Information Systems and Audit Planning at ABC Company

Posted on October 2, 2018

View this essay online:
https://academic-master.com/information-systems-and-audit-planning-at-abc-company/

Business Overview:

ABC Company is involved in a wide range of business elements that provide business process services to the financial services industry. ABC includes fifteen Operating Segments and forty-two Business Segments. A large number of these segments have developed from various sources (e.g., through acquisitions, entrepreneurial startups, or earlier rearrangements); along these lines, many continue to operate in a fairly independent manner, both from a business viewpoint and from an innovation point of view. In the 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 its sponsorship of conveying end-to-end answers to its 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 a distributed networking system with all their business processes centrally synchronized. The company is planning an IT infrastructure audit for compliance.

Scope:

The scope of this audit plan will be centered on ABC Company's 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 policies 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 every three to five years, and its frequency 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 programs available that can assist in conducting regular audits. The duration of quarterly audits will be from two weeks to one month. The duration of high-intensity audits will vary, as we will be verifying that the IT infrastructure is assisting the business operations without any error or flaw. 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 that need to be critically analyzed. Firstly, we will analyze the degree of system 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 identify and inspect the technologies that have been implemented. There might be a huge variety at any level of the IT stack, justifying examination of 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 organization. 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 its internal policies for financial 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 increases. Moreover, we will analyze the critical components of ABC's IT network. We will analyze devices such as firewalls, routers, switches, and the DMZ and determine whether they are installed appropriately to provide security for the information

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 accurately secure 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 Security Management Act (FISMA). It is a United States law that consists of a complete framework to secure information systems in federal agencies against threats. It is also known as part of 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 federal 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 Budget, and the National Institute of Standards and Technology (NIST) (Joint Task Force Transformation Initiative, 2012). 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. FISMA is an Act passed by the United States Congress and 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. 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, threats are identified, assessed, and controlled. These threats affect the organization's business processes, capital, and earnings. These threats originate 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 control of threats to its IT assets, which include 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 analysis of the risk management plan, ensuring that it has accurately identified all possible risks and threats to IT infrastructure and that correct strategies have been adopted to resolve such risks.

Threat Analysis:

Cyber threat examination is a procedure in which knowledge of internal and external data vulnerabilities correlated to a specific association is coordinated against real cyber assaults. As for cybersecurity, this threat-oriented way of dealing with cyber assaults shows a smooth change from a condition of reactive security to a proactive one. In addition, the expected result of a threat appraisal is to provide best practices on the most proficient method to expand the defensive instruments for accessibility, privacy, and completeness without compromising 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