# IT Auditing

## *Lecture - 7*

*Ms. Saleem Adeeba*
Temporary Assistant Lecturer
*Dept. of Computing & Information Systems*
*Sabaragamuwa University of Sri Lanka*
*0720928486*
*adeesa@foc.sab.ac.lk*

# 2. The computer center

- Accountants routinely examine the physical environment of the computer center as part of their annual audit.

- The following are areas of potential exposure that can impact the quality of information, accounting records, transaction processing, and the effectiveness of other more conventional internal controls

# 2. The computer center

a) Physical Location

- The physical location of the computer center directly affects the risk of destruction to a natural or man-made disaster.
- To the extent possible, the computer center should be away from human-made and natural hazards, such as processing plants, gas and water mains, airports, high crime areas, flood plains, and geological faults.

# 2. The computer center

b) Construction

- Ideally, a computer center should be located in single story building of solid construction with controlled access (discussed next).
- Utility (power and telephone) lines should be underground.
- The building windows should not open and an air filtration system should be in place that is capable of extracting pollens, dust, and dust mites.

# 2. The computer center

c) Access

- Access to the computer center should be limited to the operators and other employees who work there.
- Physical controls, such as locked doors, should be employed to limit access to the center.
- Access should be controlled by a keypad or swipe card, though fire exits with alarms are necessary.

# 2. The computer center

d) Air Conditioning

- Computers function best in an air-conditioned environment, and providing adequate air conditioning is often a requirement of the vendor’s warranty.
- Computers operate best in a temperature range of 70 to 75 degrees Fahrenheit and a relative humidity of 50 percent.
- Logic errors can occur in computer hardware when temperatures depart significantly from this optimal range.

# 2. The computer center

f) Fault Tolerance

- Fault tolerance is the ability of the system to continue operation when part of the system fails because of hardware failure, application program error, or operator error.
- Implementing fault tolerance control ensures that no single point of potential system failure exists.
- Total failure can occur only if multiple components fail.
  - Refer Redundant arrays of independent disks (RAID) & Uninterruptible power suppliesfor your extra understanding

# 2. The computer center

- ❑ Audit Objectives

- ✓ The auditor's objective is to evaluate the controls governing computer center security.
- ✓ Specifically, the auditor must verify that:

i. Physical security controls are adequate to reasonablyprotect the organization from physical exposures

ii. Insurance coverage on equipment is adequate to compensate the organization for the destruction of, or damage to, its computer center

# 2. The computer center

- Audit Procedures

i. Tests of Physical Construction,
ii. Tests of the Fire Detection System,
iii. Tests of Access Control,
iv. Tests of Raid,
v. Tests of the Uninterruptible Power Supply,
vi. Tests for Insurance Coverage,

# Next Lecture

- Disaster recovery planning