Risk Management In Private Sector

*Rahul Reddy Nadikattu**
Department of Information Technology, University of Cumberlands,
6178 College Station Drive, Williamsburg, KY 40769, United States

ABSTRACT

The present study focuses on the critical areas of a typical Information Technology in the Private Sector within the USA that has narrowed down economic and national security assurance within the USA. The process of risk management in the IT Sector within the USA in regards to the structuring and management of risk associated with its strategic planning. Thus the article insights on the role of risk management to meet the success rate. The risk environment of the Private Sector's IT in the USA is inherently dynamic and complex. Hence articles highlight each component of risk management and its role to overcome the associated risk.

Keywords: Risk management, IT Department, Risk Factors, Risk Processes

I. INTRODUCTION

The recent technology displays the structuring of the organization to carry out the business in the competitive world. [1]. In order to meet the desired targets, there are innumerable challenges which should be overcome. Hence planning and implementation of strategies plays important role in company such as IT, Biotech, Sports, to name a few [2]. Especially in the country like America, which is considered to be the hub of innovation, companies must be well planned and structure to survive in the long run. One such important strategy include, risk management which forms the key role towards planning and executing the market. When planning the risk assessment, monitoring of current organizational plan and forecasting the risk associated with its channel must be studied [3]. Risk management influences on profit-lose ratio of the company by providing the probability of forecasting the associated risk, its prevent measures by differentiating the internal risk and external risk [4]. Once the potential risk is defined and addressed, there will be fundamental gains which aids the company to flourish and grow in the competitive market [5,6]. The present study aims to focus the risk management strategy using advance tools which can easily identify and categorize the associated risk throughout the planned organization life. The main subject of interest in the present study relies into the economic gains coupled with national security and quality assurance within the companies established in United States. Based on these facts, the present paper, is designed and executed to identify the four important assets in IT industries such as website, portraying the companies profile which can improve the inflow of customers and projects. Further, data center, Server and SQL database which enables the growth pattern of the company by documenting the outcome of the productivity and its beneficial aspects. These four assets, are the pillar of any organization especially in United states which insights the overall efficiency and productivity of the company.

II. PRIVATE SECTOR'S IT RISK ENVIRONMENT IN THE USA

The risk environment of the Private Sector's IT in the USA is inherently dynamic and complex. Few primary characteristics shape the evolving climate of risk in the Private Sector in the USA: interdependencies amid the Private Sector's IT and other critical infrastructure sectors; IT infrastructure's international, interconnected, virtual, and highly diverse nature; and the landscape of continually altering threat. The Private Sector within the USA has worldwide operations that are interconnected and interdependent with other infrastructures. These operations increase effectiveness and efficiency, along with increasing the Sector's resilience. They, however, face several multifaceted international threats daily from human-made and natural events. The majority of these threats frequently occur but do not have noteworthy outcomes due to response capabilities and existing Security of individual entities. Some of these threats, however, are tactical and could impact functions of the critical IT Sector. The IT Sector's high interdependency degree, it's unidentifiable and non-traceable, and interconnectedness actors make assessing vulnerabilities, identifying threats, and evaluating outcomes difficult and needs to be managed within a creative and collaborative manner [7].

III. SEVERAL RISK MANAGEMENT APPROACHES OF ENTITIES

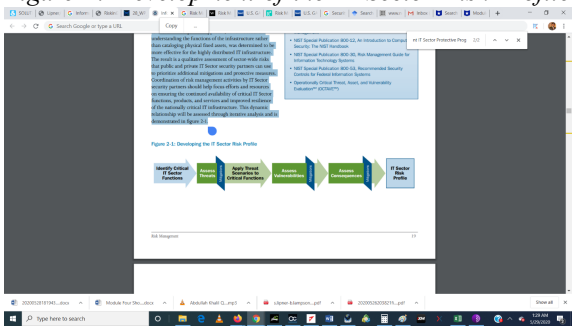
Throughout the Private IT Sector in the USA, the used approaches of risk management are grounded on several tools, methodologies, and philosophies. Entities in the Private Sector usually ground their tactics on business objectives, for example, customer service, efficacy, and shareholder value. Across entities, requirements of regulatory compliance related to the privacy initiatives, and integrity of financial reporting are increasing awareness within the risk management approaches. As part of their plans to risk management, numerous private sector IT entities have elected pivotal points for control of Security and risk. Within their organizations, few have centralized this function; on the other hand, others across their operations have selected to have it distributed. Furthermore, Entities in the Private Sector measure numerous risk types (e.g., compliance, legal, supply chain, human, and

financial) with the help of multiple approaches (e.g., simulation and modeling, qualitative, and quantitative) leveraging both government and commercial customized tools off-the-shelf and products. These entities use a range of frameworks of standard risk management for proactively managing steady-state risk [8,9].

IV. DEVELOPING AN IT SECTOR RISK PROFILE

For developing the overall profile of IT Sector risk, there is a need for identifying functions collaboratively of critical Sector, analyzing functions' threats, assessing vulnerabilities, evaluating consequences, along with identifying mitigations for the Private Sector. The focus would be on a top-down that ponders sector objectives and goals to determine whether or not the current risk level is satisfactory or whether there is a need for further mitigation in the innovative programs form or other mechanisms considered for reducing risk to an adequate level. This top-down approach focused on comprehending the infrastructure's functions instead of cataloging physical assets and was determined for being more useful for the extremely distributed infrastructure of IT. The outcome is a sector-wide risks' qualitative assessment that Private Sector's IT can use for prioritizing further innovative measures and mitigations [10,11]. Risk management coordination activities by IT Sector needs to assist in focusing on resources and efforts in making sure the sustained accessibility of critical IT Sector services, products, and functions and nationally crucial IT infrastructure's improved resilience. With the help of iterative analysis, this dynamic relation will be evaluated and is shown in figure 1.

Figure 1: Development of the IT Sector Risk Profile



V. IDENTIFYING CRITICAL FUNCTIONS

The infrastructure of IT is distributed functions' aggregate, supported by numerous networks, systems, and assets. The foundation's distributed nature integrally provides virtual and physical resilience; though, certain features might have physical, limited supporting cyber and the infrastructure's human elements that could show risk and possibly raise their susceptibility. The Sector where there is the identification of risk will use the process of evaluation for raising awareness amid the organization that depends on the crucial functions, along with proposing particular defensive abilities for mitigating risks, where suitable [11,12]. Features include the processes that assist in producing, providing, and maintaining services and products. The IT sector features include the full processes (e.g., maintenance, upgrades, distribution, manufacturing, and research and development) engaged in the transformation of supply inputs into IT services and products. These functions assist in supporting the Sector's ability to produce and provide high-assurance practices, services, and products that are resistant to threats and can be recovered rapidly. Assurance is needed for attaining the vision of the Sector and is consequently an essential aspect of every critical function. The vital functions' sub-functions address this aspect directly and work to create high-assurance services and products consistently. The political or geographic boundaries do not limit the IT sector's features, and it increases the need for worldwide coordination and collaboration for risk activities of assessment, along with the design and implementation of the innovative risk management program and best practices [13,14]. It recognizes critical functions in the IT Sector, along with their descriptions, rounded on the criteria of consequence. These are the functions essential for maintaining or reconstituting the network (e.g., extensive area networks, local networks, and the Internet) and related services. The list shows consensus on critical functions in IT Sector that are essential for economic and National Security in the USA.

VI. DEVELOPMENT AND IMPLEMENTATION INNOVATIVE RISK MANAGEMENT PROGRAMS

Innovative risk management programs comprise activities or measures that various organizations within the Private Sector in the USA undertakes for getting prepared for prevention, protecting against, responding to, and recovering from events that can influence critical functions of the IT Sector. Programs are led and sponsored by Private Sector, or they signify a partnership between the private and public sectors.

VII. CURRENT INNOVATIVE RISK MANAGEMENT PROGRAMS FOR IT SECTOR

Table 2 describes the capabilities of the innovative risk management program that supports the IT sector's goals. Numerous innovative risk management programs include creative activities and measures that apply to the IT sector and other critical sectors of infrastructure.

Current Innovative Risk Management Programs for IT Sector

Table 2 describes the capabilities of the innovative risk management program that support the goals of the IT Sector. Numerous innovative risk management programs include innovative activities and measures that are applicable to the IT Sector, along with a number of other critical sectors of infrastructure.

Table 2: Capabilities of Innovative Program that Support Goals of IT Sector

Goal	Outcome and Capability	Innovative Programs' Services
Protection and prevention through the management of risk	Reduction in Vulnerability	It is a means for identifying and obtaining appropriate data on vulnerabilities of the Sector; access to mitigation, and remediation best practices and actions.
	Analysis of Threat	It comprises the comprehension of the threats faced today by the IT Sector and the USA as a whole.
	Simulation and Modeling	It comprises the capabilities for analyzing and understanding the interdependencies of critical infrastructure.
	High-Assurance Services and Products	It comprises the Services and Products with incorporated Security.
	Best practice of Security	It comprises the mechanism to identify and share innovative measures and best practices for IT security.
Situational Awareness	Tactical Analysis, Indications, and Warning	Information regarding incidents, along with other events as they unfold and detected to raise the current operating environment's understanding and awareness.
	Communications and Sharing of Information	A means to access and share information that allows decision-makers for comprehending the existing operating surroundings, form an outlook regarding the Security's existing state, and take actions for responding to the events.
Response, Recovery, and Reconstitution	Communications of National Emergency	It comprises the mechanisms to ensure that the Private Sector can communicate with each other throughout incidents.

	Coordination of Incident Response and Incident Management	It comprises the Capabilities for coordinating efforts for detecting, containing, eradicating, and recovering from incidents. Additionally, evaluation of lessons learned during the phase of the management life cycle of each incident develops prevention capabilities and preparedness.
	Attribution and Investigation	Methods to attribute incidents to an individual or individuals with the eventual objective of prosecuting and apprehending the suspected accountable parties.
	National-Level Planning/ Contingency Planning	It comprises the actions that assist in facilitating the plans' exercise, procedures, and processes for ensuring the Sector, organizations, individuals, and the Nation can recover from and respond to the incidents. Formal allocation and planning resource assists in identifying uses of and needs for accessible mechanisms for materials' coordination and expertise for facilitating recovery.

VIII. IDENTIFY AND IMPLEMENT AN INNOVATIVE RISK MANAGEMENT PROGRAM

The following section focuses on a process for determining the necessary types of innovative actions for the IT sector to address priorities recognized through the approach of risk management of the Sector. This is the process that will be utilized where the individual entities do not provide mitigation, no feasible solution for the private Sector exists to meet the needs, or legal barriers, high costs of the transaction, or other impairments would become the reason for implementation challenges or significant coordination

IX. ESTABLISHING AN INNOVATIVE RISK MANAGEMENT PROGRAM

An Innovative risk management program needs to be developed for the IT Sector for accomplishing the following:

- *Determining whether current programs satisfactorily promote the critical IT Sector*

functions' Security;

- *Identifying any anticipated capabilities required for addressing risk;*
- *Framing needs of future innovative risk management program; and*
- *Making recommendations to the IT Sector Coordinating Council and Government Coordinating Council for the specific innovative risk management program.*

An active, innovative risk management program needs to comprise representatives of the private Sector from entities, for example, the IT GCC, IT SCC NCSD, and other security partners.

Determine Capabilities and Needs

The innovative risk management program will recognize areas where every innovative measure is most desirable for achieving the Sector-sector's goals. During the initial process of development of the program, the members of IT GCC and IT SCC identified the subsequent instances of capabilities that might be considered further to enhance the IT Sector s

Sector security:

- *Capabilities of Robust Coordinated Response. The ability to recover from and respond to a noteworthy nationwide event is crucial in promoting the IT Sector's resilience and other sectors. An all-hazards capability for operational recovery and response is required for bringing the Private Sector together for coordinating activities. Analytical tools, collaboration, and emergency communications could develop effective response; this might comprise boosting existing capabilities and resources of the Private Sector.*
- *Data Reconstitution. ools and techniques for data reconstitution are required for ensuring data availability and integrity. The development of an innovative risk management program needs to be closely associated with R & D activities designed for developing and piloting capabilities that allow private-sector systems to rapidly reconstituting information that could be corrupted, either unintentionally or intentionally.*
- *Reconstitution of Networks and Communications Services. An innovative risk management program initiative might be developed for assisting with Federal Government authorities' implementation under the Communications Act's Section 706 applicable to the Internet's critical functions. This program also needs to comprise the development of the mechanisms, applications and plans to identify and refine requirements and develop capabilities of reconstitution.*
- *The capability of Out-of-Band Data Delivery. An innovative risk management program is required for providing mechanisms for the delivery of patches along with other software to key users if essential network/Internet functions are unavailable.*

X. IMPLEMENTATION PLAN

An initial plan for implementation is developed for the above-identified needs. The project will comprise the recommendations related to the parties accountable for the implementation of the risk management program, resources (for example, procedures, processes, budget, and facilities), schedule, collaboration with different applications, potential problems to success, along with other considerations for program's effective maintenance and initiation [15].

XI. CONCLUSION

Technology is impacting how several organizations conduct business in a growing market. The risk environment of the Private Sector's IT in the USA is inherently dynamic and complex. Throughout the Private IT Sector in the USA, the used approaches of risk management are grounded on several tools, methodologies, and philosophies. For developing the overall profile of IT Sector risk, there is a need for identifying functions collaboratively of critical Sector, analyzing functions' threats, assessing vulnerabilities, evaluating consequences, along with identifying mitigations for the Private Sector. The infrastructure of IT is distributed functions' aggregate, supported by numerous networks, systems, and assets. Innovative risk management programs comprise activities or measures that various organizations within the Private Sector in the USA undertakes for getting prepared for prevention, protecting against, responding to, and recovering from events that can influence critical functions of the IT Sector. The innovative risk management program will recognize areas where every innovative measure is most desirable for achieving the Sectorsector's goals.

XII. ACKNOWLEDGEMENTS

Author is thankful for the University of Cumberlands for providing the infrastructure to carry out the present study.

XIII. REFERENCES

1. *A. Rostami, J. Sommerville, I.L. Wong, and C. Lee, "Risk management implementation in small and medium enterprises in the UK construction industry", Engineering, Construction and Architectural Management, 2015, 22, 91-107. https://*

doi.org/10.1108/ECAM-04-2014-0057

2. *K.S. Namahoot, and T. Laohavichien, "Assessing the intentions to use internet banking: The role of perceived risk and trust as mediating factors", International Journal of Bank Marketing, 2018, 36, 2, 256-276*

3. *T. Aven, "Risk assessment and risk management: review of recent advances on their foundation", 2016, European Journal of Operational Research, 253, 1–13.*

4. *T.J. Andersen, "Global Derivatives: A Strategic Risk Management Perspective", Pearson Education, London, 2005*

5. *J. Fraser and B. Simkins (Eds.). (2010). "Enterprise risk management: Today's leading research and best practices for tomorrow's executives" 2010, 3, John Wiley & Sons. 178*

6. *Z. A. Collier, D. DiMase, S. Walters, M.M. Tehranipoor, J.H. Lambert, I. Linkov, "Cybersecurity standards: Managing risk and creating resilience". Computer, 2014, 47(9), 70-76.*

7. *G. Stoneburner, A. Goguen, A. Feringa, "Risk management guide for information technology systems". National Institute of Standards and Technology Special Publication, 2001, 800(30)*

8. *B. Tiganoaia, A. Niculescu, O. Negoita, M. Popescu, M, "A New Sustainable Model for Risk Management—RiMM". Sustainability, 2019, 11, 1178.*

9. *Y. Haimes Yacov, and G. Clyde Chittester. "A Roadmap for Quantifying the Efficacy of Risk Management of Information Security and Interdependent SCADA Systems." Journal of Homeland Security and Emergency Management 2.2 (2005).*

10. *S. Maserang, "Project Management: Tools & Techniques". MSIS 488: Systems Analysis & Design 2013, (15)*