Commentary

Inspection Process in all Organizations through Accounting Audit

Huihui Xiao*

Department of Accounting and Corporate Governance, Macquarie University, Sydney, Australia

DESCRIPTION

A physical inventory check is followed by an auditor's review or inspection of various books of accounts to ensure that all departments are using the same documented system of documenting transactions. For an effective audit of Internet of Things (IoT) networks and devices, IT auditing firms must have the right resources. IT auditing is of utmost importance as the world becomes more digital. Due to the common subject of risk assessment and controls, IT auditors can help firms in a variety of distinct sectors of expertise. To a certain extent, the majority of businesses rely on the Internet to access various applications and interact with data, facilitated through a network that is supported by physical infrastructure a certain extent, most businesses use the Internet to access a variety of applications and interact with data, which is often over a network that relies on physical infrastructure.

Society has recently started to move away from the old IT infrastructure as businesses begin to incorporate cloud computing, IoT technology, and artificial intelligence into their everyday operations. The implementation of more IoT devices in a number of industries has improved the usability of simple tasks for workers, clients, and other stakeholders. An organizational network cannot be accurately and completely assessed by using traditional IT auditing standards and techniques to examine IoT devices. Such erroneous auditing reports might cause even more serious issues, such as (a) the business's denial that the IT infrastructure is in top condition.

A suitable IoT auditing framework is required to direct the process and give the most effective network with the least amount of risk. This not only underlines the usefulness of IoT devices but also the significance of the differences and the necessity for regulation. Compared to traditional IT infrastructure, there are more IoT components that are susceptible to hostile behavior. Simply put, in order to give correct recommendations for IoT devices, an auditing framework for IoT devices must be created. During an audit, it is essential to consider the unique features of IoT devices, including scalability and autonomous operations. To streamline the process and facilitate

rapid understanding of IoT characteristics, they need to develop a customized questionnaire that precisely addresses the aspects we focus on while auditing IoT devices. They need to take into account the hardware, network, firmware, logical/physical security, and privacy audits when it comes to IoT device auditing. We must also take into account how employees will use technology within the organizations. An IoT auditing framework is provided in this research paper, and the framework's functionality is supported by examples and case studies.

The regulatory, legal, and business environments of organizations have changed, and audit techniques have developed to reflect these developments. Business Risk Auditing which began in sizable audit firms in the late 1990s and is now extensively used, is one of these novel audit approaches. One important aspect of BRA (Business Risk Auditing) is that it analyzes and evaluates the risk that a company won't achieve its business objectives because of internal and external hindrances. The typical risk audit methodology is transaction-based (a bottom-up approach), compliance-oriented, and focuses on risks related to transactions and specific accounts.

Contrarily, under Business Risk Auditing, an auditor first evaluates business risk by doing a strategic analysis of a client's company environment, business processes, as well as the related internal control systems. The auditor then evaluates how the preparation of financial statements by managers is impacted by business risk. Numerous national and international standard-setters have adopted Business Risk Auditing, and it is also employed by numerous auditing firms. Because of this, it is believed that the real impact of Business Risk Auditing will be critical to both the future strengthening and viability of the market for audit services and the social significance of the audit function itself.

CONCLUSION

Early-career auditors, those with four years' experience or fewer, were the focus of semi-structured interviews. Having just finished their education, this population is in a great position to offer perspective on Allowance for Doubtful Accounts (ADA) within

the audit curriculum. In NSOEs but not in SOEs, their find that BRA adoption has an incrementally favorable impact on the link between business risk and audit hours. We discover that an increase in audit hours corresponds to an improvement in audit quality, as expected. Auditing these intricate infrastructures is difficult because there isn't a specific IoT auditing methodology.