Information Systems and Audit Planning at ABC Company

Posted on October 2, 2018

Business Overview:

ABC Company is involved in a wide range of business elements that give business process services to the money-related services industry. ABC includes fifteen Operating Segments and forty-two Business Segments. A large number of these fragments have developed from various purposes of source (e.g., by means of obtaining, by means of an entrepreneurial startup, through earlier rearrangements); along these lines, numerous keep on operating in a fairly independent manner, both from a business viewpoint and from an innovation point of view. In a half year since the corporate level rearrangements, extraordinary steps have been made to adjust the specialty units and to convey lucidity to ABC's general system and vision. The new Executive Management group is clear in their sponsorship of conveying end-to-end answers to their clients, which will bring about expanded market entrance and expanded general incomes. This sponsorship includes the business viewpoint as well as the innovation angle.

The head office of ABC company is located in New York, United States. Its other offices are established in different cities of the United States. They have distributed networking system having all their business process centrally synchronized. The company is planning an IT infrastructure auditing for compliance.

Scope:

The Scope of this audit plan will be central to ABC's Company network. It includes the evaluation of IT infrastructure that accurately supports the business processes and operations. The scope of this audit also includes the security controls and measures applied in the network. The audit will also confirm whether the company has implemented the rules and standards according to its own and government policies. Moving further, this audit plan will ensure that the company is working according to the implemented policies.

Goals And Objectives:

The goal is to implement proper security controls for the company's information systems. (ISACA, 2018) We will examine the company's IT infrastructure and computer network and determine the security flaws and errors that can lead to a security breach. The audit will target the alignment of

ABC’s business strategy with IT infrastructure and IT security.

Audit Frequency:

The audit will be conducted after every three to five years, and it will be proportional to the risk assessment. However, we will also conduct quarterly audits.

Duration Of Audits:

The duration of the audit will be based on the type of audit we want to conduct at the time. There are many software available that can assist in conducting regular audits. The duration of quarterly audits will be from two weeks to one month. The high-intense audit duration will vary as we will be verifying that the IT infrastructure is assisting the business operations without any error or flow. The highly intense audits will usually take at least two months.

Identifying The Critical Requirements Of The Audit:

Before conducting an audit, we will identify the critical requirements of the organization which need to be critically analyzed. Firstly, we will analyze the degree of the systems and geographic centralization. We will analyze whether the organization has truly implemented the centralized organizational structure as it will affect the allocation of IT resources. We will figure out and inspect the technologies that have been implemented. There might be a huge assorted variety at any level of the IT stack, justifying examination in a particular application’s program code, database, operating system, and network foundation. We will inspect the quality of customized software components and whether such customization is according to the policies of the organizations. Is there appropriate technical support for the customized software available in the organization? We will examine and evaluate the intensity of company policies and standards that define IT governance. An association’s regulatory prerequisites must be considered in the scope of risk characterization and IT audits. Any association enrolled with the Securities and Exchange Commission is required by the Sarbanes-Oxley Act to provide details regarding the adequacy of their inside policies for monetary reporting. This audit planning includes the inspection of the level of operational standardization. This will affect the dependability and perfection of the IT foundation and related procedures. We will analyze an association’s IT infrastructure by evaluating the level of dependence on innovation in that association. The more an association depends on the accessibility and usefulness of various innovations in the IT world in everyday business tasks, the more the potential hazard increments. Moreover, we will analyze the critical components of ABC’s IT network. We will analyze the devices such as firewalls, routers, switches, and DMZ and whether they are installed appropriately to provide the information security that flows across the network. We will also audit the installation of IPS/IDS. We will inspect the rules defined in the firewalls so that the firewalls are accurately securing the network from

attackers.

Privacy Laws:

We will audit the privacy and security controls implemented in the organization to determine whether they are according to the rules and regulations defined by the Federal Information Management Act (FISMA). It is a United States legislation that consists of a complete framework to secure information systems in federal agencies against threats. It is also known as the E-government Act, signed in 2002. This Act is complete and comprehensive, and it has also been enacted by the private sector to effectively deal with threats and secure critical information assets of an organization. The main objective of FISMA is to develop a policy of risk analysis and mitigation to achieve cost-effective security. The Government enforces this act to ensure that the federal government and agencies secure their information assets by adopting risk analysis and mitigation strategies.

FISMA is responsible for assigning duties to federal agencies, the Office of Management and Business, and the National Institute of Standards and Technology(NIST). (Joint Task Force Transformation Initiative, 2012) The NIST is a non-regulatory government agency. It is responsible for developing technology metrics and guidelines. Federal agencies or government organizations that comply with NIST may also further ensure compliance with FISMA as NIST guidelines direct organizations to comply with FISMA. NIST has provided nine rules to move towards FISMA compliance. It is compulsory for U.S-based organizations to adopt the standards developed by NIST to initiate innovation and economic competitiveness. The FISMA is an Act released by the United States Congress, governed by the United States Government. The Government, through this Act, ensures that other IT organizations and federal agencies must secure their information assets. Hence, the government took this step to implement the security strategies adopted by other organizations that are beneficial for the United States' security interests.

Assessing The IT Security:

Analyzing IT security is an important part of reviewing the IT infrastructure for compliance. Through audits, we can find fraud, inefficient IT procedures, inaccurate utilization of IT resources, and weak security. The IT security is tested to ensure that the security controls are accurately placed. In order to assess IT security, we need to know about and implement risk management.

Risk Management:

In the risk management process, the threats are identified, assessed, and controlled. These threats affect the organization's business process, capital, and earnings. These threats originated from many sources, which include financial unpredictability, natural disasters, and strategic management flaws. The security threats related to IT infrastructure and information risks are mitigated by risk

management strategies. Resolving such risks and threats related to IT has become the top priority for today's companies. So, the risk management plan clearly addresses the identification and controlling of threats to its IT assets, which includes the security of critical information of organizations and other resources. The risk management plan also addresses the strategies to resolve such risks. Our audit will include the proper analyses of the risk management plan, ensuring that it has accurately identified all possible risks and threats to IT infrastructure and corrects strategies adopted to resolve such risks.

Threat Analysis:

Cyber threat examination is a procedure in which the learning of interior and outside data vulnerabilities correlated to a specific association is coordinated against true cyber assaults. As for cyber security, this threat-situated way to deal with fighting cyber assaults shows a smooth change from a condition of receptive security to a condition of proactive one. In addition, the expected result of a threat appraisal is to give best practices on the most proficient method to expand the defensive instruments for accessibility, privacy, and completeness without swinging back to ease of use and functionality conditions.

References

ISACA. (2018). *COBIT 2019 framework: Introduction and methodology*. https://www.isaca.org/resources/cobit

Joint Task Force Transformation Initiative. (2012). Guide for conducting risk assessments (NIST SP 800-30 Rev. 1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-30r1