NOVATEUR PUBLICATIONS
INTERNATIONAL JOURNAL OF INNOVATIONS IN ENGINEERING RESEARCH AND TECHNOLOGY [IJIERT]
ISSN: 2394-3696
VOLUME 7, ISSUE 5, May-2020

RISK MANAGEMENT IN INFORMATION TECHNOLOGY

SIKENDER MOHSIENUDDIN MOHAMMAD
Dev Ops, Information Technology USA
sikendermohammad@gmail.com

ABSTRACT
Risk management in information technology is the research problem in my essay. Research has shown that business risks related to information technology risk management can be considered and adopted within an organization or enterprise. The study has been demonstrated that some organizations have a well-laid enterprise risk management set out. In this case, therefore, risk management is seen as part of enterprise risk management. The study will also further expound on the risk management methodology, which constitutes a generic framework. The framework must, therefore, be considered as a risk management exercise. Based on a review of literature, the risk management procedure has taken into account risk assessment that ENISA has over time, reviewed the process to parameterize the entire risk management process. Risk identification states that there can be potential losses when threats, assets vulnerabilities, consequences, and related business processes are not considered. Therefore risk management in information technology must revolve around integrating risk management through the system development life cycle. The process cannot be termed as complete if risk management methods are not considered. In 2006, the threat sketch started a cybersecurity risk assessment that targeted small companies. In this study, the methodology uses real options, to prioritize and forecast a list of fixed high-level threats.

KEYWORDS: Risk Management, Information Technology, Mitigation, Industries.

INTRODUCTION
Risk management is the act of evaluating and forecasting financial risks. The process also entails the identification of procedures to minimize the impacts. Information technology, on the other hand, is the study and use of systems. The study is used to retrieve, store, and send information. Risk management in information technology should be termed as the application of financial risks and the identification of procedures to reduce losses in the information technology field. The two have, in detail, been featured in the literature review, where assessment, methods, methodology have been touched on. Definitions have also been included to understand better the different organizations that deal with the identification of information technology risk management processes.

LITERATURE REVIEW
Information technology risk management is an application that manages risks involved in an organization's management in matters to do with information technology. This is also viewed as part of the broader enterprise risk management system, established to perform updates regularly in information security management systems. The systematic approach for the identification process is used to give information regarding security risks. According to the risk information technology framework, risk in this field is strictly tied to the uncertainty of decision theory. Generally, the risk is considered a product of likelihood. Information technology can be defined as a product of vulnerability, threat, and asset values. The value is acquired through Risk = Threat * vulnerability
* Asset (Minoli & Kouns, 2011). According to research, the process of risk management is termed an ongoing alternative method, and must continuously be repeated indefinitely. In this literature review, the main subject of the study was based on risk management, and it has struck a balance between cost, productivity, and the value of information assets, being protected.

DEFINITION:
Reliable information, in regards to risks associated with information technology, was produced in 2006. The report was presented by ISACA, which is an international professional association. The association focuses

on IT governance, providing definitions of risk management (Isaca, 2009). In this case, risk managers are in a better position to balance economic and operational protective measures. The head of the IT organization must be in a position to understand that capabilities ought to accomplish its mission. Also, the national information assurance training and education center defines risk management as the process of identifying and minimizing the impacts of uncertain events. In this department, risk management aims to reduce risk as well as obtain and better still maintain approval. Besides the two, another source, managerial science, also verifies that risk management in information technology encompasses four phases. The first phrase is a management decision, effectiveness review, control implementation, and risk assessment, as received from an evaluation of threats and vulnerabilities.

The general process of risk management in information technology is eliminating or minimizing uncertain events, affecting system resources. Therefore, risk management in information technology is encompassed under risk analysis, security evaluation of safeguards, implementation and test, and finally, overall security review.

Chapman (2011) defined risk as exposure to possible financial gains or losses. To better understand different authors, breaking it down to three stages, first approached the task of risk management. Risk analysis is the first, risk identification, the second, and risk response the third.

RISK MANAGEMENT BREAKDOWN

A methodology for risk management was first developed by Leung and Tummala (2011). Still on the same, the two aimed at the assessment, measurement, evaluation, and monitoring. Applying methodology sought to manage the risk of the high cost. The cost, in this case, was in regards to an EHV transmission line project. William, (2007), also reviewed a couple of researches related to project risk management. In his work, therefore, William was able to describe and analyze tools used by researchers and practitioners. His work also touched on the management structures and procedures required to manage risks in information technology. Another example is Turner (2016). Turner's argument is based on expert judgment. Further, his study is based on identifying risk factors.

The analysis focused on analyzing the project as a whole. The management, in this case, is, therefore, after two aspects being the activities critical in determining the risk management in information technology and the total duration covered. As seen, many authors have laid down the distribution of time's events, terming it as the classical distribution. However, some authors (Farnum and Stanton, 2007) proposed their distributions for practical simulations.

RISK MANAGEMENT IN SOFTWARE DEVELOPMENT

A couple of researchers have been identified as first-hand reporters of risk on software development (Barki et al., 2010). However, most of the information passed out is based on anecdotal evidence, or most occasions, based on limited studies. Therefore, this means that education, in this case, is narrowed down to a portion of the development process. Additionally, indulging the process operators does not identify risk management in information technology.

The fact is contradicted by Ross and Boehm (2015), who provide some meaningful classification. The classification does not, however, revolve around any strategy for risk mitigation. Boehm (2011), had his work termed as the most important because of one critical factor. The factor in line is that he identified the top ten most software risk items. On the other hand, Keil et al. (2016), developed a framework for strategy development and risk classification. However, his study was not up to standard, for he did not link it to the software development cycle. Another prominent figure is Baccarini et al. (2004). He is seen to have prioritized and featured IT projects risk through empirical research. Any framework for software risk management is not catered for in the study.

MANAGING RISK IN SOFTWARE DEVELOPMENT UNDER INFORMATION TECHNOLOGY

Risk management, in this case, is not comprehensive. (Bandyopadhyay et al., 2018). It is so because they deal with particular types of risks. Rainer et al. (2011) have also proposed a framework for

identifying the strategic dangers of information technology. The structure in it carries quantitative and qualitative methodologies. Epich and Person (2011), have, on the other hand, proposed a disaster recovery plan to reduce IT risk methodically. The risk management framework is based on identifying risky work packages, analyzing risk, identifying risk events, and developing a risk management plan. All these features are equally crucial for they are very vulnerable to cost, time, and quality targets. Target failures are, on the other hand, identified with both functional and IT executives.

APPLICATION

Application, in this case, is entirely based on scope work breakdown and requirement analysis. Requirement analysis is done through the process reengineering framework. (Dey, 2001). Through the use of IT and a competent workforce from TCPO, the framework that involves the scope and work breakdown structure is achieved. The range helps in deriving the project as well as deriving risk management with the active involvement of project owners as well as software developer representatives. The breakdown of risk management is still, in this case, broken down in packages. The first one is the registry module, planning module, data conversion of existing data, and documentation of modules.

RISK MANAGEMENT IN INFORMATION TECHNOLOGY

Information Technology has dramatically grown into an indispensable business paradigm that is more of a department. Information Technology predominantly drives the changing world of business. Planning, management, risk mitigation, and system operations are majorly taking shape under IT structures and systems. The global economy would be something else if the factor of Information Technology. The phenomenon has grown drastically, and it has been imperatively integrated into our personal and career lives. With the colossal impact, role, and intervention of IT, the gates for risk paradigms and forces open (R. Baskerville, P. Spagnoletti, and J. Kim, 2014). IT project policies, regulations, and management establish a multifaceted and obscure environment that translates to a unique range of risks. A downfall of the IT system, error, risk, and threats can target any business segment or facet (Thakurta, 2014). Mitigating harmful threats, impacts, and outcomes are the foundation of any initiative and policy of risk management. The challenge and process of risk management is a whole new menace that is giving IT experts and software managers sleepless nights. IT project managers are the custodians of all risk management processes adopted in an organization.

Before sinking deeper into the topic discussion, it is highly valuable to encounter the dilemma of compliance to regulations and requirements that are intricately changing and shifting in intensity and magnitude (L. Lema et al., 2015). IT risk mitigation regulations are dynamically evolving, and system updates are updated from time to time.

Over the past decade, numerous studies on risk mitigation and management in Information Technology have been done. In a significant way, most of the reviews are aligned with the identification and prioritization of risks through integrated empirical research findings (Irfandhi, 2016). Experts are regularly and tirelessly working to offer solutions to the bulging security counter plans and executions initiated, supported, and even funded by cybercrime cartels. The process of IT Risk Management is the systematic formulation, testing, and application of risk management protocols to fight the threats posed by IT risk. Risk management has swollen to the capacities of integrated enterprise risk mitigation protocols and systems. Robust risk mitigation and management tool are the Information Security Management System (ISMS) (Knut Haufe et al., 2016). The device has been heightened as a massive indicator of a company's commitment to identifying, analyzing and managing risks and threats of information security (Talet, A. N., Mat- Zin, R., & Houari, M, 2014). The ISMS tool comes with a stringent IT framework architecture that only indulges the negative implications of operations and service delivery that are poised to birth losses in value, destructive performances, and the broader leverage of missing opportunities.

Risk management is a continuous process whose iterative nature should never be compromised by adjustments in leadership, business lines, and expansion policies. One of the top sustainability challenges in the current business world is keeping a vibrant and well-protected risk management system in IT systems and networks. For sustainability goals, the counter-measures adopted must be accurate and firm in striking a resolute balance between cost, productivity, effectiveness, and reliability of the measures (W. Pieters, C. W.

Probst, S. Lukszo and L. Montoya, 2014). The value of the informational asset and system under threat should be the primary focus to foster the importance of ultimate customer satisfaction and production growth.

Risk management is a protocol framework for identifying, assessing, and mitigating risks to hit acceptable levels. Risk assessment gives business organizations the foundation of determining the depth of a potential threat in an IT system. Once the assessment process is finished, the outcome highlights the appropriate control steps to reduce the chances of future complexities. The guide of the assessment process highlights the development of an effective risk mitigation plan.

The entire process should be guided by a prime objective of creating a system development life cycle (SDLC). The SLDC should be given top-most attention and investment from all organizational segments. The top management has the sole responsibility of ensuring and funding the implementation of the SDLC. With the risk assessment guideline, SDLC gives the organization tailor-made infrastructure to face the unfathomable implication of attackers. Integrated and continually evaluated cost-effective updates and controls. Across many organizations, IT systems are on the surge dominated by change, updates, embedded software versions that are made to replace the outdated systems and programs.

With the increase in new adoptions and systems in IT risk management, the call for skill development and personnel changes is even louder. In this regard, the actualized changes translate to newly defined risks that may be more puzzling and sophisticated. If the proper steps to mitigate the new developments are not considered, a resurgence in the adverse implication of the previous system threats sets in. All said it becomes a reality that risk management is a delicate process that is constant and full of evolving realms.

Risk Management is a critical process that supports IT managers and experts to strike a balanced ground for operational and economic costs of protective and mitigative measures for measurable milestones in secured system capacities in IT and data management. The process of Risk Management is synonymous with the IT environment, and it permeates and controls decision-making in all aspects and sections of economic production and general daily lives. At the mix of the measures and policies of Risk Management in IT lies the various organizational leadership. They are the key policymakers in the process, and their responsibilities should be informed by technical advice that should come from all key stakeholders in IT management and data handling networks. To uplift the IT management systems, improved budget allocations, and resources should be enhanced and maintained across the year. The mission-essential system handling should be supported to ensure that every move step is helpful and productive in helping risk and data management.

METHODOLOGIES OF RISK MANAGEMENT IN INFORMATION TECHNOLOGY

As per the overall Information Technology Risk framework provided by the ISACA, it is clear that risk management is part of the objectives of the enterprise risk management (Rodríguez, Ortega, & Concepción, 2017). The risk in Information Technology needs to be administered in the Enterprise risk management framework. The degree of risk sensitivity and risk appetite of the entire enterprise should provide directions to the process of Information Technology risk management. The enterprise risk management must deliver the necessary objectives to IT risk management (Ramos, & Yoo, (2019, March). While the methodologies managing risks in Information Technology does not outline a particular approach that should be followed. Risk management methodology in the Information Technology sector can be subdivided into ton sub-processes of risk management, which appear in a systematic order. In the context risk management, the term methodology implies to the systematic steps combined with regulations and principles that drive action of managing risk in the information technology.

Because of the complex nature as well as having cost-benefit analysis as a need, Information Technology (IT) risks are administered or managed to utilize a methodology that is subdivided into the following three phases as per the NIST SP 800-30. The first phase is the risk assessment, the second step is risk mitigation, and the third phase entails risk evaluation and assessment (Pillitteri, 2019). A risk management approach that is effective and efficient should be ultimately be integrated into the systems development life cycle. In the IT sector, any critical analysis of information that is conducted on different applications, hardware and software installation, network systems, and that system that are undergoing development must be done through structured methodologies.

ESTABLISHING THE SETTING OF RISK

According to the ISO/IEC framework, setting the context of risk is the first and foremost step in risk management in the Information and technology sector. Several elementary operations are perceived as the initial step of risk assessment in Information Technology (Borkovskaya, Roe, & Bardenwerper, 2018). This phase incorporates the actual acquisition of every viable data concerning the organization's information technology and the evaluation of the critical criteria, objectives, and scope of risk management processes. The requirements, in this case, entails risk evaluation, risk acceptance, and effect determination requirements. The criteria usually are conditioned and guided by the legal requirements, the business value for its information technology, stakeholders' expectations, and the business reputation. In typical cases, the objectives are complying with the minimum regulatory standards and provision of tangible evidence. For information technology, the scope can be a given incident response plan.

RISK ASSESSMENT

Managing Risk in Information Technology is a recurrent process that incorporates different activities such as analysis, planning, execution, control, and review of the executed risk and security measurements as well as the security policies that are enforced by both the law and organization (Aven, 2016). In Information Technology, assessment of risk is usually done at discrete time intervals. And this gives a non-permanent perception of the assessed risk while making the whole process of risk management permanent. Risk assessment is the process of managing risk in Information Technology that is usually done in more than a single iteration.

The initial one is the high-level assessment that is utilized in identifying those high risks. Whereas the second iterations are composed of the examination of the critical risks.

In the Information Technology sector, risk assessment alludes to the critical study of the potential vulnerabilities, threats, uncertainty, loss, and the non-practical impact of the set security measures. Information Technology utilizes the outcomes of a risk assessment process in developing the security needs and different specifications of the risk management process. Additionally, in the information technology sector, risk assessment can include the techniques of determining potential threats and vulnerabilities postulated and known to evaluate the expected degree of loss and develop a particular level of acceptability to the system's operations. Risk assessment provides a systematic approach for assessing the critical value and the potential of computer and network installation assets, examining the vulnerabilities, anticipating the loss expectancy, examining the protection measures in place and adding more alternatives for protection. Those viable decisions for executing more protection features are usually dependent on the availability of a good ratio between benefit and cost of the information asset that needs to be given security. The methodologies of risk assessment can include qualitative or quantitative techniques or both of these techniques. It can be done as an informal review of a microcomputer network as well as a big computer installation. In the process, the outcome of establishing the setting phase is used as input for the risk assessment step.

The risk analysis process is again subdivided into risk identification, risk estimation, and risk evaluation (Barafort, Mesquida, & Mas, 2017). Risk identification defines the immediate cause of a given loss. In the process of risk identification, it is crucial to identify the threats, vulnerabilities, consequences, the primary assets involved, and the security measures in place and those planned. In the information technology sector, the outcome of risk identification can be a list of vulnerabilities that are not connected to those threats that are defined, several different incident concerns as well as their consequences and the assets as well as networks that are to be risk- managed.

Risk estimation is the other part of risk analysis/assessment, and we have qualitative and quantitative approaches to risk estimation (Pitera, & Schmidt, 2018). The quantitative risk is associated with numerical calculations that depend on different security metrics on the information technology asset. For the quantitative approaches, we take into consideration various risk factors. Different mathematical processes are utilized in estimating the degree of risks. The probability of occurrence is a fundamental mathematical concept that is employed for the quantitative approach. It is important to note that not only is the value of those assets that are affected that should be taken into account but the amount of all the assets that are

engaged. On the other hand, qualitative risk analysis is utilized when the Information Technology sector wants to conduct a risk assessment process within a short duration and with a tight budget and does have too much technicality. A lesser amount of data is utilized in the process. Generally, risks that originate from security threats and other potential adversary attacks might not be easy to estimate.

Risk evaluation compares the various levels of risk against the risk acceptance criteria (Rodríguez, Ortega, & Concepción, 2016). This process also tends to priorities the amount and levels of chances with the indication of treating risks. To evaluate the potential of a future lethal occurrence, the potential threats to an Information Technology system need to be in line with the vulnerabilities and the implemented measures for the IT system.

RISK MITIGATION

Being the second and third process by SP 800-30 and ISO 27005, respectively, risk mitigation entails prioritization, analysis, and implementation of the most suitable risk control approach as per the risk assessment recommendations (NEJM Catalyst, 2018). Complete elimination of risks is an ideal situation that is impractical. Having that, top leadership and management should invest in the least-cost approach to plummet the adversity and severity of mission risk. The whole intervention protocol should inflict no harmful effect on enterprise resources, strategic plans, and mission statements.

In a considerable measure, the risk treatment process necessitates security interventions to lower, avoid, or transfer risk with the imposition of a risk mitigation policy and plan. The outcome of the mitigation should meet the acceptance threshold from the management scale of analysis.

Numerous security measures are available for selection. The choice made by an organization depends primarily on the business strategy, business environmental constraints (NEJM Catalyst, 2018). All said and done, the decision should always be firm, non-obscure, and documented. The process of accepting risk is never easy, and it sometimes comes with a tremendous cost. Risk acceptance is a crucial step in the entire journey to mitigate a threat and danger.

In the event of a very impactful risk, the option of risk transfer becomes the alternative. Internal systems of security control cannot be employed, given the high chances of being overwhelmed. Insurance policies are the external realms that should be designed to mitigate costs and, eventually, reach a stable ground for treating the risk (Rouse, 2018). If the option of an insurance policy becomes unreachable, a person with the capacity to manage and mitigate the risk can be outsourced.

Risk avoidance and aversion is another potential action that encompasses new and alternative business ways to block the gates and opportunities of risk occurrence. The choice of banning cash transactions and adopting digital and mobile money payments is a risk avoidance approach (Qazi Abroon, John Quigley, and Alex Dickson, 2018). Without cash handling systems, the company can avoid the risk of fake money and the agony of cash transaction fraudsters. As mentioned earlier, the space for utter elimination of risk is nowhere near realization. After a risk mitigation process, the remnants of risk elements form the residual risks. The magnitude of the residual risk is a determinant of the new step taken in the affected segment of business operations (Rouse, 2018). If the residual risk is still intricate, then the treatment and mitigation process is iterated and revitalized.

Another approach to mitigate risk is through integrated research and acknowledgment. At all times, they are lowering losses by acknowledging the flaw. Through analysis, necessary corrections are analyzed to counter the effects of vulnerability (Qazi Abroon, John Quigley, and Alex Dickson, 2018). In all situations, the top leadership should create an essential infrastructure that helps in offering systematic and intelligent research solutions to mitigate particular risks.

MONITORING OF RISKS

Risk management is a continuous process that exists so long as a business entity is alive and kicking. At all times, the leadership and top management are tasked with monitoring the stages of risk mitigation. Relevant reviews and adjustments are rendered after considerations from the assigned officers and expertise. The implemented changes should be driven towards lifting the performance efficacies of the affected department or process. As time goes, business opportunities and vulnerabilities change (Rouse, 2018). Hence, the precarious calls for adjustments in the risk handling frameworks.

As a stringent component and aspect of risk monitoring, regular and comprehensive audits should be adopted in the system. For authenticity and trust in the risk audit procedures, the services should be outsourced (Rouse, 2018). The audit service provider should also ensure that daily ISMS management is protected and ultimately performed.

REFERENCES

1) Aven, T. (2016). Risk assessment and risk management: Review of recent advances on their foundation. European Journal of Operational Research, 253(1), 1-13.
2) Barafort, B., Mesquida, A. L., & Mas, A. (2017). Integrating risk management in IT settings from ISO standards and management systems perspectives. Computer Standards &
3) Interfaces, 54, 176-185.
4) Bakos, J. Y., & Treacy, M. E. (1986). Information technology and corporate strategy: a research perspective. MIS quarterly, 107-119.
5) Chapman, R. J. (2011). Simple tools and techniques for enterprise risk management (Vol. 553). John Wiley & Sons.
6) Nadikattu, Rahul Reddy, Risk Management in the IT Department (May 21, 2020). Risk Management in the IT Department, International Journal Of Advance Research And Innovative Ideas In Education, Volume 6, Issue 3, 2020. Available at SSRN: https://ssrn.com/abstract=3620047
7) Chitty, A. (1987). Information technology and people: designing for the future. Design Studies, 8(2), 117-118.
8) Kouns, J., & Minoli, D. (2011). Information technology risk management in enterprise environments: A review of industry practices and a practical guide to risk management teams.John Wiley & Sons.
9) Raisinghani, M. S. (Ed.). (2008). Handbook of Research on Global Information Technology Management in the Digital Economy. IGI Global. Rhodes, W. L. (1986). Infosystems Volume 33, Issue 8.
10) Turban, E. (2008). Information technology for management. John Wiley & Sons, Inc. [11]Borkovskaya, V. G., Roe, R., & Bardenwerper, W. (2018, October). Sustainability Risk Management: The Case for Using Interactive Methodologies for Teaching, Training, and Practice in Environmental Engineering and Other Fields. In The International Science and Technology Conference" FarEastCon" (pp. 251-260). Springer, Cham.
11) [12]Pillitteri, V. (2019). The Next Generation Risk Management Framework (RMF 2.0): A Holistic Methodology to Manage Information Security, Privacy, and Supply Chain Risk (No. ITL Bulletin, February 2019). National Institute of Standards and Technology. [13]Pitera, M., & Schmidt, T. (2018). Unbiased estimation of risk. Journal of Banking & Finance, 91, 133-145.
12) [14]Rodríguez, A., Ortega, F., & Concepción, R. (2016). A method for the evaluation of risk in IT projects. Expert Systems with Applications, 45, 273-285.
13) R. Baskerville, P. Spagnoletti, and J. Kim. (2014). Incident-centered information security: Managing a strategic balance between prevention and response. Information & Management Journal, vol. 51, no. 1, 138–151.
14) Rodríguez, A., Ortega, F., & Concepción, R. (2017). An intuitionistic method for the selection of a risk management approach to information technology projects. Information Sciences, 375, 202-218.
15) Ramos, M. J. B., & Yoo, S. G. (2019, March). Developing an Information Security Management System for Libraries Based on an Improved Risk Analysis Methodology Compatible with ISO/IEC 27001. The International Conference on Advances in Emerging Trends and Technologies (pp. 371-379). Springer, Cham.
16) Irfandhi, K. (2016). Risk Management in Information Technology Project: An Empirical Study. ComTech Vol. 7 No. 3, 191-199.
17) Knut Haufe et al. (2016). A process framework for information security management. International Journal of Information Systems and Project Management, 27-47.
18) [20]L. Lema et al. (2015). ITIL in small to medium-sized enterprises software companies: towards an implementation sequence. Journal of Software: Evolution and Process, vol. 27, no. 8, 528–538.

19) Talet, A. N., Mat-Zin, R., & Houari, M. (2014). Risk Management and Information Technology Project. International Journal of Digital Information and Wireless Communications, 4(1), 1-9.
20) Thakurta, R. (2014). Managing Software Projects Under Foreseen Uncertainty. Journal of Information Technology Management, 25(2), 40-52.
21) W. Pieters, C. W. Probst, S. Lukszo, and L. Montoya. (2014). Cost-effectiveness of Security Measures: A model-based framework. Approaches and Processes for Managing the Economics of Information Systems, 139.
22) NEJM Catalyst. (2018). What Is Risk Management in Healthcare? https://catalyst.nejm.org/doi/full/10.1056/CAT.18.0197.
23) Qazi Abroon, John Quigley, and Alex Dickson. (2018). Cost-Effectiveness and Manageability Based Prioritisation of Supply Chain Risk Mitigation Strategies. Supply Chain Risk Management. Springer, Singapore, 23-42.
24) Rouse, M. (2018, June 29). Risk Mitigation. Retrieved from Techtarget.com: https:// search disasterrecovery .techtarget.com/definition/risk-mitigation.