An Approach to Address Risk Management Challenges: Focused on IT Governance Framework

Razan M. Boodai
Dhahran, Saudi Arabia
Razan.Boodai@aramco.com

Hadeel A. Alessa
Dhahran, Saudi Arabia
Hadeel.Alessa@aramco.com

Arwa H. Alanazi
Dhahran, Saudi Arabia
Alanazi.h.arwa@gmail.com

2022 IEEE International Conference on Cyber Security and Resilience (CSR) | 978-1-6654-9952-1/22/$31.00 ©2022 IEEE | DOI: 10.1109/CSR54599.2022.9850318

***Abstract*— Information Technology (IT) governance crosses the organization practices, culture, and policy that support IT management in controlling five key functions, which are strategic alignment, performance management, resource management, value delivery, and risk management. The line of sight is extended from the corporate strategy to the risk management, and risk controls are assessed against operational goals. Thus, the risk management model is concerned with ensuring that the corporate risks are sufficiently controlled and managed. Many organizations rely on IT services to facilitate and sustain their operations, which mandate the existence of a risk management model in their IT governance. This paper examines prior research based on IT governance by using a risk management framework. It also proposes a new method for calculating and classifying IT-related risks. Additionally, we assessed our technique with one of the critical IT services that proves the reliability and accuracy of the implemented model.**

Keywords — Risk Management, IT Governance, IT Framework, Automation, Risk Management Model, Information Systems, Risk Assessment, Strategic Alignment.

I. INTRODUCTION

Information Technology (IT) governance provides the necessary policies and practices to the organization to manage and control its functions. There are several standards and methodologies to enable the standardization of IT. According to [1], executives directors, and management, are accountable for IT governance of the organizational structures and processes to ensure that IT services are sustainable and aligned with the organization's strategies and goals.

IT governance focuses on maximizing business value by developing and maintaining an effective IT control with five key functions, which are: (1) strategic alignment that aligns the enterprise and IT operations; (2) value delivery that ensures IT value is provided via delivery cycle; (3) resource management that assures proper management of IT assets; (4) performance management tracks and monitors IT projects implementation; and lastly; and (5) Risk Management to ensure the organization risks are addressed.

An effective Risk Management Model (RMM) has a positive impact on the performance, business deliverables, exploits new opportunities, reduces potential losses, and mitigates risks [6][7]. Assessing and directing IT usage to support the organization, monitoring the plans execution, implementing a strategy and policies to achieve its goals, and aligning the goals with IT strategy are all considered part of IT governance objectives. The ultimate goals of IT governance are mitigating IT risk and ensuring that IT investments are generating business value.

This paper intends to provide a conceptual understanding of one of the key domains for IT governance, which is risk management. It is an effect of uncertainty on events that can result in positive or negative impacts on the organization [22]. The paper illustrates our research on risk management models, including identifying, classifying, and tracking IT risks with an automated monitoring system. This paper is organized as follows: Section II details the literature reviews from previous research on IT governance and risk management. Section III illustrates the current challenges that this research would address. The risk management methodology is presented in section IV. Section V demonstrates the result of RMM automation approach and enhanced solution. Finally, the model limitations and conclusion are presented in section VI.

II. LITERATURE REVIEW OF RELATED STUDY

The aim of IT governance frameworks is to provide processes and structure for effective IT decision-making [8]. In today's world, IT has become vital to the growth and sustainability of all organizations. A governance framework for IT is a way for an organization to manage and control its IT resources, including its people and infrastructure. The framework of IT governance is composed of structures, processes, and mechanisms that relate to each other and each has a function. They should all contribute to the success of the organization when implemented. Selecting the right mechanism for a particular context can be a complex process [20].

Mature IT governance results have a positive impact on IT-business alignment and performance with effective internal control and efficient IT systems [8]. 80% of Chief Information Officers (CIOs) recognized that organizations need effective IT governance to achieve the corporate performance objectives [10]. According to [6], the firms with proper implementation of IT governance framework increase their profit by more than 25%. Based on Gartner's research [2], expenditure on global IT governance projects is more than three trillion US dollars. According to [13], corporate performance is negatively impacted with the raised number of cybersecurity breaches by exploiting the weaknesses of networked industrial systems. So,

978-1-6654-9952-1/22/$31.00 ©2022 IEEE

risk assessment is a reactive procedure in conventional software development practice, carried out either during the deployment phase or during the evaluation of software for business. Forecasting cyberattacks based on time-series through data from honeypots, network telescopes, and automated intrusion detection and avoidance systems is a typical strategy to combat cyber threats [11].

Therefore, organizations need to understand all potential risks holistically with unconventional risk management models and business strategies to maximize business performance and establish sustainable development at the lowest possible cost [7][5]. The risk assessment process involves humans, which is time consuming, prone to mistakes, and costly. In addition, the result of the adoption and IT governance frameworks is not only mechanical, as it produces an opportunistic impact on the managerial behavior [9]. Based on [16], risk assessment and management are scientific domains that were recognized 30–40 years back. Methodologies and means have been established for how to assess, conceive, and manage risk. Although there have been many advancements in both theoretical platforms and experimental models and processes, these concepts and approaches still constitute a large scope of the field's basis today. Even though risks have a large impact on strategic choices, there has been a debate on how to recognize them [18].

There are many security techniques used to assess the risks. The traditional security technique that guides the developers on what to do through manual checklists, and conventional methods, this technique is considered challenging to implement [12]. Clarke and Liesch [3] stated that risk management model shall be implemented with a "wait-and-see" strategy, which is implemented gradually with the measured decision results from existing commitments of an international business relationship. For example, a UK retailer existed in the US market without proper risk assessment, which impacted its after-tax profits, around one billion British pounds. Consequently, the risk management model assures the firm's sustainability by strengthening investors' confidence and enhancing economic efficiency and growth [7].

The studies in [12] show that current industry approaches are unable to offer the application security that organizations need. Environments and application programming interfaces can be improved to address this problem. Investigating technologies to automate security improvements and assisting programmers in improving security within existing limits will considerably aid in the resolution of the problem. Security specialists also employ "threat modelling" approaches, which identify the causes and potential outcomes for a variety of risks to the considered systems. Cyberattacks on sensitive industrial equipment have the potential to jeopardize a company's business model in some situations. Identifying and analyzing the primary vital assets to be secured from prospective cyberattacks, as well as the business effects that may occur, is a competitive advantage [13]. The traditional security technique of telling developers what to do with checklists, methods, and failures to avoid, has demonstrated implementation challenges [12].

With the growing concerns about cybersecurity, the need to calculate security risk is vital. The process of evaluating these calculations is complex and largely private to the group conducting the study. To appropriately evaluate the security structure, some aspects must be conceded [10]. For the design of systems security evaluation, Chandy and Wortman [10] introduced the model of security risk-based adversarial tool. The tool's feature is that it automates the assessment of security attack trees and offers useful comparable metrics. This program converts an attack graph into a model of system security and gathers the essential data to determine the optimal solution built on an estimated security risk conveyed as an economic value. Other literature analyses and studies [11] employed a Bayesian State-Space Model for forecasting cyber threats one week ahead could be anticipated with fair accuracy and increased threat awareness, hence improving cybersecurity by assisting in the optimization of human and technical cyber defensive capabilities.

III. CHALLENGES

Risk management plays a critical role in IT governance to identify and assess the risk. Management can face some challenges and make incorrect decisions if they do not have enough information, or do not follow a specific framework or metrics when they assess the risk. RMM Subjective assessments is a key challenge that need to be resolved which is based on the provided information where it could be complete, incomplete, or hesitant information [19]. Brain-storming sessions, different mindsets, and diverse technical backgrounds are considered key areas for subjective assessments in the RMM. Following these areas will result in determining decisions that lack quality, performance, and consistency. Therefore, to have a useful assessment, management must be clear about the requirements and have enough information [21]. Moreover, subjectivity can be influenced by the organization, environment, situation, or even the implemented solutions. As a result, determining impact and making relevant decisions might be challenging.

Another challenge is the RMM misalignment with corporate strategy, which is usually difficult to spot and identified. Yet without proper alignment, the RMM will be out of sync with the strategic goals and organization mission. Thus, it is crucial to identify strategic misalignment and associate it with the business and IT engagement to increase the firm value [9]. Misalignment and ineffective IT governance lead to poor performance of IT, inaccurate data quality, inefficient business and operation costs [17].

Additionally, the manual approach to handling the RMM raises another challenge due to its difficulty to manage, time-consuming, and inefficient process. The current approaches assess the effects without considering the undesirable consequences of relying on manual risk evaluations [15]. According to [14], The manual processes of detecting threats can be error-prone, with the chance of inaccurate risk analysis, and it consumes a lot of time and effort. Challenges arise due to the fact that not all the users have the required knowledge to comprehend the underlying threats [14]. Therefore, automation can greatly help in overcoming these challenges for assessing business risks and providing possible solutions.

This problem will be addressed in greater depth in this study by using an Enterprise Risk Management Solution to automate the RMM. Consequently, results will be shown at the end.

IV. Research Methodology

To overcome the above challenges, we performed this research with an intensive literature review covering two concepts: IT governance and risk management. Designing the risk management model should be subjected to guiding principles, as follows [17]:

- Business drivers guarantee the alignment with the corporate objectives to assure the model meets the overall enterprise vision.
- Governance policies assure it is designed based on the approved corporate policies by the board of directors.
- Risk baseline ensures the risk appetite, strategies, and key risk indicators are defined with an acceptable level based on the quantitative or qualitative measures of the business impact.
- IT Risk Committee; the existence of a committee that is responsible and accountable for managing IT risks and performing regulatory compliance.

To properly protect IT organizations against possible misuses, we have designed the IT risk management model to outline the acceptable risk level that gives the assurance level to certain IT processes and services based on the corporate policies and standards.

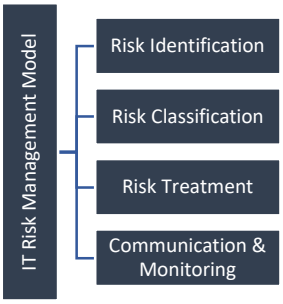

Fig. 1. IT Risk Management Model

A. Risk Identification

There are several ways to identify IT risks that include: (1) Continuous risk identification through checklist and schedule that cover duration and cost estimates, with the involvement of the support's members; (2) external identification of risks through the third party; and (3) historical database from previous incidents and events by identifying any potential future risk. This approach focuses on an existing artifact and reduces subjective assessment. Thus, we have eliminated one of the known methods for identifying risks, which is brainstorming sessions. The management review is an essential step that has a significant impact on the identification of events to assure the model is aligned with the business drivers and enterprise vision.

B. Risk Classification

Risk classification is highly dependent on the business impact, triggers, and event categorization. Understanding the impact and building up a methodology to classify the risk is not easy, as it requires a clear view of the organization's operations, in addition to the likelihood and probabilities of occurrence.

There are a number of standards in the IT governance industry such as COBIT, NIST, or ISO 31000 [25], which define frameworks to classify IT risks. It requires an internal understanding of IT risks within the organization. The classical approaches to calculate risks classification combines only two dimensions which are likelihood and Impact based on risk matrix. The elementary risk (Eri) is defined with three metrics [15], as shown in Eq. (1).

$$\text{Eri} = [\text{Likelihood}, \text{Impact}, \text{f}(\text{Likelihood}, \text{Impact})] \quad (1)$$

We took Eq. (1) into preceptive to customize a risk classification method that fit IT organizations. To calculate the likelihood and two dimensions of impact (i.e., existing and future), we came up with Eq. (2) by applying a new approach. The existing impact is known as it occurs on the current moment. Predicting the future impact introduces uncertainty. Thereby, the composition used in RL is a two-impact value, where if the future impact is unknown, then the RL is calculated based on the existing impact value. This approach helped us to overcome the challenge related to subjectivity assessment.

$$\text{RL} = \sum \text{k} \left(\frac{\text{L}_\text{k} + \text{FI}_\text{k} + \text{EI}_\text{k}}{5} \right) \quad (2)$$

Where RL is the coefficient of the risk level of the likelihood, financial impact, technical performance, stakeholder, and repatriation of the enterprise;

L_k is the likelihood with five ranges of probabilities of occurrence, as shown in Table 1 [15].

FI_k is the result of the future impact of the adverse event, as shown in Table 2; and

EI_k is the result of the current impact of an existing event. It also includes the unassigned impact, as shown in Table 2.

TABLE I. Future and Existing Impact of Risk

	Financial*	Technological Performance	Customers	Reputation	Operational
0	No Impact; unassigned				
1	< $10K	Acceptable; minor modification and does not impact the project	No impact	Department Level	Minimal Impact
2	<$30K	Within the acceptable limit	Slight impact	Organization Level	Moderate Impact

3	<$50K	Below expectation; moderate changes required	Instability over weeks	Local	High Impact
4	<$70K	Unacceptable; significant changes required	Significant impact of weeks	Reginal	Severe Impact
5	<$100K	Unacceptable; does not meet threshold requirements	Long term impact	National	Crisis Mode

TABLE II. LIKELIHOOD AND CONSEQUENCES OF RISK OCCURRENCE (L)

1	Very rare	Once every 10 years
2	Rare	Twice every five to ten years
3	Occasional	Once every five years
4	Probable	Once a year
5	Frequent	More than once during the year

$$RC = [(RL \times 2) - 1] \quad (3)$$

The probabilities, future impact, and existing impact are rated on a scale of 1 to 5. Hence, Eq. (3) calculates the overall risk classification (RC) with a score from 0 to 5, where zero indicates that the risk impact is very low, while 5 means the risk is very high and requires treatments as detailed in the below section.

C. Risk Treatment

Once risks are identified and classified, a treatment plan needs to be in place to address these threats. The plan should outline the risk treat that includes [24]: (1) Avoidance for the unacceptable risks, they can be eliminated with the step of actions and required controls to reduce the risk; (2) share as it can be transferred to third party responsibility; (3) acceptance without taking actions to prevent the outcome; (4) the risk can also be mitigated to reduce the probability of occurrence or the impact of an unfavorable event. Mitigation requires budget allocation as it is usually handled by high threats. The risk treatment plan should also specify the risk owner and target resolution date. In addition, contingency plans are required in advance to be ready and prepare in case the risk events occur.

D. Risk Monitoring

IT systems are developed with proper methods and techniques to control IT incidents and possible risks. Therefore, continuous identification, assessment, and monitoring of residual risks are crucial for organizations, especially during project execution [4]. At this phase, the risk can be reassessed based on the environmental changes or major milestones, the ratings and prioritization can be changed with further qualitative or quantitative risk analysis. It also can help in examining and documenting the risk audits with an effective response to control risk [23]. In addition, corporate strategic priorities usually change over time. Thus, the risk identification and assessment should address those changes to ensure strategic alignment is maintained to support the strategic decision-making.

Implementing RMM with a traditional approach is not easy as handing the risk management portfolio requires an automated solution to ensure the risks are consistent and efficient to capture the remaining unidentified risks. In addition, it helps document workflow risk assessment, while supporting generating reporting and recommending remediation. Our research aims to address this dilemma by automating the RMM with an enterprise risk management solution that provides a centralized risk repository. It is required to consolidate the entire organization's risks with IT-related risks to conduct an appropriate risk assessment.

Automating RMM has added many advantages to our process, such as (1) shifting RMM from reactive models toward a proactive approach to predict potential risks; (2) presenting a clear RMM workflow and reporting process, as it improves the process in analyzing and managing critical risks; (3) maintain up-to-date data, as it helps in getting more accurate and on-time accessible data; and (4) eliminate insurmountable manual tasks and human error, as risk-related information can be collected, organized, and uploaded with ease and accuracy.

V. RESULTS

The automated solution provides the ability to identify business risks across the organization with a built-in centralized library, which helps in aligning IT and business risks across the organization, controlling processes, resources, and identifies interdependencies.

We have configured the system to conduct risk assessments based on our criteria, listed in Table 2. In addition, it provides the capability of monitoring and tracking the mitigating activities and controls by easily spot gaps to take immediate action for better risk management. Such solutions helped in providing interactive dashboards and risk matrices to drive and support the management with better decisions across the organization.

TABLE III. RISK PROFILE OF EMAIL SERVICE

Risk Profile	
Name: Email Outage	Abbrv.: EM_01
Risk Description: Losing email service, which is one of the smooth communication methods to deliver messages internally and externally with customers and suppliers.	
Likelihood of Occurrence: L = 5 ➔ More than once a year.	
Impact: EI = 2 ➔ Within an acceptable limit in the organization, less than $30K. FI = 3 ➔ Instability over weeks within local to reginal impact that may exceed $50K of loss.	
Risk	
Lack of internal and external communications, delay operation productivity and services delivery.	
Calculation	
$RL = \sum (\frac{5 + 3 + 2}{5}) = 2$	
$RC = [(2 \times 2) - 1] = 3$	
Result: The overall risk score for email services is 3, which is moderate.	

Testing RMM is essential to validate the effectiveness of our model in addressing the challenges of traditional risk management approaches. Thus, to further evaluate our model, the likelihood, and impact are selected as key technical indicators to validate the readiness of the solution. We have

tested our RMM with one of the critical corporate services, which is email, as losing this service can almost shut a business down. Like any other technology solution, email might be interrupted more than once a year with varying levels of impact that can be local within the organization or extended to be regional level. As detailed in Table 3, it results in an affordable risk score. In addition, the automated solution simplifies the adoption of IT governance and risk management with an up-to-date information of critical corporate risks that is visible to the concerned entities with a graphical dashboard.

VI. LIMITATIONS AND CONCLUSION

The results demonstrated a complete view of the enhanced IT risk management model based on the literature review. There are a few limitations with the presented results that can be extended further to future studies. First, the solution is limited to IT organizations, yet it could be expanded to be utilized for non-IT organizations like ministries or corporate, healthcare, and education institutions. Second, future researchers may introduce benchmarking with other IT organizations and could also examine the model for large-scale enterprises. Lastly, the presented framework can be extended by exploring alternative methods to overcome the uncertainty of risk impacts that may appear.

Risk management is driven through a framework that is designed to identify, evaluate the impact of the organization's risks, and prepare the treatment plan and response. The manual process of risk management, misalignment with corporate strategy, and subjective assessment are major challenges for organizations. In this paper, we discussed some of the key aspects of IT governance and risk management, to overcome these challenges. Our approach is designed with an IT risk management model to outline the acceptable risk level that delivers the assurance level to various IT processes and services based on corporate rules and regulations. This is to adequately protect IT businesses against any misuses, which in return helps to deliver a better perspective on the governance functions.

REFERENCES

[1] V. Grembergen, W. and S. De Haes. "Introduction to the Minitrack on IT Governance and its Mechanisms." (2018), Pages 94.

[2] Carla L. Wilkin, Paul K. Couchman, Amrik Sohal, Ambika Zutshi, “Exploring differences between smaller and large organizations' corporate governance of information technology”, International Journal of Accounting Information Systems, Volume 22, 2016, Pages 6-25. https://doi.org/10.1016/j.accinf.2016.07.002.

[3] Clarke, J.E., Liesch, P.W. “Wait-and-see strategy: Risk management in the internationalization process model”. J Int Bus Stud 48, 923–940, 2017. https://doi.org/10.1057/s41267-017-0110-z.

[4] A. Ledwoch, H. Yasarcan, A. Brintrup, “The moderating impact of supply network topology on the effectiveness of risk management”, International Journal of Production Economics, Volume 197, 2018, Pages 13-26, Online: https://doi.org/10.1016/j.ijpe.2017.12.013.

[5] M. Bevilacqua, F. Emanuele Ciarapica, “Human factor risk management in the process industry: A case study, Reliability Engineering & System Safety, Volume 169, 2018, Pages 149-159, https://doi.org/10.1016/j.ress.2017.08.013.

[6] P. Ferreira de Lima, M. Crema, C. Verbano, “Risk management in SMEs: A systematic literature review and future directions”, European Management Journal, Volume 38, Issue 1, 2020, Pages 78-94. https://doi.org/10.1016/j.emj.2019.06.005.

[7] M. Shad, F. Lai, Chuah, L. Fatt, J. Klemeš, A. Bokhari, “Integrating sustainability reporting into enterprise risk management and its relationship with business performance: A conceptual framework”, Journal of Cleaner Production, Volume 208, 2019, Pages 415-425. https://doi.org/10.1016/j.jclepro.2018.10.120.

[8] Friday, D., Ryan, S., Sridharan, R. and Collins, D. (2018), "Collaborative risk management: a systematic literature review", International Journal of Physical Distribution & Logistics Management, Vol. 48 No. 3, pp. 231-253. https://doi.org/10.1108/IJPDLM-01-2017-0035

[9] A. Joshi, L. Bollen, H. Hassink, S. De Haes, W. Van Grembergen, “Explaining IT governance disclosure through the constructs of IT governance maturity and IT strategic role, Information & Management”, Volume 55, Issue 3, 2018, Pages 368-380, https://doi.org/10.1016/j.im.2017.09.003.

[10] P. Wortman, J. Chandy, SMART: security model adversarial risk-based tool for systems security design evaluation, Journal of Cybersecurity, Volume 6, Issue 1, 2020, tyaa003, https://doi.org/10.1093/cybsec/tyaa003

[11] J. Bakdash, Steve Hutchinson, Erin G Zaroukian, Laura R Marusich, Saravanan Thirumuruganathan, Charmaine Sample, Blaine Hoffman, Gautam Das, Malware in the future? Forecasting of analyst detection of cyber events, Journal of Cybersecurity, Volume 4, Issue 1, 2018, tyy007, https://doi.org/10.1093/cybsec/tyy007

[12] C. Weir, A. Rashid, J. Noble, Challenging software developers: dialectic as a foundation for security assurance techniques, Journal of Cybersecurity, Volume 6, Issue 1, 2020, tyaa007, https://doi.org/10.1093/cybsec/tyaa007

[13] Corallo A, Lazoi M, Lezzi M. Cybersecurity in the context of industry 4.0: A structured classification of critical assets and business impacts. Computers in industry. 2020 Jan 1;114:103165. https://doi.org/10.1016/j.compind.2019.103165

[14] Vijayakumar, K., Arun, C. Automated risk identification using NLP in cloud-based development environments. J Ambient Intell Human Comput (2017). https://doi.org/10.1007/s12652-017-0503-7

[15] Gonzalez-Granadillo G, Dubus S, Motzek A, Garcia-Alfaro J, Alvarez E, Merialdo M, Papillon S, Debar H. Dynamic risk management response system to handle cyber threats. Future Generation Computer Systems. 2018 Jun 1;83:535-52. https://doi.org/10.1016/j.future.2017.05.043

[16] T. Aven. Risk assessment and risk management: Review of recent advances on their foundation; European Journal of Operational Research, Volume 253, Issue 1, 2016, Pages 1-13, Online: https://doi.org/10.1016/j.ejor.2015.12.023.

[17] Ali, Syaiful, and Peter Green. "Effective information technology (IT) governance mechanisms: An IT outsourcing perspective." Information Systems Frontiers 14.2 (2012): 179-193.

[18] E. Game, J. Fitzsimons, G. Moore and E. Madden. Subjective risk assessment for planning conservation projects, Volume 8, Number 4, 2013, Environmental Research Letters.

[19] T. Wen, H. Chung, K. Chang, Z. Li, A flexible risk assessment approach integrating subjective and objective weights under uncertainty, Engineering Applications of Artificial Intelligence, Volume 103, 2021. Online: https://doi.org/10.1016/j.engappai. 2021.104310.

[20] M. Khouja, I. Rodriguez, Y. Halima, S. Moalla; "IT Governance in Higher Education Institutions: A Systematic Literature Review," International Journal of Human Capital and Information Technology Professionals (IJHCITP), IGI Global, Volume 9(2), pages 52-67, 2018.

[21] D. Dobrygowski, D. Vadala; “Does Your Board Really Understand Your Cyber Risks?”; Harvard Business Review Digital Article. 2020. Online: https://hbr.org/2020/09/ does-your-board-really-understand-your-cyber-risks.

[22] P. Hopkin “Fundamentals of risk management: understanding, evaluating and implementing effective risk management”. Kogan Page Publishers, 2018.

[23] Van Grembergen, Wim, and Steven De Haes. "Introduction to the Minitrack on IT Governance and its Mechanisms." 2018, Page 3.

[24] Giannakis, Mihalis, and Thanos Papadopoulos. "Supply chain sustainability: A risk management approach." International Journal of Production Economics 171 (2016): 455-470.

[25] Olechowski, Alison, et al. "The professionalization of risk management: What role can the ISO 31000 risk management principles play?" International Journal of Project Management 34.8 (2016): 1568-1578.