Andree Salvo

Southern New Hampshire University

CYB 400

2-2 Journal: Systems Thinking in IT Audits

Instructor: Robert Chubbuck

When you apply systems thinking to IT audits, reviewing potential regulatory requirements is a critical step because organizations often can operate under legal and industry standards that dictate how systems and data must be handled. Regulations such as HIPAA, PCI DSS, or GDPR can impose to strict guidelines on security and privacy, and failing to meet them can result in legal penalties, financial loss, and damage to reputation. When you keep these requirements in focus, auditors will ensure that the organization's systems are evaluated not just for internal effectiveness but also for compliance with external expectations. This approach highlights how different parts of the system, technology, processes, and people are interconnected within broader regulatory environments.

When it comes to identifying both in and out of scope for the audit. If you don't have clear boundaries, audits can become unfocused and overlook critical risks or a waste of time on irrelevant areas. Scope definition enables auditors to focus resources on the most significant systems, data, or processes, recognizing dependencies that may indirectly impact them. However, defining critical requirements for the audit provides a clear standard for what success looks like. Suppose you ensure that the audit objectives align with organizational goals, regulatory expectations, and stakeholder needs. Together, these steps create a structured, system-oriented approach that enables auditors to understand how each decision or control influences the larger organizational system.