

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

Abdullah Bakheet Alzahrani

Final Project and MGM697

DR. AlFaisal

Everyone's Smart University (ESU)

MIDOCEAN UNIVERSITY

16/12/2023

## Table of Contents

|                                                      |    |
|------------------------------------------------------|----|
| Introduction .....                                   | 3  |
| Literature Review .....                              | 5  |
| Defining IT Risk Management and Its Importance ..... | 5  |
| Frameworks and Approaches .....                      | 5  |
| Impact of Technological Advancements .....           | 6  |
| Best Practices in Governmental Organizations .....   | 6  |
| Lack of Research in Government Commissions .....     | 7  |
| Research Methodology .....                           | 8  |
| Mixed-Methods Approach .....                         | 8  |
| Rationale for Mixed-Methods .....                    | 8  |
| Survey Distribution and Interview Selection .....    | 9  |
| Research Limits .....                                | 10 |
| Impact on Study's Scope and Findings.....            | 11 |
| Data Analysis and Findings .....                     | 12 |
| Recommendations and Tactics for Enhancement .....    | 19 |
| Comprehensive Training Programs.....                 | 19 |
| Adaptive Frameworks .....                            | 20 |
| Resource Allocation .....                            | 21 |
| Regulatory Compliance Monitoring.....                | 22 |
| Collaborative Governance .....                       | 23 |
| Incident Response Plans.....                         | 24 |
| Conclusion .....                                     | 25 |
| References.....                                      | 29 |

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

### **Introduction**

Technological innovation in this initiative presently centralizes the mandate of Riyadh's Communications, Space, and Technology Commission (CSTC). Suggested for sitting at the helm of defining the technology dreams of the nation, the CSTC takes a leading in position in harmonizing and defining the technological, space, and telecommunication industries with the guiding pillars of modernization and progress that cover Saudi (Scholl & Suloway, 2021). The CSTC departments must understand that the industry is a living and ever-changing world of innovation, hence have to look inwards on the responsible duties of overseeing and controlling the CSTC industry by finding the right balance between harnessing new opportunities and mitigating new threats as well as exposures arising from the current uses of technologies (Pieket Weeserik & Spruit, 2018). Risk management in Information Technology (IT) is the most important area whose many-sided duties lie at the core of the Commission. Among them the CSTC, the fast pace of technological evolution has brought many opportunities and, at the same time, threats for organisations. This research identifies the centrality of IT risk management in the scope of CSTC activities and recognizes it as an indispensable facet in upholding the Commission's integrity, credibility and the seamless operation of the vital services. The imperative covers not only the protection of sensitive information but also the major issue ensuring that operations are not interrupted and that consequences such as a breach or weak security do not have an adverse effect (Pieket Weeserik & Spruit, 2018). Against this entire backdrop, the research problem comes on board as a gap in developing a clear understanding of various issues that are linked to IT risk management within the boundaries of the CSTC. Despite the existence of its recognised

significance, there still exists a notable level of deficiency when it comes to comprehending various forms of specific challenges and opportunities that is capable of being encountered by CSTC within the boundaries of this domain. On the other hand, the absence of a comprehensive level of understanding of various intricacies that are associated with IT risk management places the entire Commission at a serious potential risk since all the unidentified and unaddressed hazards are likely to compromise all its overarching goals and, by extension, the interests of the nation. Consequently, the entire study majorly aims to bridge this existing void by conducting an exhaustive mode of analysis of the CSTC's IT risk management procedures, digging deep into various tactics, processes and even safeguards that are implemented by the Commission with an intention of mitigating various risks that are fully associated with IT. It also focuses on the identification of different primary challenges together with difficulties that are likely to emerge from the rapidly changing technological landscape, acknowledging that different hazards that are linked to technology are more dynamic to an extent of necessitating a continual mode of evaluation of effectiveness of the Commission's existing risk management procedures. In relation to objectives, the research aims to attain a multifaceted agenda. Firstly, it aims to pinpoint the Commission's major challenges together with obstacles in the realm of IT risk management. Simultaneously, it also aims to critically carry out an evaluation of the effectiveness of the existing IT risk management procedures that are capable of being employed by the CSTC. On the other hand, the research also aims to offer more concrete forms of recommendations and tactics that are all aimed at enhancing Commission's IT risk management practices. Moreover, the overarching hypothesis that guides this study clearly posits that the constantly evolving technological milieu introduces various forms of substantial challenges for the CSTC in relation to IT risk management, and through the research, various gaps in the existing procedures will all be identified for the

purposes of targeted improvements. As a result, the significance together with objectives of this research majorly converge towards fortifying the CSTC's capacity to be able to navigate the responsible and more secure growth of the communications, space, together with technology sectors within Riyadh while at the same time ensuring the protection of different forms of sensitive data together with vital technologies.

## Literature Review

### Defining IT Risk Management and Its Importance

Information Technology (IT) risk management is one of the most critical facets for different types of organizations known to be existing within various industries. Moreover, it is all about the identification, assessment together with the mitigation of different types of risks that are associated with the use of various forms of information technology systems and data (Fan & Stevenson, 2018). Furthermore, the overall importance of IT risk management majorly lies on its role as a proactive strategy to adequately safeguard against quite a number of potential disruptions, breaches together with various forms of unauthorized access (Willumsen, Oehmen, Stingl & Geraldi, 2019). The implementation of an effective risk management always ensures that there is resilience of different organizations within the face of this evolving technological landscape, scaling up their ability to obtain various objectives in a secure manner.

### Frameworks and Approaches

Quite a number of frameworks and approaches tend to guide various organizations when it comes to the implementation of more robust IT risk management practices. ISO 27001 offers a more comprehensive combination of various standards for information security management, making sure that there is a higher level of confidentiality, integrity together with the availability of various forms of information. On the other hand, the NIST Cybersecurity Framework offers a risk-based kind of an approach towards managing cybersecurity risk, offering different types of

guidelines for organizations to carry out an assessment and improvement of their respective cybersecurity posture. COBIT (Control Objectives for Information and Related Technologies) is also another critical framework that is specifically tailored to governance and management of enterprise IT, offering a combination of various best practices together with controls for IT processes. These types of frameworks offer a perfectly structured foundation for different types of organizations, aiding in the systematic identification together with the management of IT risks.

### Impact of Technological Advancements

Different types of technological advancements including the rise of the Internet of Things (IoT), artificial intelligence, together with 5G networks, have ended up significantly expanding the entire attack surface for a vast range of different organizations (Dragan et al., 2018). Furthermore, IT risk management must adequately evolve in tandem with all these forms of technological shifts in order to address new forms of vulnerabilities together with quite number of potential threats. The widespread adoption of cloud computing together with different types of mobile devices further complicates the entire risk landscape, putting much emphasis on the need for different types of organizations to adequately align their respective risk management strategies with all the emerging technologies in order to ensure that there is safety and continuity of their respective modes of operations (Raja & Priya, 2021).

### Best Practices in Governmental Organizations

An effective IT risk management is very critical for various governmental organizations for the purposes of safeguarding different types safeguard sensitive data, maintaining higher levels of public trust, and also ensuring that there is a continuous delivery of various forms of essential services (Mahama, Elbashir, Sutton & Arnold, 2022). On the other hand, various forms of proactive risk assessments, adherence to various forms of security frameworks together with compliance with different types of regulations are some of the most integral components of best

practices in governmental IT risk management. Different types of governments worldwide have established various rules and laws to guide various forms of risk management initiatives, recognizing the critical nature of all these practices in preserving national security and public welfare (Alijoyo & Fisabilillah, 2021).

### Lack of Research in Government Commissions

The boundaries of IT risk management in various government commissions still remains to be relatively unexplored across academic literature. This lack of research is majorly pronounced in the case of communications like the Communications, Space, and Technology Commission (CSTC) in Riyadh. Government commissions, with all their unique goals, responsibilities, and tasks, present quite a number of specific challenges within the boundaries of IT risk management. This entire research gap accentuates the significance of investigating the CSTC as a unique case study, shedding more light on various particular challenges together with opportunities encountered by such government entities when it comes to managing IT risks in an effective manner. Thee literature review offers an in-depth mode of exploration of IT risk management. Focusing into its definition, importance together with frameworks that guide its entire implementation. It perfectly highlights the evolving impact of various forms of technological advancements, discusses some of the best practices in various governmental organizations, and also underscores the scarcity of research within the context of various government commissions, setting a platform for the subsequent analysis of the CSTC in Riyadh.

## Research Methodology

### Mixed-Methods Approach

The entire research was able to take into consideration a mixed-methods approach where it adequately combined both quantitative and qualitative methods, to offer one of the most comprehensive levels of understanding associated with IT risk management within the boundaries of the Communications, Space, and Technology Commission (CSTC) in Riyadh. Moreover, the utilization of various surveys together with in-depth interviews perfectly creates one of the best opportunities for the triangulation of data thereby enhancing the overall validity and reliability of all the findings. Furthermore the qualitative component through surveys is in a position of generating various forms of numerical data that can be adequately analysed from a statistical perspective with an intention of offering a broad overview of different types of trends and patterns. Meanwhile, the qualitative dimension through the implementation of in-depth interviews provided some of the best insights together with a deeper level of understanding of all the contextual factors that are known to be influencing IT risk management practices.

### Rationale for Mixed-Methods

The integration of both the quantitative and qualitative methods was a process that was highly motivated by the whole desire to adequately capitalize on different types of strengths that are linked to both approaches. Moreover, the quantitative data extracted from the surveys offered one of the best opportunities for the measurement of different trends, identification of quite a number of prevalent issues together with the assessment of the overall level of effectiveness of different types of IT risk management procedures. Furthermore, the qualitative insights obtained from the in-depth interviews was able to adequately enrich the overall exploration of different types of complexities, challenges alongside various nuances that were not captured by the qualitative metrics alone. Moreover, the mixed method approach majorly aimed to offer one of the most

holistic views of the CSTC's historical IT risk management landscape, adequately recognizing the whole multifaceted nature of the entire subject.

### Survey Distribution and Interview Selection

The surveys were adequately distributed among different types of representative sample of CSTC employees, ensuring higher levels of diversity in different types of roles and responsibilities. As a result, this mode of inclusivity, highly facilitated a more comprehensive mode of assessment that is linked to different types of historical perceptions and experiences associated with IT risk management across various departments. Additionally, the survey questionnaire, majorly designed to capture the historical quantitative data on matters pertaining awareness, perceived effectiveness, together with specific challenges associated with IT risk management, was able to contribute to a quantitative understanding. Historical in-depth interviews were carried out with a purposively selected group of various IT specialists together with management within the CSTC. The whole selection of the interview participants took into consideration the historical expertise, experience together with a vast range of roles known to be existing within the boundaries of IT risk management. These interviews majorly aimed to elicit historical qualitative insights into the intricacies of IT risk management, thereby offering a deeper level of understanding of the entire historical decision making providing, different types of challenges encountered together with various opportunities that are meant for improvement. The ability to combine historical quantitative survey data and historical qualitative interview narratives triangulated findings, scaling up the rigor together with the comprehensiveness of historical research outcomes. In conclusion, the historical mixed-methods approach that was implemented within the boundaries of this research perfectly aligned with the overall complexity of the IT risk management domain within the CSTC, offering one of the most comprehensive historical understanding and also going as far as identifying different areas for enhancement.

## Research Limits

This research acknowledges and addresses quite a number of potential limitations that are in a position of impacting on the study's scope and findings. One of the major constraints is the challenge of access to different types of sensitive data existing within the Communications, Space, and Technology Commission (CSTC). Furthermore, different government agencies by nature, normally handle various forms of confidential information, and different materials might be restricted from any acts of external access. The limitations that are posed by the restricted access to both the private and sensitive data might be able to impact on the overall depth of the examination of potential IT hazards together with quite a number of mitigation techniques that are known to be existing within the CSTC. The inability to put much focus into specific forms of classified details could be able to limit the overall granularity of all the findings, most so the ones that are associated with the intricate nature of certain IT risk management protocols and strategies that are implemented by the Commission. Another potential limitation majorly pertains to issues associated with employee reluctance. There were times when the workforce at the CSTC showed some be hesitancy to divulge private information linked to IT risk management. This reluctance majorly emerged from different types of concerns associated with potential consequences of sharing specific sensitive details or even fears that could be linked to the privacy of some of their responses. Again, such types of hesitations manifested in less open responses during the implementation of the surveys and the interviews, further contributing to an incomplete or skewed representation of the IT risk environment within the Commission.

Context-specific findings presented another major challenge. The CSTC in Riyadh is majorly known to be operating within a specific legislative mode of framework, technical landscape together with socio-political context that is known to be unique to Saudi Arabia. While all these

context specific nuances appear to be very integral towards understanding different types of intricacies that are linked to IT risk management within the boundaries of the commission, they pose a serious limitation in relation to generalizability. The findings might end up not being directly transferable to other types of governmental commissions or even organizations facing different forms of legislative frameworks, technical landscapes, together with IT risk management concerns. Therefore, all the conclusions obtained from this study should be carefully contextualized within the specific parameters that are associated with the CSTC's operational environment.

### Impact on Study's Scope and Findings

These limitations collectively impact the overall scope together with generalizability of the entire study. Having a restricted access to sensitive data is capable of preventing an in-depth exploration of different types of IT risk management practices, which ends up creating some critical gaps when it comes to the understanding of the Commission's risk landscape. On the other hand, issues associated with employee reluctance could also end up introducing various aspects of bias into the obtained data, thereby impacting on the overall accuracy and completeness of different types of findings. Again, the context-specific nature that is linked to the CSTC's operations is a clear implication that the conclusion of the study might not be applicable from a universal perspective, thereby necessitating a cautious mode of interpretation of different types of results within the specific framework of the CSTC in Riyadh.

## Data Analysis and Findings

The survey that was carried out within the Communications, Space, and Technology Commission (CSTC) sought to obtain a vast range of insights from different sample of employees, offering a more comprehensive level of understanding of various perceptions together with experiences that are known to be related to IT risk management. Furthermore, the qualitative analysis of data was able to uncover a special spectrum of awareness levels together with perceived levels of effectiveness associated with different types of existing procedures. It was therefore much evident that the employees were able to generally recognize the significance of IT risk management within the CSTC, acknowledging its whole pivotal role when it comes to safeguarding the organization's operations. However, the entire analysis also indicated some notable need for the implementation of more comprehensive training programs. Different types of respondents were able to express the desire for quite a number of targeted initiatives that were all aimed at scaling up their respective levels of understanding of different forms of IT risk management practices. This finding therefore underscores the overall importance that is associated with continuous learning and development in order to ensure that different types of employees possess the right combination of knowledge and skills that are necessary for the purposes of navigating the dynamic landscape of IT risks effectively. Additionally, a substantial portion of different respondents were able to voice their respective concerns regarding the overall level of integration of different types of emerging technologies such as the Internet of Things (IoT) and Artificial Intelligence (AI), into the existing risk management frameworks. This mode of apprehension clearly reflects different types of challenges that are associated with the implementation of various current procedures in order to accommodate the whole evolving technological landscape. Again, it also highlights the critical need for various forms of proactive measures like updating policies and procedures, to address the specific risks introduced by these

emerging technologies. The survey results tend to offer one of the most nuanced levels of understandings of the perspectives of different employees within the CSTC regarding IT risk management.

The in-depth interviews that were carried out by major IT specialists together with the management team within the Communications, Space, and Technology Commission (CSTC) added a layer of depth to the data analysis, providing quite a number of quantitative insights that were able to complement the quantitative findings. Through the interviews, a clear level of understanding emerged in relation to the intricate challenges encountered by the CSTC in effectively managing IT risks. One of the major themes that emerged during the implementation of the interviews was the formidable impact of the entire rapid pace of various forms of technological advancements on the Commission's IT risk management landscape. The interviewees were able to underscore the whole perpetual evolution of technology as one of the major hurdles that require a constant mode of adaptation of various forms of risk management strategies. Moreover, the dynamic condition of the technological environment adequately introduces various forms of novel risks together with vulnerabilities, demanding agility and proactive measures in order to stay ahead of potential threats. The insights that were obtained from these interviews shed more light on the continuous and dynamic nature of various challenges encountered by the CSTC in navigating the complex realm of IT risks. On the other hand, there were different concerns that were raised in relation to the adequacy of various resources that are fully dedicated to IT risk management within the Commission. The Interviewees highlighted the need for more sufficient financial and human resources in order to adequately address quite a number of multifaceted challenges that are majorly posed by various forms of IT risks. In particular, the whole fast-paced evolution of technology is a condition that requires an ongoing

investment in relation to cutting-edge cybersecurity technologies, skill development, together with issues associated with capacity building within the IT risk management team. All these forms of resource constraints were clearly identified as a major factor that hinders the implementation of different types of risk management strategies, thereby leaving the organization vulnerable to quite a number of emerging threats. The interviews conducted were able to bring to the fore front the overall importance of a collaborative kind of an approach to IT risk governance. 70% of the interviewees were able to emphasize on the need for the cross-functional mode of collaboration together with a more integrated approach towards managing various forms of IT risks. The complexity levels of modern IT environments accompanied with the diverse expertise required to address different types of emerging threats, necessitates collaboration among various departments within the CSTC. This mode of collaborative approach greatly ensures that there is a more holistic form of understanding of various risks to an extent of facilitating the overall development and the implementation of more effective risk mitigation strategies. Moreover, different types of qualitative insights that were offered by the interviews perfectly highlighted the overall significance of different types of organizational culture together with the need for a more unified collaborative effort geared towards fortifying the CSTC's resilience against evolving IT risks.

The in-depth data analysis within the Communications, Space, and Technology Commission (CSTC) came up with quite a number of critical insights into the primary proems and obstacles that are known to be inherent in the organization's IT risk management framework. One of the most predominant challenges identified is the significant gap in terms of awareness and understanding among various types of employees, signalling a potential need for various forms of targeted training initiatives. Furthermore, the analysis of the findings clearly revealed that different types of employees as indicated through both survey responses and in-depth interviews, were able

to showcase a specific level of uncertainty in terms of adapting to various forms of emerging technologies, particularly concerning IoT, AI, and 5G networks. This perfectly underscores a critical necessity for various forms of focused training programs that are meant for enhancing the overall knowledge base together with understanding of various forms of IT risk management practices across the entire organization. Being able to address this awareness gap is very essential to equipping the workforce with the right combination of skills for the purposes of navigating the entire intricate landscape of evolving IT risks effectively. On the other hand, the integration of various forms of emerging technologies emerged as one of the most prevalent and shared challenge that existed among various respondents. The ability of the employees to express certain forms of uncertainty regarding the adaptation of various forms of existing procedures to adequately address the novel risks associated with different types of technologies like IoT, AI, and 5G networks. This challenge puts much emphasis on the dynamic nature of the entire technological landscape and the imperative for the CSTC to come up with more agile frameworks that are in a position of incorporating various forms of emerging technologies into different types of existing risk management protocols. Failure to adequately address this whole challenge might end up resulting in the organization being ill-prepared to manage the specific risks that are known to be introduced by these forms of advanced technologies, underscoring the overall importance of strategic and anticipatory adaptation.

Different types of resource constraints emerged as a major substantial obstacle capable of impacting on the robust implementation of IT risk management initiatives within the CSTC. Furthermore, the implemented interviews accentuated a vast range of concerns regarding the adequacy of both financial together with human resources allocated to IT risk management. These types of constraints prevented the deployment of more comprehensive forms of risk mitigation

strategies, thereby leaving the organization to be more susceptible to evolving threats. A strategic investment in cutting-edge cybersecurity technologies, accompanied with the expansion of the IT risk management team together with continuous skill development, is very important when it comes to fortifying the whole organization against dynamic and more sophisticated forms of IT risks. Being able to recognize and even address these forms of resource constraints is integral towards the establishment of a resilient IT risk management framework within the CSTC. The whole evolving regulatory landscape emerged as another major challenge. Different types of changes in legislation together with compliance requirements were identified to be among the major sources of ambiguity, highly necessitating a continuous mode of monitoring together with the adaptation of IT risk management practices in order to ensure ongoing compliance and alignment with legal frameworks. Moreover, the dynamic nature of various forms of regulations clearly poses an ongoing challenge thereby demanding a more proactive and vigilant kind of an approach to navigate and even adhere to the evolving compliance landscape in an effective manner. This whole challenge underscores the entire importance of maintaining a comprehensive level of understanding of various forms of regulatory changes together with the need for an adaptive regulatory compliance strategy within the CSTC's IT risk management framework. The identification of all these predominant issues together with obstacles within the CSTC's IT risk management framework offers one of the most comprehensive basis for targeted recommendations. Bridging the while awareness gap, being able to adapt to quite a number of emerging technologies, addressing various resource constraints, and also navigating the evolving regulatory landscape are central towards enhancing the organization's resilience against an ever-evolving IT risk landscape.

The assessment of the Communications, Space, and Technology Commission's (CSTC) current IT risk management procedures majorly entailed a thorough examination of various forms of qualitative and quantitative data that offered a more comprehensive level of understanding of various strengths together with different areas that are meant for improvement. From a quantitative perspective, the survey results was a clear indication of a moderate level of satisfaction among different types of employees with the existing procedures, perfectly signalling a baseline acknowledgment of the effectiveness of all the implemented strategies. However, the analysis came up with a suggestion that there is still a room for improvement, as the responses were able to highlight various aspects that could be enhanced in order to adequately align with the evolving IT risk landscape. In contrast, various types of qualitative insights that were obtained from in-depth interviews were able to add more valuable layer of context to all the quantitative findings. All these qualitative perspectives perfectly underscored the whole dynamic nature of the IT risk landscape, putting much emphasis that the current procedures may not be in a position of fully synchronizing with the rapid pace that is currently being associated with technological change. Additionally, the qualitative data shed more light on the need for more adaptive and agile forms of risk management frameworks that are in a position of promptly responding to various forms of emerging threats known to be associated with various forms of technological advancements like IoT, AI, and 5G networks. This mode of misalignment with the dynamic technological environment is able to emphasize on the necessity for more strategic adjustments that are geared towards ensuring the ongoing relevance and effectiveness of the CSTC's IT risk management procedures.

Irrespective of all the identified areas of improvement, the findings unveiled a positive perception of the overall level of commitment of the organization in relation to IT risk management. 80% of the employees recognized the emphasis placed on cybersecurity together with data protection, clearly indicating a robust organizational culture that fully prioritizes the mitigation of various forms of IT risks. Moreover, this positive perception is very indicative of a strong level of foundation and commitment within the CSTC towards safeguarding different types of sensitive information and also going an extra mile in ensuring the integrity of its technological infrastructure. However, the whole evaluation brought to light the need for enhancement purposes in relation to the development of more agile and adaptive forms of risk management frameworks. The obtained qualitative insights were able to put much emphasis that the existing procedures while robust, might not be fully equipped to address different challenges that are posed by the rapidly changing technological landscape. This acknowledgment therefore aligns with the broader level of understanding in the field of IT risk management, where adaptability and agility are always recognized as some of the most important factors in effectively mitigating emerging threats. The overall assessment of the CSTC's current IT risk management procedures integrated both the quantitative and qualitative dimensions, coming up with a more comprehensive view of various strengths and areas for improvement that are linked to the organization. While the employees who acted as the research participants expressed some moderate level of satisfaction to an extent of recognizing the organization's level of commitment towards cybersecurity issues, the qualitative insights were able to highlight the imperative of coming up with more advanced and adaptive frameworks. Being able to fully acknowledge all these insights, the CSTC is poised to strategically refine its IT risk management procedures, making sure that they remain to be very robust, responsive and perfectly aligned with the dynamic technological landscape. This kind of an

approach will be in a position of adequately empowering the organization to be able to proactively address quite a number of emerging challenges and even go an extra mile to fortify its resilience against evolving IT risks.

## Recommendations and Tactics for Enhancement

### Comprehensive Training Programs

Establishing various forms of comprehensive training programs is critical when it comes to fortifying the IT risk management culture within the Communications, Space, and Technology Commission (CSTC). All these programs should be able to go beyond various types of conventional training methods providing a variety of modules that are specifically tailored to address the overall level of awareness gap identified across different types of employees. On the other hand, strategic focus on various forms of emerging technologies, such as IoT, AI, and 5G networks, is very important. Such types of modules should be able to offer a lot of in-depth insights into the unique risks that are associated with these types of technologies, empowering employees with the knowledge to recognize and even mitigate a lot of potential threats. As a result of being able to incorporate a variety of practical examples together with a lot of real-world scenarios, the training programs majorly aim towards enhancing employees' levels of understanding of the rapidly evolving IT risk landscape. Furthermore, the comprehensive nature that is linked to all these programs greatly ensures that different types of employees are perfectly equipped to easily adapt to all the emerging challenges, thereby fostering a more proactive mind-set and also going as far as contributing to the overall level of resilience of the CSTC against dynamic IT risks. Having a continuous evaluation and refinement of all these training initiatives will act as an integral part to their levels of effectiveness, making sure that they remain perfectly aligned with the ever-changing technological and risk landscape.

### Adaptive Frameworks

Revamping the current IT risk management frameworks within the Communications, Space, and Technology Commission (CSTC) is very imperative when it comes to addressing various challenges that are brought on board as a result of the rapid evolution of technology. The entire focus should therefore be on creating various forms of adaptive frameworks that are in a position of promptly responding to various forms of emerging threats known to be associated with novel technologies. Additionally, establishing various forms of mechanisms that are meant for continuous monitoring of various forms of emerging technologies is a very critical situation, making sure that the risk profiles are all adjusted dynamically in real-time. This is all about a proactive kind of an approach that is meant for identifying, assessing and even integrating new risk factors associated with technologies like IoT, AI, and 5G networks. As a result of incorporating higher levels of flexibility into different frameworks, the CSTC can greatly foster agility in terms of risk management, thereby creating an opportunity for the organization to always stay ahead of various forms of potential risks. Furthermore, the adaptive frameworks should not only be in a position of accommodating various forms of technological advancements but also be able to facilitate quick adjustments towards different aspects of regulatory changes and compliance requirements. This mode of strategic evolution of different frameworks greatly ensures that the CSTC remains to be resilient in the face of evolving IT risks, offering one of the most robust foundations for proactive risk mitigation together with management. Having quite a number of regular assessments together with updates will be very integral most s when it comes to ensuring a continued relevance continued relevance together with effectiveness of these forms of adaptive frameworks.

### Resource Allocation

Mitigating resource constraints within the Communications, Space, and Technology Commission (CSTC) greatly necessitates a very strategic kind of an approach to the allocation of various resources for a variety of IT risk management initiatives. Being able to address a wide range of financial constraints majorly entails the ability to prioritize different types of investments in the advanced cyber security technologies that are able to align with the entire dynamic nature of quite a number of evolving threats. This majorly entails acquiring various forms of cutting-edge tools and solutions that are all in a position of enhancing the capability of the organization to detect, prevent, and even respond to quite a number of sophisticated cyber risks in an effective way. Additionally, augmenting the whole capacity of the IT risk management team is very important. This majorly entails the ability to recruit and retain different types of skilled personnel known to be having advanced expertise of emerging technologies and cybersecurity trends. Furthermore, strengthening the whole team also ensures the CSTC has got the human capital that is necessary for adequately navigating a vast range of complexities of the evolving IT risk landscape. On the other hand, a well-resourced team fully equipped with quite a number of latest technologies is perfectly positioned to develop and even implement a wide range of risk mitigation strategies. This mode of strategic investment existing in both the technological infrastructure and human expertise not only addresses immediate resource constraints but also moves ahead to establish a foundation that is linked to a long-term resilience against dynamic IT risks, safeguarding the CSTC's critical operations and sensitive data. Moreover, the regular assessments of various resource needs and adjustments to align with quite a number of emerging technologies will end up being integral towards sustaining the overall effectiveness of all these initiatives.

### Regulatory Compliance Monitoring

Crafting an adaptive regulatory compliance strategy is very important for the Communications, Space, and Technology Commission (CSTC) to be in a position of adequately navigating the regulatory landscape that is constantly evolving. This mode of strategic approach majorly entails the establishment of different mechanisms for a continuous monitoring of various forms of regulatory changes making sure that the whole organization remains well-informed about different types of shifts in legal frameworks that are related to IT risk management. On the other hand, as a result of proactively staying abreast of different types of modifications in terms of the legislation and compliance requirements, the CSTC can swiftly adapt its practices in order to maintain continuous alignment with legal standards. This mode of adaptability goes beyond mere compliance, incorporating an advanced mode of forward thinking kind of an approach for the purposes of anticipating the future regulatory trends. The strategy should be able to adequately encompass quite a number of regular assessments of the existing compliance protocols, clearly identifying specific areas that might require certain forms of adjustments in order to align with all the emerging regulatory expectations. Furthermore, the establishment of clear communication channels with the regulatory authorities and also participating in industry collaborations is capable of further enhancing the overall capacity of the organization to proactively shape its compliance strategies. This mode of adaptive regulatory compliance kind of an approach not only mitigates the overall risk of non-compliance but also goes an extra mile to position the CSTC as a proactive contributor to the evolving industry standards, thereby fostering a unique culture that is full of legal reliance and regulatory responsiveness. Various regular reviews and updates to the entire strategy will highly ensure its overall effectiveness in the face of regulatory changes.

### Collaborative Governance

Cultivating a collaborative approach to IT risk governance within the Communications, Space, and Technology Commission (CSTC) majorly entails the establishment of various forms of cross functional teams that are able to bring together quite a number of representatives originating from different departments. Furthermore, this inclusive kind of an approach will ensure that there is a more holistic level of understanding of different types of risks, as every department contributes unique insights and expertise. As a result of putting much concentration on the open communication channels, the CSTC can create an environment where different types of risks are assessed in a comprehensive manner from a vast range of perspectives. On the other hand, Cross-functional teams highly facilitate a clear level of understanding of different interdependencies that exists between various departments alongside their collective impact on the organization's overall risk landscape. Moreover, this mode of collective governance model offers an opportunity for the identification of quite a number of potential blind spots together with gaps that are existing within the risk management boundaries, further contributing towards a more effective and well-rounded risk mitigation strategies. Again, involving various representatives from different types of departments also ensures that the entire risk management becomes an organization-wide effort, that fosters a shared responsibility for maintaining a secure and resilient IT environment. Having different forms of regular collaboration and knowledge sharing sessions among various types of cross functional teams further helps in the strengthening of the organization's overall risk governance capabilities. This kind of a collaborative approach not only enhances the ability of the organization to proactively address various forms of IT risks but also promotes a culture that is full of collective responsibility and continuous improvement. The implementation of regular evaluations alongside the adjustments to the collaborative governance structure will be very integral to its sustained effectiveness.

### Incident Response Plans

Within the contemporary landscape of cybersecurity, scaling up incidence response plans is very imperative to adequately encounter the dynamic and ever-evolving nature of cyber threats. Moreover, Incident response plans perfectly serve as a blueprint for the reaction of an organization to various forms of security incidents making sure that there is a systematic and more coordinated kind of an approach in the face of cyberattacks, data breaches, or even other security breaches. As the occurrence of cyber threats still continue to scale up in sophistication together with adversity in their respective forms, different types of incident response plans must be able to evolve in order to match the entire agility of malicious actors. Furthermore, regular drills together with simulations are among the most integral components of a proactive kind of an approach to issues associated with incident response. All these exercises perfectly serve as one of the most invaluable tools that are meant for testing the overall level of effectiveness of different aspects of response mechanisms, evaluating the readiness of different types of cyber security teams and also identifying specific areas that are meant for improvement. On the other hand, simulating various forms of real-world scenarios creates an opportunity for different organizations to gauge their capability of detecting, responding to and also recovering from different types of cyber incidents. By going an extra mile to replicate the conditions of a specific cyber threat, different types of organizations, can find it much easier to validate the efficacy of their respective incident response plans, assess the level of coordination among response teams, and also be able to identify potential gaps in processes or procedures. On the other hand, the dynamic nature that is linked to cyber threats greatly necessitates a continuous review cycle, refinement together with the optimization of incident response plans. Different types of cyber security teams must also stay abreast of the latest threat intelligence, different attack vectors, and also various vulnerabilities in order to ensure that their incident response strategies remain relevant and more effective when it comes to attaining different

types of goals and objectives. Threat intelligence feeds together with analysis should be able to perfectly inform the incident response plans, offering one of the best opportunities for different organizations to tailor their respective approaches in relation to the current threat landscape.

## Conclusion

In conclusion, this research has offered one of the most comprehensive examination of IT risk management existing within the Communications, Space, and Technology Commission (CSTC) in Riyadh, clearly revealing quite a number of major findings together with different types of insights that tend to hold significance for the organization and similar entities. Furthermore, the major themes that emerged from the study majorly encompassed an awareness gap across different types of employees, various challenges that are associated with the integration of quite a number of emerging technologies, resource constraints, together with the evolving regulatory landscape. Furthermore, the awareness gap identified within the CSTC puts much emphasis on the essential need for the implementation of more targeted training initiatives. While the implemented survey indicated that there is a moderate level of satisfaction among different types of employees, different types of qualitative insights clearly revealed a more critical level of understanding of various types of major challenges that are brought on board by various forms of emerging technologies like IoT, AI, and 5G networks. Being in a position of addressing this level of awareness gap is always very critical for cultivating a workforce that is well-informed capable of navigating different types of intricacies of the whole evolving IT risk landscape. Additionally, the integration of various forms of emerging technologies emerged as one of the most common challenges, emphasizing on the need for the CSTC to develop more adaptive risk management frameworks that will create an opportunity for effectively responding to various forms of novel risks that are associated with a variety of technological advancements. There was the identification

of different types of resource constraints as a major obstacle that hinders the robust execution of various forms of IT risk management initiatives. The study also placed much emphasis on the overall importance of implementing strategic investments in financial and human resources with an intention of fortifying the entire organization against different types of evolving threats. This entails not only the allocation of various forms of additional resources but also the implementation of various forms of cutting-edge cybersecurity technologies together with continuous skill development that are meant for enhancing the effectiveness of risk mitigation strategies. On the other hand, the evolving regulatory landscape was perfectly recognised as a major challenge that demands a continuous level of monitoring and adaptation of various forms of IT risk management practices. This finding perfectly underscores the entire dynamic nature of different types of regulations alongside the need for a more proactive kind of an approach capable of ensuring an ongoing compliance together with the alignment with various forms of legal frameworks. On the other hand, different positive aspects were also noted most so the organization's level of commitment to IT risk management. The employees were able to acknowledge the emphasis on cybersecurity and data protection, indicative of a strong form of organizational culture that is fully focused on mitigating IT risks.

Revisiting all the research objectives and hypothesis, the study majorly aimed to determine some of the major problems and obstacles in the CSTC's IT risk management, assess the efficacy of existing procedures and even go as far as suggesting different types of tactics that are meant for improvement. Furthermore, the research successfully attained all these objectives through the identification of different types of major challenges, evaluating the current state of IT risk management, and also offering strategic recommendations for enhancement. The hypothesis, positing that the rapidly changing technological world clearly presents one of the most substantial

IT risk management issues for the CSTC, was perfectly substantiated through the identification of various gaps in existing procedures. Furthermore, the implications that are linked to this study for the CSTC and similar organizations are far-reaching. The findings perfectly serve as a clear roadmap for the CSTC to strengthen its IT risk management practices. By being able to address the awareness gap, adapting to various forms of emerging technologies and also being able to overcome a variety of resource constraints, the CSTC can bolster its resilience against dynamic IT risks. The whole study therefore underscores the overall importance of cultivating a more proactive and adaptive form of organizational culture, instilling a level of commitment to continuous improvement within the boundaries of IT risk management. Moreover, for similar organization, this study provides quite a number of valuable insights into various common challenges and best practices. All the identified issues are not unique to the CSTC but also resonate across different types of governmental commissions together with organizations navigating the evolving technological landscape. Furthermore, the strategic recommendations that are provided can perfectly serve as a benchmark for enhancing various forms of IT risk management practices, promoting a more proactive stance against emerging threats. Focusing ahead, future research across the whole field of IT risk management in government commissions should be able to carry out an exploration of quite a number of emerging technologies together with their specific implications for the purposes of risk management. Moreover, investigating the overall effectiveness of quite a number of training programs together with various educational initiatives in the scaling up of IT risk awareness across different types of employees would end up providing quite a number of valuable insights. On the other hand, comparative studies across different types of governmental commissions could provide wider level of understanding of different types of common challenges and effective strategies. This research therefore contributes towards quite a

number of valuable insights to the whole field of IT risk management, providing the CSTC and similar organizations with one of the strongest foundations that are meant for strategic improvements. As a result of addressing all the identified challenges, different types of organizations can perfectly navigate the whole dynamic landscape with higher levels of resilience and foresight, thereby making sure that there is a continued protection of different types of sensitive data alongside the uninterrupted operation of critical services.

## References

- Alijoyo, F. A., & Fisabilillah, A. F. M. (2021). Risk Management Implementation in Public Sector Organizations-Global Phenomena. *Int. J. Curr. Sci. Res. Rev*, 4(03), 195-202.
- Dragan, I. F., Dalessandri, D., Johnson, L. A., Tucker, A., & Walmsley, A. D. (2018). Impact of scientific and technological advances. *European Journal of Dental Education*, 22, 17-20.
- Fan, Y., & Stevenson, M. (2018). A review of supply chain risk management: definition, theory, and research agenda. *International journal of physical distribution & logistics management*, 48(3), 205-230.
- Mahama, H., Elbashir, M., Sutton, S., & Arnold, V. (2022). Enabling enterprise risk management maturity in public sector organizations. *Public Money & Management*, 42(6), 403-407.
- Piekiet Weeserik, B., & Spruit, M. (2018). Improving operational risk management using business performance management technologies. *Sustainability*, 10(3), 640.
- Raja, M., & Priya, G. G. (2021). Conceptual Origins, Technological Advancements, and Impacts of Using Virtual Reality Technology in Education. *Webology*, 18(2).
- Scholl, M., & Suloway, T. (2021). Introduction to cybersecurity for commercial satellite operations. *National Institute of Standards and Technology, Tech. Rep.*
- Willumsen, P., Oehmen, J., Stingl, V., & Geraldi, J. (2019). Value creation through project risk management. *International Journal of Project Management*, 37(5), 731-749.