OPEN ACCESS Freely available online

ISSN: 2472-114X
International Journal of Accounting Research

Opinion Article

Strategic Analysis in Business Risk Auditing

Habibi Xeng*

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

DESCRIPTION

After a physical inventory check, an auditor reviews or inspects various books of accounts to ensure that all departments use the same established procedure for tracking transactions. IT auditing organizations must have adequate resources to conduct an efficient audit of Internet of Things (IoT) networks and devices. IT auditing is becoming important as the world gets more digital. Because risk assessment and controls are such frequent topics, IT auditors may assist businesses in a wide range of industries. To some extent, the majority of businesses rely on the internet to access various apps and interact with data, which is facilitated by a network supported by physical infrastructure. To some extent, most organizations utilize the internet to access a variety of applications and interact with data, which is frequently over a network that relies on physical infrastructure.

Society has recently begun to shift away from traditional IT infrastructure as firms integrate cloud computing, IoT technology, and artificial intelligence into their daily operations. The increased use of IoT devices in a variety of industries has enhanced the usability of simple activities for employees, clients, and other stakeholders. Traditional IT auditing standards and procedures cannot accurately and comprehensively assess an organization's network when examining IoT devices. Such incorrect auditing reports may lead to even more significant difficulties, such as the company's denial that the IT infrastructure is in top condition.

An appropriate IoT auditing framework is necessary to guide the process and provide the most effective network with the lowest level of risk. This demonstrates not only the use of IoT devices, but also the importance of differences and the need for regulation. Compared to traditional IT infrastructure, IoT components are more vulnerable to malicious activities. Simply said, an auditing framework for IoT devices is required in order to make accurate suggestions. During an audit, it is important to evaluate the specific aspects of IoT devices, such as scalability and autonomous operation.

To shorten the process and promote rapid comprehension of IoT features, they must create a customized questionnaire that meets the specific areas their focus on when auditing IoT devices. When auditing IoT devices, they must consider hardware, network, firmware, logical/physical security, and privacy. They must also consider how employees will use technology within their firms. This study provides an IoT auditing framework, including examples and case studies to support its capabilities.

Organizations regulatory, legal, and business environments have changed, and audit procedures have evolved. Business risk auditing, which originated in large audit firms in the late 1990s and is now widely employed, is one of these unique audit methodologies. One essential component of BRA (Business Risk Auditing) is that it studies and assesses the risk that a firm will fail to meet its business objectives due to internal and external barriers. The standard risk audit methodology is transaction-based (a bottom-up approach), compliance-oriented, and focuses on risks associated with transactions and specific accounts.

In contrast, under business risk auditing, an auditor first assesses business risk by conducting a strategic analysis of a client's firm environment, business processes, and internal control systems. The auditor then assesses how company risk influences manager-prepared financial statements. Business risk Auditing has been embraced by various national and international standard setters, as well as by a large number of auditing companies. As a result, it is expected that the true impact of Business Risk Auditing will be critical to both the future strength and viability of the audit services market and the social significance of the audit function itself.

Semi-structured interviews were conducted with early-career auditors, namely those with four years or less of experience. Having recently completed their schooling, this group is well-positioned to provide feedback on Allowance for Doubtful Accounts (ADA) within the audit curriculum. In NSOEs but not SOEs, they discovered that Banking Regulation Act (BRA) adoption has an incrementally positive impact on the relationship between business risk and audit hours. We discover

Correspondence to: Habibi Xeng, Department of Accounting and Corporate Governance, Macquarie University, Sydney, Australia, E-mail: habibixeng@acc.au

Received: 03-Jun-2024, Manuscript No. IJAR-24-26330; **Editor assigned:** 05-Jun-2024, Pre QC No. IJAR-24-26330 (PQ); **Reviewed:** 20-Jun-2024, QC No. IJAR-24-26330; **Revised:** 26-Jun-2024, Manuscript No. IJAR-24-26330 (R); **Published:** 05-Jul-2024, DOI: 10.35248/2472-114X.24.12.383

Citation: Xeng H (2024) Strategic Analysis in Business Risk Auditing. Int J Account Res.12:383.

that increasing audit hours results in an improvement in audit quality, as expected. Auditing these complex infrastructures is challenging because there is no specialized IoT auditing technique.