IT Infrastructure Review Questions

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

Hardware

Software Source Code

Operating Systems

Databases

Hardware

IT systems and business processes rely on hardware. Hardware encompasses all the physical components of a computer system, including the equipment and devices that process, store and transmit data. When auditing hardware, an IT auditor should review and consider the following categories and questions:

Hardware acquisition plan:

- Is the plan aligned with business requirements?
- Is the plan aligned with the enterprise architecture?
- Is the plan compared regularly to business plans to ensure continued synchronization with business requirements?
- Is the plan synchronized with IS plans?
- Have criteria for the acquisition of hardware been developed?
- Is the environment adequate to accommodate the currently installed hardware and new hardware to be added under the approved hardware acquisition plan?
- Are the hardware and software specifications, installation requirements and the likely lead time associated with planned acquisitions adequately documented?

Acquisition of hardware:

- Is the acquisition in line with the hardware acquisition plan?
- Have the IS management staff issued written policy statements regarding the acquisition and use of hardware, and have these statements been communicated to the users?
- Have procedures and forms been established to facilitate the acquisition approval process?
- Are requests accompanied by a cost-benefit analysis?
- Are purchases routed through the purchasing department to streamline the process, avoid duplications, ensure compliance with tendering requirements and legislation and to take advantage of quantity and quality benefits such as volume discounts?

IT hardware asset management:

- Has the hardware been tagged?
- Has an owner been designated?
- Where will the hardware be located?
- Have we retained a copy of the contracts/SLAs?

Capacity management and monitoring:

- Are criteria used in the hardware performance monitoring plan based on historical data and analysis obtained from the IS trouble logs, processing schedules, job accounting system reports, preventive maintenance schedules and reports?
- Is continuous review performed of hardware and system software performance and capacity?
- Is monitoring adequate for equipment that has been programmed to contact its manufacturer (without manual or human intervention) in the case of equipment failure?

Preventive maintenance schedule:

- Is the prescribed maintenance frequency recommended by the respective hardware vendors being observed?
- Is maintenance performed during off-peak workload periods?
- Is preventive maintenance performed at times other than when the system is processing critical or sensitive applications?

Hardware availability and utilization reports:

- Is scheduling adequate to meet workload schedules and user requirements?
- Is scheduling sufficiently flexible to accommodate required hardware preventive maintenance?
- Are IS resources readily available for critical application programs?

Problem logs and job accounting system reports:

- Have IS management staff reviewed hardware malfunctions, reruns, abnormal system terminations and operator actions?

Software Source Code

Source code is the language in which a software program is written. It is translated into object code by assemblers and compilers and tells the computer what to do. By its very nature, source code may contain intellectual property. It should be protected, and access should be restricted.

The actual source code should be managed using a version control system (VCS), often called revision control software (RCS). The code is maintained in a central repository, which allows programmers to check out a program source to make changes to it. An IT auditor should always be aware of the following regarding source code:

- Who has access to the source code?
- Who can commit the code (push the code to production)?
- Is there an alignment of program source code with program objects?
- Is there an alignment with change and release management?
- Are there backups of source code (including code maintained offsite) and escrow agreements?

Operating Systems

The most significant system software related to a computer is its operating system (OS). The OS contains programs that provide interfaces between the user, processor and applications software. The OS is a master control program that runs the computer and acts as a scheduler and traffic controller. It provides the primary means of managing the sharing and use of computer resources, such as processors, real memory (RAM), auxiliary memory (disk storage) and input/output devices.

When conducting a review of operating software development, acquisition or maintenance, an IT auditor should review and consider the following categories and questions:

System software selection procedures

- Do they align with the enterprise architecture?
- Do they comply with short- and long-range IS plans?
- Do they meet the IS requirements?
- Are they properly aligned with the objectives of the business?
- Do they include IS processing and control requirements?
- Do they include an overview of the capabilities of the software and control options?

Feasibility Study and Selection Process

- Are same selection criteria applied to all proposals?
- Has the cost-benefit analysis of system software procedures addressed:
    - Direct financial costs associated with the product?
    - Cost of product maintenance?
    - Hardware requirements and capacity of the product?
    - Training and technical support requirements?
    - Impact of the product on processing reliability?
    - Impact on data security?
    - Financial stability of the vendor's operations?

System software security

- Have procedures been established to restrict the ability to circumvent logical security access controls?
- Have procedures been implemented to limit access to the system interrupt capability?
- Have procedures been implemented to manage software patches and keep the system software up-to-date?
- Are existing physical and logical security provisions adequate to restrict access to the master consoles?
- Were vendor-supplied installation passwords for the system software changed at the time of installation?

IT Asset Management

- Has an owner been designated?
- Have we retained a copy of the contracts/SLAs?
- What is the license agreement? Are we in compliance with it?

System software implementation

- Are controls adequate in:
  - Change procedures?
  - Authorization procedures?
  - Access security features?
  - Documentation requirements?
  - Documentation of system testing?
  - Audit trails?
  - Access controls over the software in production?

Authorization Documentation

- Have additions, deletions or changes to access authorization been documented?
- Does documentation exist of any attempted violations? If so, has there been follow-up?

System Documentation

- Are the following areas adequately documented:
  - Installation control statements?
  - Parameter tables?
  - Exit definitions?
  - Activity logs/reports?

System Software Maintenance Activities

- Is documentation available for changes made to the system software?
- Are current versions of the software supported by the vendor?
- Is there a defined patching process?

System Software Change Controls

- Is access to the libraries containing the system software limited to individual(s) needing to have such access?
- Are changes to the software adequately documented and tested prior to implementation?
- Is software authorized properly prior to moving from the test environment to the production environment?

Databases

Databases contain valuable and potentially sensitive information used by the enterprise in the regular course of business. When conducting a review of databases an IT auditor should review and consider the following categories and questions:

Logical Schema

- Do all entities in the entity-relation diagram exist as tables or views?
- Are all relations represented through foreign keys?
- Are constraints specified clearly?
- Are nulls for foreign keys allowed only when they are in accordance with the cardinality expressed in the entity-relation model?

Physical Schema

- Has allocation of initial and extension space (storage) for tables, logs, indexes and temporary areas been executed based on the requirements?
- Are indexes by primary key or keys of frequent access present?
- If the database is not normalized, is justification accepted?

Access Time Reports

- Are indexes used to minimize access time?
- Have indexes been constructed correctly?
- If open searches not based on indexes are used, are they justified?

Database Security Controls

- Are security levels for all users and their roles identified within the database and access rights for all users and/ or groups of users justified?
- Do referential integrity rules exist and are they followed?
- How is a trigger created and when does it fire?
- Is there a system for setting passwords? Does change of passwords exist and is it followed?
- How many users have been given system administrator privileges? Do these users require the privilege to execute their job function?
- Has an auditing utility been enabled? Are audit trails being monitored?
- Can database resources be accessed without using DBMS commands and SQL statements?
- Is system administrator authority granted to job scheduler?
- Are actual passwords embedded into database utility jobs and scripts?
- Has encryption been enabled where required?
- Are copies of production data authorized?
- Are copies of production data altered or masked to protected sensitive data?

Interfaces with other programs/software

- Are integrity and confidentiality of data not affected by data import and export procedures?
- Have mechanisms and procedures been put in place to ensure the adequate handling of consistency and integrity during concurrent accesses?

Backup and Disaster Recovery Procedures and Controls

- Do backup and disaster recovery procedures exist to ensure the reliability and availability of the database?
- Are there technical controls to ensure high availability and/or fast recovery of the database?

Database-supported Information Security Controls

- Is access to shared data appropriate?
- Are adequate change procedures utilized to ensure the integrity of the database management software?
- Is data redundancy minimized by the database management system? Where redundant data exist, is appropriate cross-referencing maintained within the system's data dictionary or other documentation?
- Is the integrity of the database management system's data dictionary maintained?

IT Asset Management

- Has an owner been designated?
- Have we retained a copy of the contracts/SLAs?
- What is the license agreement? Are we in compliance with it?