

**IT Risk Management in the Communications, Space, and Technology Commission in
Riyadh**

Name of Student

Course Name and Code

Professor

Institution

Date

IT Risk Management in the Communications, Space, and Technology Commission in Riyadh

Introduction

The dynamic and constantly changing panorama of technical innovation in Saudi Arabia is anchored by the Communications, Space, and Technology Commission located in Riyadh. The Commission is leading the charge in determining the direction of technology in this country at a period of unrelenting advancement and invention (Scholl & Suloway, 2021). Its mandate includes supervising and controlling the technology, space, and telecommunications industries to make sure they are in line with the Kingdom's overall modernization and advancement goals. The Commission is confronted with a multitude of complex and diverse challenges as the digital sphere grows and technological frontiers are pushed farther. Of these, information technology (IT) risk management is one of the most critical (Piekiet Weeserik & Spruit, 2018). These difficulties are a result of the rapid advancement of technology, which has created a multitude of new opportunities as well as a number of hazards and weaknesses. An integral part of the Commission's activities is IT risk management. Upholding the integrity and credibility of the Commission itself is just as important as protecting sensitive data and guaranteeing the uninterrupted operation of vital services. Any errors or inadequacies in this area might have negative effects, such as data loss, security breaches, and even interruptions to the Commission's essential operations. The goal of this study project is to conduct a thorough analysis of the nuances of IT risk management procedures used by the Communications, Space, and Technology Commission in Riyadh. It seeks to go in-depth with the tactics, procedures, and safeguards the Commission has put in place to lessen risks associated with IT. It also aims to pinpoint the main problems and difficulties that have arisen as a consequence of the quickly changing technological environment. The hazards that come

with technology are always changing, so it's critical to evaluate how well the Commission's present risk management procedures are working.

Research Problem

One of the most important organizations in charge of monitoring and controlling the quickly changing communications, space, and technology scene is the Communications, Space, and Technology Commission (CSTC) in Riyadh. Effective IT risk management has evolved from a need to a strategic imperative in this changing environment. The CSTC handles more sensitive data and cutting-edge technologies as technology develops, which exposes the company to a variety of IT-related dangers. There is a clear vacuum in the field of IT risk management research, despite the field's recognition of its significance. The particular possibilities and difficulties the CSTC faces in the field of IT risk management are not well understood. Due to this vacuum, the Commission is exposed to hazards that are not recognized and handled and might jeopardize both its goals and the interests of the country it represents. This study aims to close this gap by taking a close look at the CSTC's IT risk management procedures, guidelines, and tactics. It seeks to pinpoint the particular difficulties the CSTC has in handling IT risks as well as any room for development. In doing so, this research will increase the Commission's role in encouraging the responsible and secure growth of the communications, space, and technology sectors inside Riyadh and help to improve its capacity to protect sensitive data and vital technologies.

The Importance and Objectives of the Research

The goal of this research is to improve the Communications, Space, and Technology Commission's IT risk management procedures, which makes it extremely important. The following are the main objectives:

- Determining the Commission's main problems and obstacles with IT risk management.
- Assessing the efficacy of the present IT risk management procedures.
- Making suggestions and offering tactics to enhance IT risk management.

Research Hypothesis

We hypothesize that the constantly changing technological world presents substantial IT risk management issues for the Communications, Space, and Technology Commission in Riyadh. We anticipate identifying gaps in their present IT risk management procedures.

Literature Review

IT Risk Management

Organizations in a variety of industries must prioritize effective IT risk management because of the constantly changing nature of technology and the resulting vulnerabilities. Information technology and data security risks must be identified, evaluated, and mitigated as part of IT risk management (Force, 2018). As technology develops, this field's importance has increased dramatically and companies are becoming more and more dependent on digital systems and data. IT risk management principles are provided by a number of well-known frameworks and approaches, including ISO 27001, NIST Cybersecurity Framework, and COBIT; nevertheless, the environment in which they are implemented can have a substantial impact.

Technology Advancements

One of the main reasons that strong IT risk management is necessary is the quick pace of technological advancement. Organizations must modify and advance their risk management methods in light of the expanding attack surface that emerging technologies like the Internet of Things (IoT), artificial intelligence, and 5G networks have created (Halili, 2019). Further complications have been brought forth by the widespread use of cloud computing and mobile devices. These developments highlight how crucial it is to match IT risk management with more general technology developments in order to guarantee the safety and uninterrupted functioning of business activities.

Best Practices in Governmental Organizations

Effective IT risk management is essential for governmental entities to safeguard sensitive data, uphold public confidence, and guarantee the uninterrupted provision of essential services. Proactive risk assessment, security frameworks, and regulatory compliance are frequently combined in best practices (Epstein, 2018). Governmental organizations from all around the world have created rules and laws to assist with risk management initiatives because they understand how important these practices are.

IT Risk Management in Governmental Commissions

Since there isn't much research on IT risk management in government commissions, the Communications, Space, and Technology Commission (CSTC) in Riyadh is a particularly interesting case study. Commissions established by the government, such as the CSTC, have specific goals, duties, and tasks. Understanding the particular difficulties encountered by these

commissions requires research in this area, particularly in light of the quickly developing technology landscape.

Research Methodology

The research will adopt a mixed-methods approach. Quantitative data will be collected through the use of surveys that will be distributed among Commission employees, while qualitative data will be gathered through the use of in-depth interviews with IT specialists and management. This approach will offer a more comprehensive view of the current state of IT risk management within the Commission.

Research Limits

The objective of this study is to offer significant perspectives on the field of IT risk management at the Communications, Space, and Technology Commission (CSTC) located in Riyadh. It is important to recognize certain constraints that may affect the extent and applicability of the results.

1. **Access to Sensitive Data:** The possible restriction on access to private and sensitive data within the CSTC is one of the study's main limitations. Secret information is usually handled by government agencies, and other researchers may not be permitted access to some material. A thorough examination of all potential IT hazards and mitigation techniques may be hampered by this constraint.
2. **Employee Reluctance:** Workers and staff at the CSTC could be reluctant to divulge private information about IT risk management. Afraid of the consequences or worries about privacy may prevent open answers in surveys or interviews. This hesitation might lead to an inaccurate representation of the IT risk environment.

3. **Context-Specific Findings:** The only subject of this study is the CSTC in Riyadh, which has a distinct function and purpose within Saudi Arabia's regulatory framework. Since various governmental commissions and organizations may face different legislative frameworks, technical landscapes, and IT risk management concerns, the conclusions may not be immediately relevant to them.

General Perception of the Research

Structure The research will be structured as follows:

- Introduction: Providing an overview of the research topic and its significance.
- Research Problem: Determining the particular difficulties with IT risk management.
- Importance and Objectives: Outlining the significance and research objectives.
- Research Hypothesis: Outlining the anticipated results.
- Literature Review: A summary of pertinent research and body of knowledge
- Research Methodology: Describes the data gathering, analysis, and research strategy in detail.

References

- Epstein, M. J. (2018). *Making sustainability work: Best practices in managing and measuring corporate social, environmental and economic impacts.*
- Force, J. T. (2018). Risk management framework for information systems and organizations. *NIST Special Publication, 800, 37.*
- Halili, S. H. (2019). Technological advancements in education 4.0. *The Online Journal of Distance Education and e-Learning, 7*(1), 63-69.
- Pieket Weeserik, B., & Spruit, M. (2018). Improving operational risk management using business performance management technologies. *Sustainability, 10*(3), 640.
- Scholl, M., & Suloway, T. (2021). Introduction to cybersecurity for commercial satellite operations. *National Institute of Standards and Technology, Tech. Rep.*