Overview of is audits (ip)

Technology, Information Technology

ASSIGN BUSTER

Full Paper Overview of Information System Audit Prior to performing any network audit, the scope is recognized by the audit charter. Likewise, the primary objective is to foresee the impact of directional changes and their implementation on the Information Technology function. However, for reaching success, it is vital for the business to understand auditor’s role. Moreover, IT auditors facilitate the organization for aligning business goals with IT applications along with the assurance of system protection, system availability and system integrity. As the principle objective of an auditor is assurance, it is the responsibility of the management to ensure the types of controls that are operational where required. The role of an IS auditor has evolved with new advancements in technology (Information systems control & audit1999). The information system cannot be considered only as a computing station, as it is comprised of many elements for facilitating business processes that will contribute to one of the business objectives. However, there is still no guarantee for the level of protecting these business systems demonstrates. Likewise, the most common vulnerability can be considered as the total strength. The first element for IS audit is the physical and environmental review. Likewise, this element incorporates physical security, supply of power, temperature control and other associated environmental factors. The second element is the system administration review, as it incorporates operating systems, system administration, procedures and compliance and database management and administration. The third element is the application software review. This review involves the processes associated with the payroll, invoicing, online customer order processing system, entity resource planning etc. however, review of complex and integrated application requires authorizations & access control, exception handling , and it travels within the application and controls and procedures. The fourth element will be the network security review that incorporates internal and external connectivity with the system, firewall, network security, access control list defined in routing devices, port scanning and detection of typical domains. The fifth element is the business continuity review. This review is critical and includes redundancy and maintenance of components such as hardware, software, backups, redundant WAN links, storage all documented and tested disaster recovery plan. The sixth element is the data integrity review that incorporates examination of live data for validating the appropriateness of controls and its impact of limitations. Likewise, this type of testing is conducted by using traditional auditing software and tools such as computer assisted audit techniques. A committee comprising of senior managers is essential for conducting a formal audit, as this group involving stakeholders provide audit charter, scope, oversight issues, along with the project plan with tentative deadlines. The committee discusses and resolves issues that facilitate the audit process in a smooth way. Likewise, after the completion of audit evaluation, findings and suggestions are communicated via a presentation to the senior management for corrective actions. This methodology assures through understanding, as it enhances buy-in for recommendations from audit. Moreover, it also provides an extra channel for the auditors to review the raised issues. In the end, a report is made that already incorporates issues that were also discussed and debated comprehensively and hence, the effectiveness of the report enhances considerably. References References Information systems control & audit (1999). Pearson Education.