Chapter 13
Information Technology Risk Management

Gurdip Kaur and Arash Habibi Lashkari

13.1 Introduction to Risk Management

In the techno-savvy world, information technology (IT) risk management is one of the crucial issues faced by IT professionals. With the unprecedented upsurge in IT infrastructure, security issues arising from assets have also increased steeply. The rising security issues have made IT assets more vulnerable to IT risks. The use of IT is prone to several potential risks in organizations. According to a survey published by the Security Boulevard [1], global IT spending is expected to increase to $3.9 Trillion by the end of 2020. Another report by the Federal Bureau of Investigation's Internet Crime Complaint Center (FBI/IC3) 2019 indicates that over $3.5 billion is reported as a loss against cybercrime in 2019 alone. This includes a total of 467,351 incidents reported by businesses and individuals [2]. Therefore, it is pertinent to manage these risks faced by IT professionals.

The objective of risk management is to protect information technology assets such as hardware, software, data, applications, personnel, and facilities from internal and external threats so that cost of losses is minimized [3]. Internal threats include technical outage, unauthorized access, and sabotage, whereas external threats include natural disasters such as earthquakes and tornadoes. The purpose of performing risk management is to reduce or avoid the losses incurred due to unavoidable situations. This helps the management to take informed decisions to plan and justify their IT expenditures.

IT risk management undergoes multifaceted challenges including changing technology; integrating hardware, software, data, and applications; identifying the right talent; implementing work ethics; and complying to policies and standards. All

G. Kaur (✉) · A. H. Lashkari
Faculty of Computer Science, Canadian Institute for Cybersecurity (CIC), University of New Brunswick, Fredericton, NB, Canada
e-mail: Gurdip.Kaur@unb.ca; A.Habibi.L@unb.ca

K. Daimi, C. Peoples (eds.), *Advances in Cybersecurity Management*,
https://doi.org/10.1007/978-3-030-71381-2_13

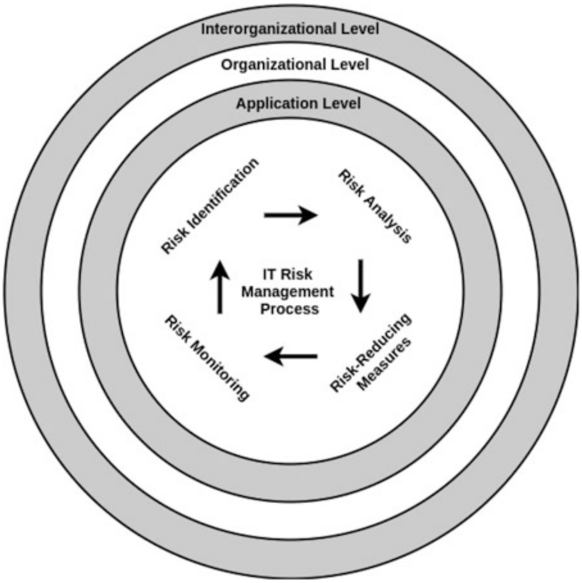
these challenges need proper redressal to mitigate risks at the organizational level. IT risk management is a continuous process that addresses the following fundamental questions:

- What are the system characteristics and potential threats to assets?
- What are potential vulnerabilities and the likelihood of their occurrence?
- How can the risk associated with IT environment be mitigated?
- Who is responsible for preparing a safeguard plan to mitigate risks?

According to the National Institute of Standards and Technology Special Publication (NIST SP) 800-30, risk management cycle comprises three primary components: risk assessment, risk mitigation, and risk evaluation and assessment. Risk assessment process includes risk identification and evaluation to determine its impact and recommendation of risk-reducing measures. The risk mitigation refers to prioritizing, implementing, and maintaining the appropriate risk-reducing measures proposed in risk assessment component. Finally, the third component performs continuous evaluation [4]. Figure 13.1 provides a traditional and popular integrated IT risk management framework that sheds light on interconnections between the levels and the risk management components.

This framework classifies IT environment into three levels: application, organizational, and interorganizational. Application-level concentrates on risks related to technical failure and implementations arising from internal and external sources. Organizational level deals with the impact of IT operations on all functional areas in the organization. Interorganizational level considers risks associated with organizations working in a networked environment. There are many potential risks

Fig. 13.1 Relationship between risk management components and levels in IT environment [1]



associated with every level, but data security risk is common to all of them. This framework considers four risk management components as the core of its functionality.

The primary objectives of this chapter include a comprehensive introduction to the concept of information technology risk management. It summarizes the existing information technology risk management frameworks and explains the information technology risk management life cycle, depicting all the phases. Further, it highlights special issues and challenges in information technology risk management. Finally, it outlines the emerging trends in information technology risk management.

The rest of the chapter is organized as follows: Sect. 13.2 sheds light on the existing IT risk management frameworks, their functions, and brief comparison. Section 13.3 introduces threat identification in IT risk management and is followed by vulnerability identification in Sect. 13.4. Section 13.5 puts forward the concept of risk assessment. It is followed by risk analysis and risk mitigation in Sects. 13.6 and 13.7, respectively. Section 13.8 discusses some special issues and challenges in IT risk management. Section 13.9 presents emerging trends and future research directions in IT risk management which is followed by the chapter summary.

13.2 IT Risk Management Frameworks

IT risk management is a very complex and multifaced activity based on four pillars of foundation: strategic goals, operations, financial reporting, and compliance with law and regulations. Every risk management model traverses these pillars in one way or the other. Contemporary risk management frameworks cater to the recent requirements of commercial and government organizations to group key activities into processes and control insider threats. This section introduces two prominent risk management frameworks and compares them to the integrated risk management framework at the end of this section.

13.2.1 NIST SP 800-30 Risk Framework

This framework constitutes of three risk management domains: risk assessment, risk mitigation, and risk evaluation and assessment [4]. Figure 13.2 presents these domains with extended functions performed by them.

13.2.1.1 Risk Assessment

Risk assessment methodology starts with system characterization to define the IT resources in the system. This involves identifying all the hardware, software, IT

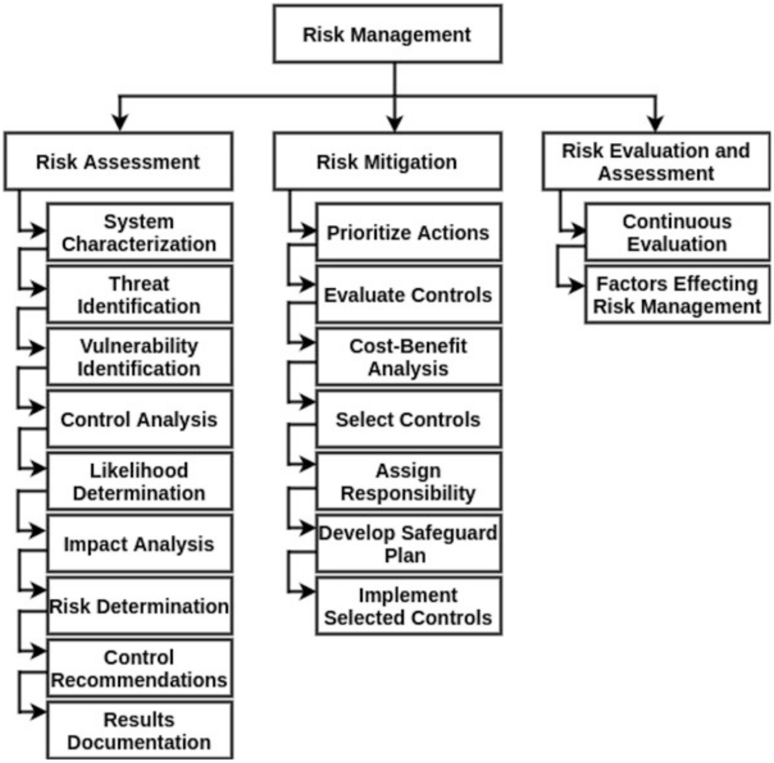


Fig. 13.2 Risk management framework by NIST SP 800-30

personnel, and network connectivity devices in the IT environment and delineating the system boundary. Once all the IT resources are compiled, risk assessment identifies potential internal and external threats. Common threat sources comprise natural calamities (earthquake, tornado, and hurricane, etc.), hackers, terrorists, malicious insiders, competitors, and rivals. At the end of threat identification, a threat statement is prepared that contains the potential threat sources which may exploit system vulnerabilities. Vulnerability identification is concerned with weaknesses or flaws in system security in terms of design, development, implementation, maintenance, or security procedures that could result in a data breach. This step develops a security requirements checklist highlighting the technical, operational, and management security controls that can be implemented to avoid a security breach. The controls highlighted in the previous step are used to mitigate the likelihood of exploiting a vulnerability. In the likelihood determination step, an overall likelihood rating (high, medium, and low) is assigned to each vulnerability that may be exercised.

The next major step in measuring the risk impacts analysis that takes as input confidentiality, integrity, and availability. It considers pros and cons of qualitative and quantitative assessment to measure the magnitude of impact (high, medium, and low). A risk matrix is created to measure the risk and then, controls are recommended to mitigate risk. Finally, at the end of risk assessment, a complete risk assessment report containing threats, vulnerabilities, risk measures, and recommendations for controls is submitted to management.

13.2.1.2 Risk Mitigation

Risk mitigation is the systematic strategy followed by the management to reduce the negative impact of risk. It begins with prioritizing the actions based on the risk assessment report and evaluating the recommended cost-effective controls. After performing the cost–benefit analysis, the management selects the cost-effective controls and assigns the most skilled personnel the responsibility to develop a safeguard implementation plan. Finally, based on implemented controls, calculated risk is reduced, but the residual risk remains.

13.2.1.3 Risk Evaluation and Assessment

The third domain of risk management framework is an ongoing process that continuously evaluates and assesses the risk factors that contribute to successful risk management.

13.2.2 Risk IT Framework by Information Systems Audit and Control Association (ISACA)

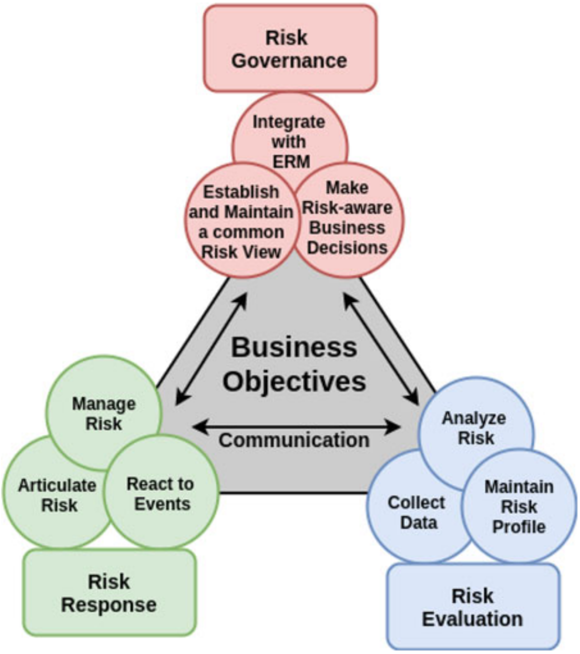
This is the most recent risk management framework that revolves around three domains: risk governance, risk evaluation, and risk response [5]. These domains are further grouped into three processes each as shown in Fig. 13.3.

13.2.2.1 Risk Governance

Risk governance integrates Enterprise Risk Management (ERM) program, helps to take risk-aware business decisions, and establishes a common risk view. It is centered at the following points:

- *Risk appetite and risk tolerance:* Risk appetite is the amount of risk an organization is ready to accept when trying to achieve its business objectives. It sets a threshold level for risk that the organization can absorb. Risk tolerance is the deviation from that threshold level.

Fig. 13.3 Risk IT framework by ISACA [5]



- *Responsibilities and accountability:* Risk management process involves several roles played by different people at different levels in the organizational structure. The role players take responsibilities and ensure that people who own the resources are accountable for the optimum usage of those resources.
- *Awareness and communication:* Risk awareness acknowledges that risk is an integral part of every business, and it needs to be communicated clearly to avoid a crisis.
- *Risk culture:* Risk culture introduces several behaviors such as taking a risk, following policies to mitigate risk, and ingesting the negative impact of risk.

13.2.2.2 Risk Evaluation

Risk evaluation incorporates three processes: collecting data to identify risks, analyzing risks by considering the relationship between business and risk factors, and maintaining risk profile by completing a risk inventory comprising of risk attributes such as resources, impact, and expected frequency. It concentrates on describing business impact in terms of prioritizing risks and creating risk scenarios to identify and analyze risks. Risk scenarios can be derived either in a top-down approach or in a bottom-up approach. The top-down approach begins with overall business objectives and moves toward specific business objectives down the tree. On the other hand, the bottom-up approach starts with generic scenarios and proceeds toward more concrete and customized scenarios applicable at the enterprise level.

13.2.2.3 Risk Response

Risk response includes the articulation of risk, managing risk, and reacting to risk events. Its primary goal is to identify risk indicators and prioritize risk response. Risk indicators measure the risk an organization is subject to or a risk that measures beyond the risk appetite. Every enterprise has unique risk indicators that depend on several internal and external environmental factors such as size and complexity of the enterprise. Risk response follows risk mitigation strategies, such as risk avoidance, reduction, transfer, and acceptance to prioritize response to a particular risk.

After understanding current risk frameworks in practice, Table 13.1 compares them with an integrated risk management framework. It is evident that the integrated framework is the primary risk management framework that focused on various feasible levels of communication. NIST SP 800-30 framework is a standard risk management framework adopted unanimously by the government and commercial sector, while ISACA's IT risk framework is the latest and structured framework that aligns with the COBIT framework for IT risk management.

In addition to these risk frameworks, International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC) 27005:2008 (E) [6] is another standard primarily designed for information security risk management in the IT environment. It consists of context establishment, risk assessment, risk treatment, risk acceptance, risk communication, and risk monitoring. The uniqueness of this standard lies in the fact that it follows an iterative approach to perform a risk assessment that minimizes the time and effort required to identify controls.

Table 13.1 Comparison of IT risk management frameworks

Attribute	Integrated	NIST SP 800-30	ISACA's framework
Core of framework	Three levels of communication	IT resources	Business objectives
Main domains	Risk identification, analysis, risk-reducing measures, and monitoring	Risk assessment, mitigation, and evaluation and assessment	Risk governance, evaluation, and response
Novelty	Basic risk framework that integrates risk at application, organizational and interorganizational levels	Fits well into Software Development Life Cycle (SDLC)	Structured framework that aligns with COBIT framework

A knowledge-based risk management framework for IT projects makes use of knowledge management processes to enhance and facilitate risk identification, analysis, response, and mitigation processes [7]. It is based on integral knowledge of risk modeling required to operate an IT system. In the first stage of the framework, system boundaries are characterized by capturing stakeholder's requirements. These requirements help in making decisions involving risks and profiling a complete IT system. In the second stage, the framework performs risk identification, analysis, response planning, and risk execution processes to utilize the knowledge base collected during the first stage to monitor and mitigate risks.

13.3 Threat Identification

Threat is the potential of a threat source to exploit a specific vulnerability, intentionally or unintentionally. Threats can be classified as internal or external. Internal threats include malicious insiders or humans who launch deliberate attacks, gain unauthorized access to data or perform intentional acts to compromise crucial systems. For example, a terminated employee logging illegitimately to alter payment records of the company. External threats encompass hackers, crackers, competitors, business rivals, and terrorists. An example of external threats is a cracker writing a Trojan Horse program to bypass the security for financial gain.

Threat identification is the process of finding all threats that may pose a danger to IT resources and compiling a threat statement listing all the found threats. As mentioned in NIST SP 800-30 risk management framework, a threat statement constitutes all the potential threats and threat sources that could exploit system vulnerabilities [4]. Every organization has a different threat statement that depends on the IT resources possessed by it. Moreover, known threats as identified by government and private sector organizations remain the same in every organization.

Threat statement can further be correlated with Common Attack Pattern Enumeration and Classification (CAPEC) database to determine how adversaries can exploit the weaknesses in applications by exercising potentially identified threats. CAPEC was established by the U.S. Department of Homeland Security in 2007. It contains an evolving list for identifying, collecting, sharing, and refining attack patterns.

Threat identification also plays a significant role in Business Continuity Planning (BCP) program, which involves assessing risks to organizational processes and creating policies and procedures to minimize the impact of those risks. BCP focuses on maintaining the continuity in business operations with reduced infrastructure, and threat statement lists the potential threats that may disrupt the business operations.

13.4 Vulnerability and Weaknesses Identification

Vulnerability is the weakness in design, implementation, and security procedures of a system, which when exploited by the potential threats, may result in a security breach or violation of security policy [4]. In the terminated employee example, if his login credentials are not deactivated or removed from the system after termination, it is considered a vulnerability that he can exploit by allegedly logging to the system. Every organization has different types of vulnerabilities depending upon the assets possessed by that organization. Apparently, a different vulnerability identification system is needed to tackle those vulnerabilities.

In a typical threat, vulnerability, and risk life cycle, as shown in Fig. 13.4, a threat exploits a vulnerability that poses risks to an organization. These risks can be combatted by planning and deploying safeguards that protect IT resources and assets that are prone to threats [4]. It is pertinent to mention that organizational assets are not limited to IT resources, but they cover all other resources that the organization relies on for its functioning.

Vulnerability identification process formally analyzes the IT system, security features, and technical, administrative, and operational controls used to protect the system. At the end of this analysis, a list of technical and non-technical system vulnerabilities associated with the IT environment is compiled that could be exploited by the potential threat sources identified in the previous section. Vulnerability identification uses vulnerability sources, security requirements checklist, and system security testing as the primary means of collecting vulnerability information.

13.4.1 Vulnerability Sources

Several techniques such as questionnaires, on-site interviews, policy, and security document review, and automated scanning tools are used to gather information.

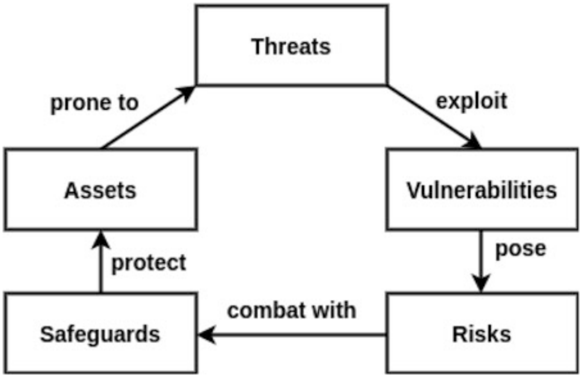


Fig. 13.4 Threat, vulnerability, and risk life cycle

These techniques help characterize the IT system. Following additional vulnerability sources can be explored to identify vulnerabilities related to an organization:

- National Vulnerability Database (NVD) that consists of lists of vulnerabilities and their description.
- Common Vulnerabilities and Exposures (CVE) for identifying publicly available known information security vulnerabilities. CVE is a unique identifier for one vulnerability and provides a standard description for that vulnerability. Every vulnerability is assigned a Common Vulnerability Scoring System (CVSS) score that determines the severity of that vulnerability.
- Common Weakness Enumeration (CWE) for a software or hardware. CWE is community developed.
- Previous IT risk assessment document, audit reports, system anomaly reports, system test, and evaluation reports.
- Vendor advisories.
- Information Assurance and Vulnerability Alert (IAVA) for military systems.
- Information from Computer Emergency Response Team (CERT) to identify a vulnerability and procedure to exploit and fix a vulnerability.
- Data breach databases.

13.4.2 Security Requirements Checklist

A security requirements checklist contains the basic security standards to identify and evaluate the vulnerabilities in IT assets by classifying it into three areas: management, operational, and technical [4]. Management security includes assigning responsibilities, separation of duties, technical training, mandatory vacations, dual control, incident response capabilities, risk assessment plan, authorization, and authentication. Operational security consists of temperature and humidity control, working equipment, electrical and mechanical devices, and storage media. Technical security comprises data protection schemes, intrusion detection, security audits, and communication devices. The outcomes of security requirements checklist are used as input to evaluate compliance and noncompliance to security policies and procedures. A comprehensive checklist provides a clear distinction between different types of system, process, and procedural vulnerabilities that exist in an IT environment.

13.4.3 System Security Testing

System security testing encompasses two types of testing measures: penetration testing and automated vulnerability scanning tools. Penetration testing is a complete process in which a third party is granted permission to identify and exploit system vulnerabilities and provide a detailed report on what vulnerabilities exist in the system and how they can be exploited. It helps the organization to detect potential failures in the protection mechanisms deployed in the IT system.

Automated vulnerability scanning tools such as Nessus, QualysGuard, and OpenVAS can be used by the security professionals to identify specific vulnerabilities on chosen systems and ports. These tools provide a brief description, CVE number, and CVSS score related to the vulnerability and suggest the remediation to mitigate it. Vulnerability scanning tools scan the ports for specific vulnerabilities, common misconfigurations, compliance to organizational policies and procedures, and default password usage.

13.5 Risk Assessment

Risk assessment is the first step in the risk management process. It estimates the risks associated with IT system by identifying potential threats and vulnerabilities, determining the likelihood of occurrence of threats, and estimating its impact on the IT system. It is primarily exercised by the upper management to identify the risks that can be mitigated [8]. The risk assessment methodology is quantitative or qualitative in nature. Quantitative risk assessment estimates the real-time monetary loss associated with risks. On the contrary, qualitative risk assessment is subjective and assigns intangible value to the loss of assets. Both methodologies contribute to the effective risk assessment to obtain a balanced view of security concerns. After obtaining the list of system vulnerabilities and threats, risk assessment analyzes the planned security controls that are in use by the IT system or can be used to mitigate the likelihood of a vulnerability being exploited by a threat source and minimize the impact of such an event.

13.5.1 Likelihood and Impact Determination

Likelihood can be described as high, medium, or low depending upon the motivation of the threat-source, nature of the vulnerability, and effective controls in place. A likelihood rating indicates the probability that a vulnerability may be exercised in the IT environment.

Impact analysis is performed to ascertain the magnitude of impact as high, medium, or low. It considers sensitivity and criticality of data to ensure that confidentiality, integrity, and availability of data are not tampered with. Impact analysis can be performed quantitatively and qualitatively. Tangible impacts can be measured quantitatively, while intangible impacts need to be analyzed qualitatively. For example, the cost of repairing a system is tangible and can be measured in real-time monetary value. On the other hand, loss of reputation owing to financial or critical data leakage is intangible and can be expressed qualitatively. Both

Table 13.2 An example risk matrix

Likelihood	Impact		
	Low	Medium	High
High	Low	Medium	High
Medium	Low	Medium	Medium
Low	Low	Low	Low

methodologies have their pros and cons. None of them is considered better over the other.

13.5.2 Risk Determination

The main objective of risk determination is to assess the level of risk associated with the IT system. It can be expressed as a function of likelihood, magnitude of impact, and suitability of planned or existing security controls [4]. A risk matrix is created to plot the likelihood of a threat and its magnitude of impact. An example risk matrix is shown in Table 13.2.

Based on Table 13.2, if the likelihood of occurrence of a threat is high, and the magnitude of the impact is low, the risk level to the IT system is considered low. Similarly, if both the likelihood and the impact are high, then the risk level is high. Risk matrix facilitates the upper management to prioritize risks and take the following appropriate actions based on the level of risk:

- If the risk is reported as high, the management needs to take a decision regarding the additional corrective measures that need to be in place as soon as possible to remediate the situation.
- If the risk is reported as a medium, the management needs corrective actions within a stipulated time.
- If the risk is reported as low, the management needs to discuss whether corrective actions are still needed or not.

Once the risk assessment is completed, a detailed document is prepared that describes the threats and vulnerabilities, the likelihood of threats and magnitude of vulnerabilities, and risk matrix to determine the corrective actions needed to mitigate the risk.

13.6 Risk Analysis

A well-documented risk analysis helps to estimate cost–benefit measures, suggest improvements in financial analyses, and plan for better security measures [9]. Risk analysis can be performed in a quantitative or qualitative manner. Quantitative risk analysis includes numerals to compute a real-time cost–benefit value, while the qualitative risk analysis provides a subjective value to assets under question.

13.6.1 Quantitative Risk Analysis

The process of quantitative risk analysis starts with asset valuation and proceeds with computing the frequency of risk and exposure that it will have on the IT system. The following parameters are essential to calculate quantitative risk analysis:

- **Asset Value (AV):** AV computes the valuation of asset and its importance in the functioning of the IT system.
- **Exposure Factor (EF):** EF estimates the percentage of loss that the organization will have to bear in case an asset is lost or becomes unavailable due to risk.
- **Single Loss Expectancy (SLE):** SLE is the cost associated with a single risk against a specific asset. It is mathematically represented as:

$$\mathbf{SLE} = \mathbf{AV}^{*}\,\mathbf{EF}$$

- **Annualized Rate of Occurrence (ARO):** ARO is the expected frequency of occurrence of a risk in a single year.
- **Annualized Loss Expectancy (ALE):** ALE is the total annual loss incurred due to a specific risk against a specific asset. It is computed as:

$$\mathbf{ALE} = \mathbf{SLE}^{*}\,\mathbf{ARO}$$

Let us consider an example to compute the risk associated with a particular situation. The National Weather Service warns of a hurricane that may harm the $10 million headquarter building of a company. The detailed warning mentions that the hurricane will strike once a year, and there is a 10% probability that the hurricane will harm the company building. Based on these data, let us compute the annualized loss of expectancy.

From the given information, AV = $10 million, EF = 10%, and ARO = once a year = 1.

Therefore, SLE = AV * EF

$$\mathrm{SLE} = (10,000,000)\ ^{*}\ (10\%)$$

$$\mathrm{SLE} = 10,000,000^{*}\,10/100$$

$$\mathrm{SLE} = 1,000,000$$

Further, ALE = SLE * ARO

$$\mathrm{ALE} = 1,000,000\,{}^{*}\,1$$

$$\mathrm{ALE} = 1,000,000$$

Hence, the annual loss expectancy is $1 million, which is the same as single loss expectancy in this case because the hurricane is expected once in a year.

Based on the quantitative risk analysis, the computed values are used for calculating cost–benefit analysis and prioritizing and selecting risks. Based on the computed value of ALE, cost–benefit analysis can be performed using the following mathematical formula:

$$\begin{aligned}\textbf{Safeguard cost/benefit analysis} &= (\mathbf{ALE}_{\mathbf{before}}) - (\mathbf{ALE}_{\mathbf{after}})\\ &\quad - (\textbf{annual cost of safeguard}),\end{aligned}$$

where $\mathrm{ALE}_{\mathrm{before}}$ and $\mathrm{ALE}_{\mathrm{after}}$ present ALE before and after implementing the safeguard, respectively.

This value represents the value of safeguard to the company. However, these computations represent estimated values and may not reflect real-time losses which is the drawback of this methodology. SANS institute's information reading room provides a deep understanding of a step-by-step quantitative risk analysis [9].

13.6.2 Qualitative Risk Analysis

Qualitative risk analysis is based on ranking the assets rather than assigning mathematical values of risks, losses, and costs. Several techniques are used to perform qualitative analysis, including brainstorming, Delphi technique, surveys, questionnaires, checklists, interviews, and meetings. However, Delphi technique is a standard and most preferred technique used for qualitative analysis. It is an anonymous feedback process used to make anonymous consensus. In this technique, the participants write their feedback or response on a piece of paper and submit it in a single meeting room.

Both quantitative and qualitative analyses offer useful results. The quantitative analysis provides a complex, mathematical, and real-time cost–benefit analysis approach. On the contrary, qualitative analysis involves guesswork, but the results are equally informative.

13.7 Risk Mitigation and Monitoring

After assessing, prioritizing, and analyzing risk in previous sections, this section presents the risk mitigation and monitoring strategies. Risk mitigation deals with the following risk-reducing measures to minimize its impact on IT system:

- **Accept:** The IT system is aware of the risk and accepts it to continue functioning. The potential loss from an accepted risk is bearable.
- **Avoid:** Risk is avoided by eliminating its cause and consequences. Shutting down a system and isolating it in case of a targeted attack is an example of avoiding risk.
- **Transfer:** Transferring the risk to a third party such as insurance company to compensate for the potential losses incurred due to it.
- **Deter:** Risk is reduced by implementing the corrective or preventive controls designed to minimize its adverse impact.
- **Reject:** The final option is to reject the risk and continue functioning as if nothing has happened.

The amount of risk remaining after performing any of the abovementioned risk-reducing measures is called residual risk. No IT system is risk free, and none of the risk mitigation strategies can eliminate the risk completely. The challenge for the IT administration is to reduce the residual risk to an acceptable level.

Risk monitoring includes continuous monitoring of risk management activities. It helps to establish the effectiveness of the risk management process and risk controls and identify the loopholes in the existing risk management process [10]. Risk monitoring serves the following purposes: (1) review the risk management process, (2) assess the effectiveness of risk mitigation strategies, (3) identify new risks and their sources, and (4) ensure the proper functioning of corrective controls [7]. Risk monitoring takes place throughout the life cycle of an IT project to record any changes to the risk profile. The IT project managers must use data analysis tools, audits, and meetings to effectively implement risk response controls [11]. Further, the IT project team must ensure that the risk evaluation and updating is a part of every meeting progress report [12]. It must be open to face unforeseen risks.

13.8 Special Issues and Challenges in IT Risk Management

Risk management, in general, faces data breaches and business continuity as the primary risks. In addition to these general risk management issues, IT risk management deals with specific issues and challenges mentioned below:

(a) **Changing technology:** With the evolving technology such as data capturing, correlating, and analysis tools, the issues related to the integration of massive data captured by different vendor-specific tools are escalating. Correlating and analyzing such a huge volume of diverse data are critical challenge for effective IT risk management.

(b) **Recruiting the right people with the right talent, good work ethics:** Finding the right and expertise, IT risk professionals for dealing with IT risks is another issue. With plenty of workforces available, it is pertinent to identify the right people with the right talent to mitigate all risk levels.

(c) **Compliance to IT risk standards:** One of the imperative steps in IT risk management is to create an effective risk management strategy to comply with the IT risk standards and policies designed by the organization. Some of the IT compliance regulations include Control Objectives for Information and Related Technology (COBIT), ISO 27001/27002/27005, and Sarbanes-Oxley (SOX). With the changing digital transformations and voluminous data, compliance with IT risks standards has become more difficult. Complying to the multitude of regulations is a critical security concern for IT professionals, but rapid digital transformations make it hard to mitigate risks.

(d) **Correct risk assessment and prioritization:** Early and regular risk assessment is the key to evaluate residual and unforeseen IT risks. It helps to prioritize risks and apply corrective controls to mitigate risks that may result in potential business losses. However, timely evaluation is necessary to detect critical vulnerabilities and threats so that appropriate mitigation strategy can be applied to reduce the risk before it wreaks havoc.

(e) **Involvement of stakeholders:** Most of the available IT risk standards do not involve stakeholders in the risk management process except the knowledge-based risk management framework [7] that is mainly focused on including stakeholders' requirements in the risk-based decision-making process. Inculcating stakeholder's requirements facilitate building a risk profile for an IT system which helps in taking the right decisions at the right time.

(f) **Getting the managers to understand the risk:** It is imperative that managers understand the risk because the consequences of a risk are directly related to organization's budget to overcome it. Therefore, IT risk management team must foresee the ramifications of risk and plan risk management program in advance to reduce the negative impact of risk.

13.9 Emerging Trends and Research Directions

IT risk landscape is changing at a rapid pace. New opportunities and technologies also bring new challenges to IT risk management. Several emerging IT risk management trends are observed over the years, such as the use of cognitive technologies to facilitate decision-making, behavioral sciences to determine risk insights, focus on emerging risks, and increased social networking.

- **Artificial intelligence in IT risk management:** Artificial intelligence (AI) is widely used in financial institutions for identifying frauds and managing risks.

Due to the growing financial crisis in the previous decade, IT professionals are inclined to the use of cognitive technologies, especially in the banking sector, to analyze customer behavior and prevent financial frauds in advance. These systems generate a huge amount of customer's behavior data that can be used to understand behavioral trends. Advancements in such technologies help the IT system to automatically identify and mitigate the risks.

- **Behavioral sciences to improve decision making:** Behavioral analytics is used to understand, observe, and analyze the potential risks in the IT system. Data-capturing tools collect a tremendous amount of data that can be correlated, and behavioral sciences can be used to study these data and use the analyses to make decisions. Moreover, cognitive technology is also incorporated into business to take competitive advantage and identify risks in a timely manner.
- **Focus on emerging risks:** With the unprecedented upsurge in cyberattacks, IT system has witnessed unforeseen risks in the recent years. These risks have inspired the IT professionals to develop preventive controls that can foresee the espionage and threats that an enterprise is vulnerable to. These risks are difficult to quantify and may have high potential. Focus on emerging risks highlights the importance of using trend analysis or behavior analysis techniques to predict the occurrence of potential risks.
- **Impact of increased social networking:** Social networking has become an inseparable part of doing business in the contemporary era. However, it poses severe risks to the IT system through some common methods such as phishing, social engineering, unauthorized access, and use of weak passwords, to name a few. The users need to be aware of cyber policies at the organizational level and attacks that can easily target the IT systems to protect themselves from the side effects of social networking.

Based on the recent emerging trends observed in IT risk management, researchers can further examine the following aspects:

- **Degree of awareness:** Lack of risk awareness among managers is still an open challenge as well as a future direction for IT risk management. Developing a greater degree of awareness among IT risk managers can help them to foresee advanced risks and take appropriate risk-reducing measures.
- **Selection of right risk parameters:** Since the structure and taxonomy of modern risks is different from earlier IT risks, it is important to select important parameters that can be used to quantitatively analyze risk. This selection can be complemented with a machine learning technique-based quantitative risk management approach.
- **Selection of right risk management model:** Existing IT risk management models use qualitative (using questionnaires and surveys [13]) and quantitative (using mean-variance computations and fuzzy logic [14]) risk analysis approach. These models are limited to a specific industry and organizational culture. Thus, they cannot be applied to another industry of different organization size, culture, and auditing system.

13.10 Summary

Information technology risk management is a multifunctional application of risk management to manage IT risks by identifying potential threats and vulnerabilities, assessing and analyzing risks, and preparing risk response strategies to mitigate risks at an acceptable level. The core of an IT risk management framework comprises several risk governances that document the list of IT assets. The objective of IT risk management is to protect IT assets from potentially known and new risks emerging every day. IT risk managers use qualitative and quantitative risk analysis methods to compute and predict real-time losses that may incur in case a vulnerability is exercised. Emerging IT risks pose severe challenges to the IT systems that can be catered with emerging technological and behavioral analysis trends. There are instances when IT risk managers inculcated artificial intelligence and machine learning techniques to improvise the decision-making process. With rapidly surging sophisticated risks, it is pertinent to make use of cognitive approach to automatically analyze the impact of risks.

References

1. Crane, C. (2020). *The definitive cyber security statistics guide for 2020*. Security Boulevard. Retrieved October 2020, from https://securityboulevard.com/2020/05/the-definitive-cyber-security-statistics-guide-for-2020/
2. *2019 Internet Crime Report, Federal Bureau of Investigation/Internet Crime Complaint Center*. (2019). Retrieved October 2020, from https://pdf.ic3.gov/2019_IC3Report.pdf
3. Bandyopadhyay, K., Mykytyn, P. P., & Mykytyn, K. (1999). A framework for integrated risk management in information technology. *Management Decision, 37*(5), 437–444.
4. Stoneburner, G., Goguen, A., & Feringa, A. (2002). Risk management guide for information technology systems. *NIST SP*, 800–830.
5. *The risk IT framework*. (2009). ISACA. Retrieved October 2020, from https://www.hci-itil.com/ITIL_v3/docs/RiskIT_FW_30June2010_Research.pdf
6. *Information technology—Security techniques—Information security risk management*. ISO/IEC 27005 (1st ed.). Retrieved October 2020, from https://www.sis.se/api/document/preview/909897/
7. Alhawari, S., Karadsheh, L., Talet, A. N., & Mansour, E. (2012). Knowledge-based risk management framework for information technology project. *International Journal of Information Management, 32*, 50–65.
8. Chapple, M., Stewart, J. M., & Gibson, D. (2018). *Certified information systems security professional official study guide* (8th ed.). (ISC)^2, Sybex, A Wiley Brand.
9. Tan, D. (2002). *Quantitative risk analysis step-by-step*. Information Security Reading Room, SANS Institute. Retrieved October 2020, from https://www.sans.org/reading-room/whitepapers/auditing/quantitative-risk-analysis-step-by-step-849
10. Teneyuca, D. (2001). Organizational leader's use of risk management for information technology. *Information Security Technical Report, 6*(3), 54–59.
11. *A guide to the project management body of knowledge*. (2017). 6th ed. Newtown Square, PA: Project Management Institute.
12. Larson, E. W., Honig, B., Gray, C. F., Dantin, U., & Baccarini, D. (2014). *Project Management: The managerial process*. McGraw-Hill Education.

13. Saeidi, P., Saeidi, S. P., Sofian, S., Saeidi, S. P., Nilashi, M., & Mardani, A. (2019). The impact of enterprise risk management on competitive advantage by moderating role of information technology. *Computer Standards & Interfaces, 63*, 67–82.
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.