Use cases

Use Case 1: Executive Falls for Phishing Attack (Security Awareness and Training)

Scenario:

A high-level executive received a spear-phishing email disguised as a vendor invoice. The email included a malicious link that the executive clicked, granting attackers unauthorized access to internal systems. The executive did not recognize the red flags of phishing, nor was any practical training or simulation conducted for such threats in the past year. The IT department failed to provide targeted training for C-level roles.

Key compliance aspects to test:

- Was annual security awareness training provided to executives?
- Was phishing or spear-phishing training covered?
- Were practical exercises (e.g., simulations) included?
- Were training records maintained and monitored?

Use Case 2: Major Outage Without Working Backup Site (Contingency Planning)

Scenario:

A regional data center suffered a major power failure due to a fire in a nearby transformer. Although a contingency plan existed, the organization had not tested it in the past 14 months. The designated alternate processing site was outdated and lacked the equipment needed to resume operations. Critical business functions were down for 48 hours, violating SLAs and leading to financial loss and customer dissatisfaction.

Key compliance aspects to test:

- Was the contingency plan reviewed annually?
- Were recovery objectives and responsibilities clearly defined?

- Was the alternate processing site tested and up to standard?
- Were staff trained for contingency operations in the last 6 months?
- Was coordination done with disaster recovery and continuity plans?

Use Case 3: Unauthorized Entry into Server Room (Physical and Environmental Protection)

Scenario:

An unbadged third-party technician was allowed entry into the server room by a receptionist who failed to verify credentials. No logs were generated for the visit. Surveillance footage later revealed the individual connected a rogue device to a core switch. Access credentials for terminated employees were also found active during a routine audit. Emergency fire protection systems were outdated and untested for two years.

Key compliance aspects to test:

- Were physical access authorizations regularly reviewed?
- Were visitors escorted and logged properly?
- Was access monitoring conducted and logs reviewed monthly?
- Were physical access devices inventoried and updated regularly?
- Was facility penetration testing performed annually?
- Was fire protection equipment operational and tested recently?