

IT Personnel Observation

- Have controls been put in place to ensure efficiency of operations and adherence to established standards and policies?
- Is adequate supervision present?
- Have controls been put in place regarding IT management review, data integrity and security?

Operator Access

- Is access to files and documentation libraries restricted to operators?
- Are responsibilities for the operation of computer and related peripheral equipment limited?
- Is access to correcting program and data problems restricted?
- Should access to utilities that allow system fixes to software and/or data be restricted?
- Is access to production source code and data libraries (including run procedures) limited?

Operator Manuals

Are instructions adequate to address:

- The operation of the computer and its peripheral equipment?
- Startup and shutdown procedures?
- Actions to be taken in the event of machine/program failure?
- Records to be retained?
- Routine job duties and restricted activities?

Access to the library

- Is the librarian prevented from accessing computer hardware?
- Does the librarian have access only to the tape management system?
- Is access to library facilities provided to authorized staff only?
- Is removal of files restricted by production scheduling software?
- Does the librarian handle the receipt and return of foreign media entering the library?
- Are logs of the sign-in and sign-out of data files and media maintained?

Contents and location of offline storage

- Are offline file storage media containing production system programs and data clearly marked with their contents?
- Are offline library facilities located away from the computer room?
- Are policies and procedures adequate for:
- Administering the offline library?
- Checking out/in media, including requirements for signature authorizations?
- Identifying, labeling, delivering and retrieving offsite backup files?
- Encryption of offsite backup files (especially if these physically move between locations)?
- Inventorying the system for onsite and offsite media, including the specific storage locations of each tape?
- Secure disposal/destruction of media, including requirements for signature authorizations?

File handling procedures

- Have procedures been established to control the receipt and release of files and secondary storage media to/ from other locations?
- Are internal tape labels used to help ensure that the correct media are mounted for processing?
- Are these procedures adequate and in accordance with management's intent and authorization?
- Are these procedures being followed?

Data entry

- Are input documents authorized and do the documents contain appropriate signatures?
- Are batch totals reconciled?
- Does segregation of duties exist between the person who keys the data and the person who reviews the keyed data for accuracy and errors?
- Are control reports being produced? Are the reports accurate? Are the reports maintained and reviewed?

Lights-out operations

- Remote access to the master console is often granted to standby operators for contingency purposes such as automated software failure. Is access to security sufficient to guard against unauthorized use?
- Do contingency plans allow for the proper identification of a disaster in the unattended facility?
- Are the automated operation software and manual contingency procedures documented and tested adequately at the recovery site?
- Are proper program change controls and access controls present?
- Are tests of the software performed on a periodic basis, especially after changes or updates are applied?
- Do assurances exist that errors are not hidden by the software and that all errors result in operator notification?