Context-Based and Adaptive Cybersecurity Risk Management Framework

Subjects: Computer Science, Cybernetics

Contributor: Henock Mulugeta Melaku

Organizations are faced with a variety of cyber-threats and are possibly challenged by a wide range of cyber-attacks of varying frequency, complexity, and impact. However, they can do something to prevent, or at least mitigate, these cyber-attacks by first understanding and addressing their common problems regarding cybersecurity culture, developing a cyber-risk management plan, and devising a more proactive and collaborative approach that is suitable according to their organization context.

cyber-risk risk assessment risk impact likelihood rating performance metrics

1. Enterprise, IT, and Cybersecurity Risk Management Frameworks

To explore and manage cybersecurity risks, identifying security attacks and vulnerabilities is paramount to seeing the cyber-risk imposed on an organization. Therefore, appropriate security investment will be made for the risk mitigation decisions. Many cybersecurity risk management frameworks provide standards to identify and mitigate cyber-related risks. The main reasons for having risk management frameworks are that they make it easier for an organization to define the appropriate security-related processes and procedures that are needed to assess, monitor, and mitigate cyber-risks; these frameworks are also used to assess, evaluate, and improve the security status of a company. On the basis of the above useful comprehension, many frameworks, policies, and standards have been developed that help organizations understand their cyber-risk.

1.1. Enterprise Risk Management Frameworks

1.1.1. ISO 31000—Risk Management

ISO 31000:2009 delivers values, principles, and risk management guidelines and standards (Tranchard 2018). ISO 31000:2009, Risk Management—“Principles and Guidelines” offers a framework, process, and principles for managing enterprise risk. Any type and size of organization can use the framework. Organizations that use ISO 31000 can accomplish their objectives, increase the probability of identifying threats and opportunities, and enhance the optimal allocation of budget and resources for risk management.

Moreover, it gives complete and actionable steps to deal with internal and external audit programs. In addition, if an organization implements the ISO 31000 framework, it can easily compare its security posture with other recognized

standards and best practices.

As shown in **Figure 1**, ISO 31000:2009 has different risk assessment, evaluation, and treatment phases. Using this framework, organizations can manage their business risk systematically, minimize or accept the risk, identify and remove the root cause of the risk, reduce the likelihood and impact of the risk, contain the risk by following well-versed decisions, and share or transfer the risk to other companies (Tranchard 2018; Rampini et al. 2019).

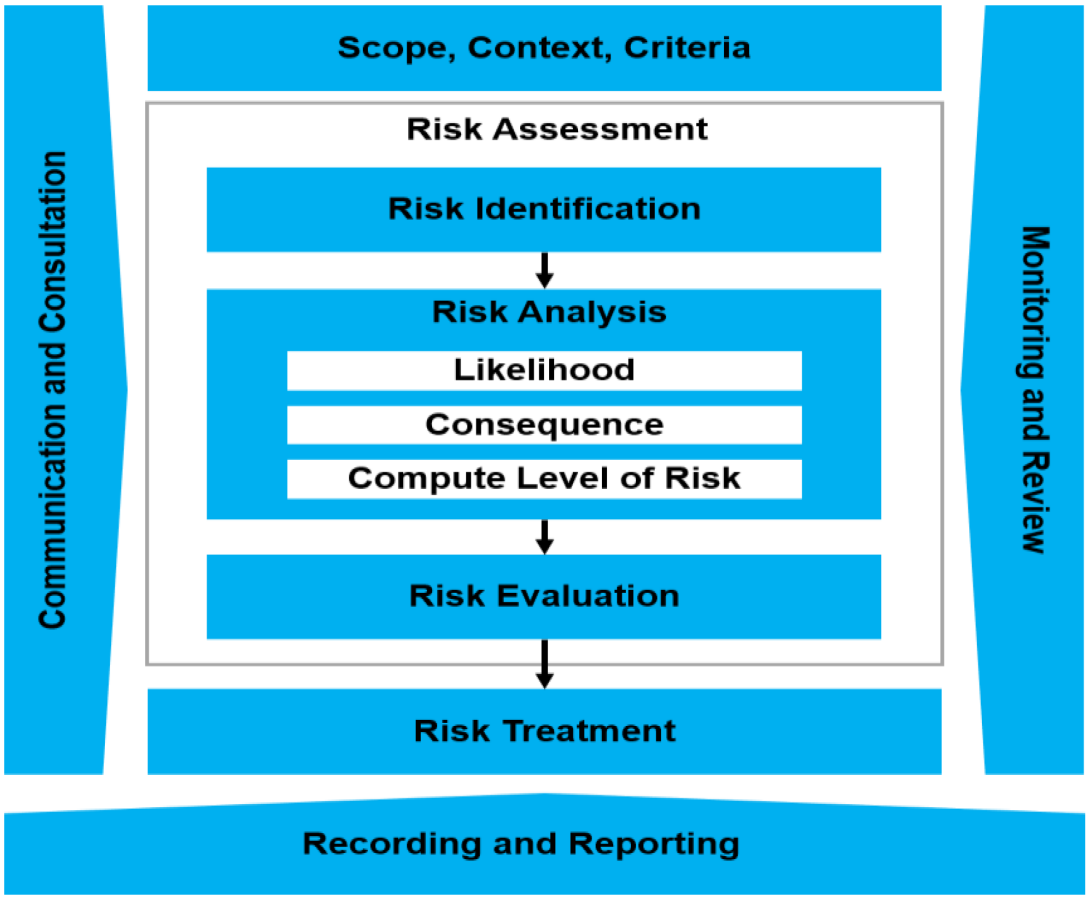

Figure 1. ISO 31000 Enterprise Risk Management Frameworks (ISO31000:2018 Risk Management Process).

1.1.2. Enterprise Risk Management (ERM)—Integrated Framework

This framework was developed by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) (Rampini et al. 2019; Shad et al. 2019). COSO released this framework in 2004. The framework discusses core principles, processes, and components. It provides guidelines and procedures to manage enterprise risks. It also offers a comprehensive method to manage enterprise risks according to an organization's risk appetite and tolerance. As shown in **Figure 2**, the framework has five main components to handle enterprise risks: risk assessment, control environment, control activities, monitoring, and information and communication (Shad et al. 2019).

Figure 2. COSO Enterprise Risk Management Framework.

The above two risk management frameworks are mainly used for addressing the issue of general enterprise-level risks. They do not consider IT and security-related risk management frameworks, processes, or programs.

1.2. IT Risk Management Framework

1.2.1. The Risk IT Framework from ISACA—ISACA (Information Systems Audit and Control Association)

The Risk IT Framework is meant to identify and fill the gap between enterprise and IT risk management processes. It also provides guidelines and standards to manage security risks (Kaur and Lashkari 2021). It is an end-to-end approach that makes it suitable to see IT risks holistically. It also includes risk mitigation options. The framework

allows organizations to comprehend and manage IT-related risks. Moreover, it builds upon ISACA's most widely used IT risk management frameworks (i.e., COBIT and Val IT). **Figure 3** shows a high-level risk management framework proposed from ISACA (Kaur and Lashkari 2021).

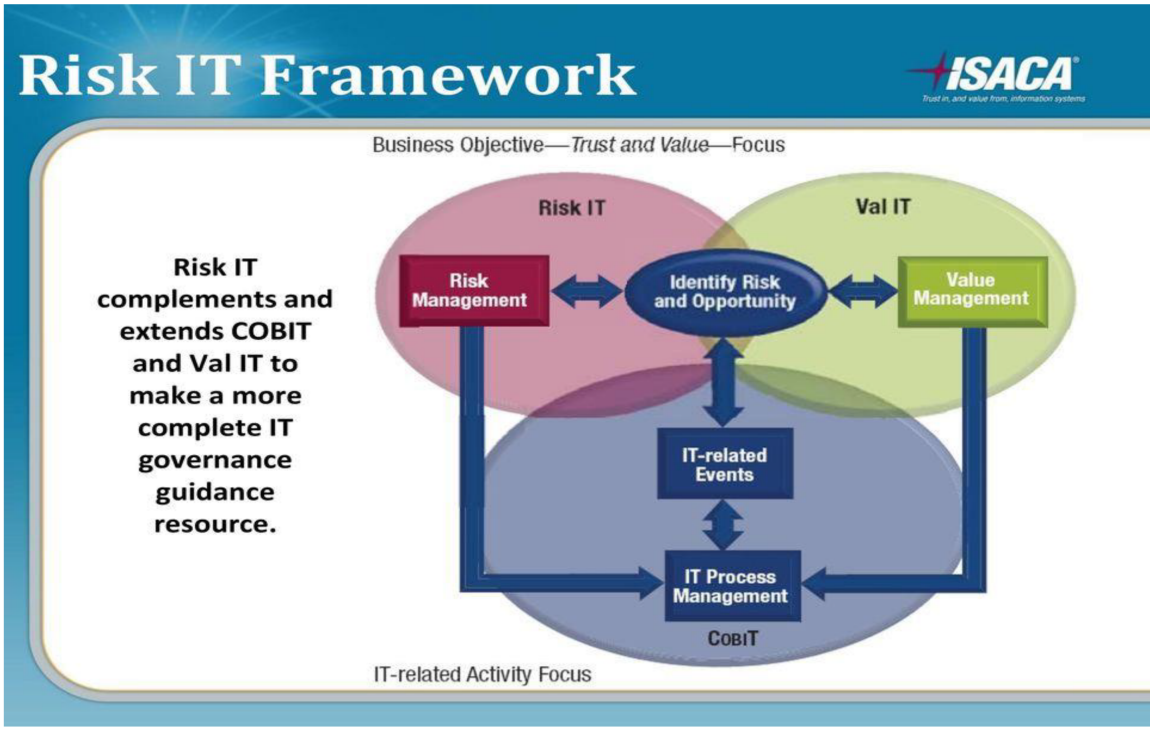

Figure 3. The Risk IT Framework from ISACA.

1.2.2. The IT Infrastructure Library (ITIL) Framework

As shown in **Figure 4**, the ITIL risk management framework comprises the following core processes: threat identification, vulnerability assessment, probability and impact analysis, determination of the risk, and continuous monitoring of the risk (Wang et al. 2022).

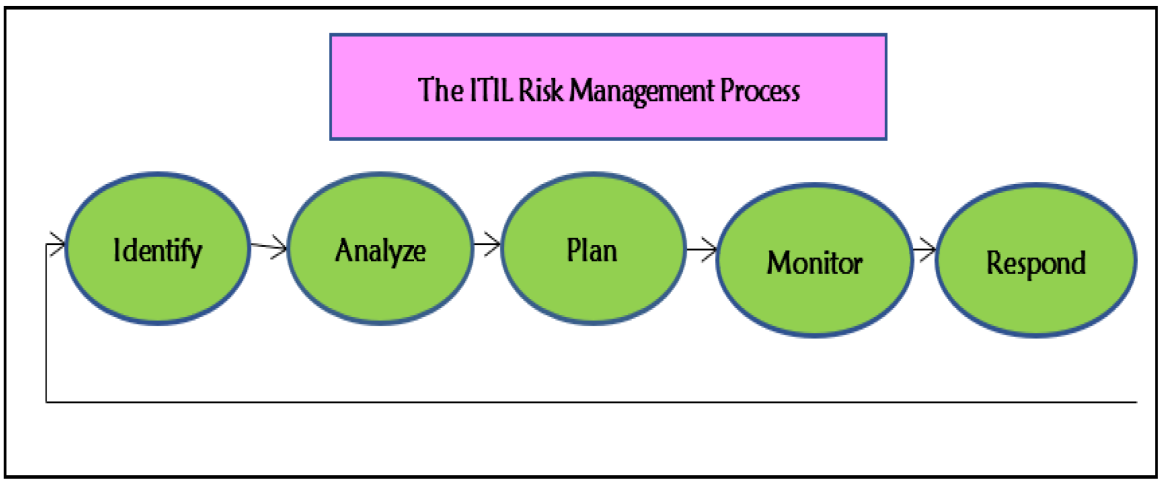

Figure 4. The IT Infrastructure Library (ITIL).

1.2.3. Control Objectives for Information and Related Technology (COBIT 5)

As shown in **Figure 5**, the IT Governance Institute issued the COBIT 5 framework, which incorporates COBIT 5.0, Risk IT, IT Assurance Framework (ITAF), Val IT 2.0, and Business Model for Information Security (BMIS) (Al-Fatlawi et al. 2021). There are two mechanisms used in COBIT 5. *Risk function*—defines well-structured risk governance and management techniques to effectively manage IT risks. *Risk management*—provides different phases to manage IT risks, such as identifying, analyzing, responding, and reporting risk (Al-Fatlawi et al. 2021).

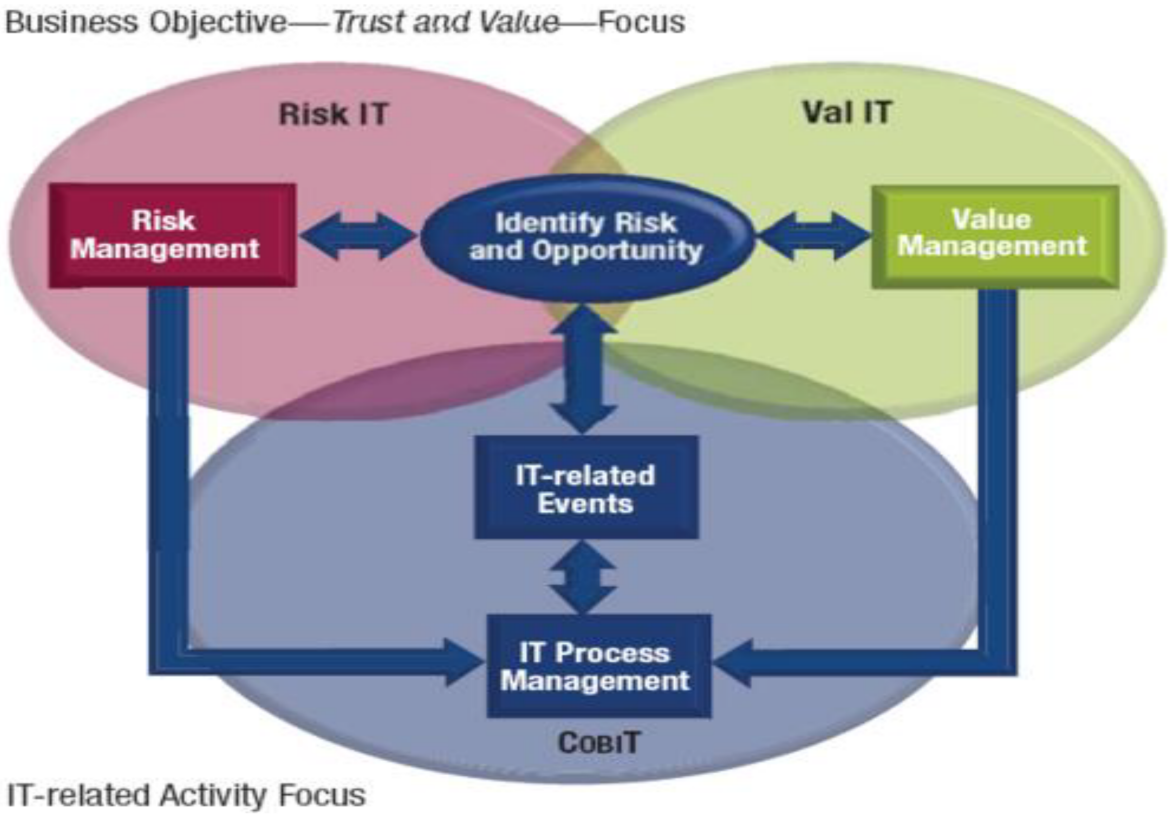

Figure 5. COBIT 5 IT Risk Management Framework.

1.3. Cybersecurity Risk Management Frameworks (CRMFs)

Different types of CRMFs have been developed to manage security risks. These CRMFs provide standards and processes to identify, analyze, and mitigate security risks (Lee 2021).

The literature points out that the reason for using cybersecurity RMFs is that they make it easier for organizations to devise suitable processes and procedures that are needed to *assess*, *analyze*, *monitor*, and *mitigate* risks; to define an appropriate set of security processes, policies, and guidelines to address the identified risks; and to measure and enhance the security posture of an organization. In light of the above facts, different cybersecurity risk management frameworks can help an organization evaluate the strength of the security controls they

implement. The currently available cybersecurity risk management frameworks tend to have a combination of security and compliance requirements (Goel et al. 2020).

Compliance-based requirements focus on protecting specific data or information. Some of the common compliance-based frameworks are GDPR HIPAA, PCI-DSS, HITRUST, SOC, and FISMA. At the same time, security-focused requirements are based on the organization's environment. NIST and ISO are examples among the many cybersecurity risk management frameworks proposed so far (Sulistyowati et al. 2020).

1.3.1. NIST Cybersecurity Framework

The National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) is one of the most prevalent frameworks in the industry (Gordon et al. 2020). The NIST CSF is a framework that can help companies to manage and mitigate cybersecurity risk in a standard way. As shown in **Figure 6**, the framework provides five essential and comprehensible functions—identify, protect, detect, respond, and recover—to manage cyber-related risks. It has a technique for mapping between each activity and outcome. NIST is responsible for developing standards, guidelines, and related methods and procedures for delivering adequate cybersecurity.

Figure 6. NIST cybersecurity framework.

As shown in **Figure 7**, risk within the first pillar (Identify), security risk assessment procedures, and guidelines are presented. More specifically, the framework recommends companies take the following steps to identify and analyze risks: identify and document asset vulnerability; acquire up-to-date threat intelligence and identify and document both internal and external threats; identify possible corporate impacts and probabilities of the security risks; make use of threat, vulnerability, probability, and effect to determine the risks; and finally identify and prioritize risk responses.

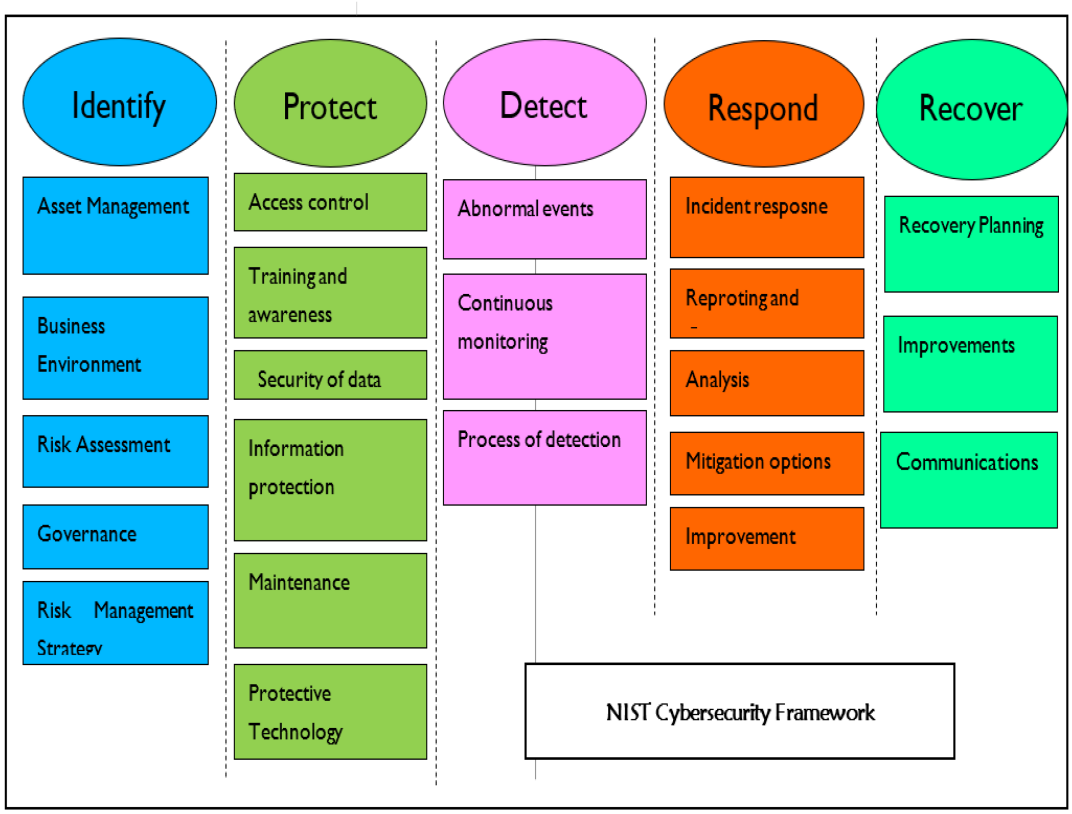

Figure 7. NIST Cybersecurity Framework.

1.3.2. NIST Cybersecurity Risk Management Framework

NIST SP-800-37 is one of the most commonly used risk management frameworks by organizations. As shown in **Figure 7**, the NIST Cybersecurity RMF comprises six phases. Each phase comprises different processes to manage cybersecurity risks (McCarthy and Harnett 2014; Almuhammadi and Alsaleh 2017). The NIST RMF provides an all-inclusive, flexible, and repeatable seven-step process to manage security and privacy risks, and relates to a set of NIST standards and guidelines to be applied for risk management programs. In this way, it is possible to meet the requirements of FISMA. FISMA gives direction on the importance of risk management compliance with appropriate laws and regulations, executive orders, directives, etc. The NIST Special Publication 800-37 (Revision 2) is a cybersecurity RMF with a standard process for implementing, monitoring, and evaluating cyber-risks (McCarthy and Harnett 2014). Although the NIST RMF was created by the US Department of Defense

(DoD), it provides a worthy reference framework for security and privacy programs that any type and size of organization can use. The NIST RMF comprises seven steps, as shown in **Figure 8** below.

Figure 8. The NIST Cybersecurity risk management framework.

1.3.3. ISO/IEC 27005:2018 Risk Management Framework

This provides a well-defined set of standards and guidelines to systematically manage risks for an organization. It also supports the general concepts that are specified in ISO 27001. ISO 27005 outlines five major pillars that are needed for the management of cybersecurity risk and seven steps that must be followed to perform a risk assessment. These five major pillars are threat identification, vulnerability assessment, risk analysis, risk mitigation, and defining security outcomes (Diamantopoulou et al. 2020). To make it more comprehensive, the ISO 2005 risk management framework comprises five processes: context understanding, analysis of risk, treatment of risk, the suggestion of risk acceptance methods, and monitoring and review of the risk.

1.3.4. OCTAVE

This is a security risk management framework that is composed of the identification, management, and evaluation of security risks. As shown in **Figure 9**, the OCTAVE framework helps an organization to identify assets, identify

security threats and system vulnerabilities, determine the likelihood, analyze the impact, and determine the risk that an organization is willing to accept the risk and pledge constant development activities to mitigate risks (Hom et al. 2020).

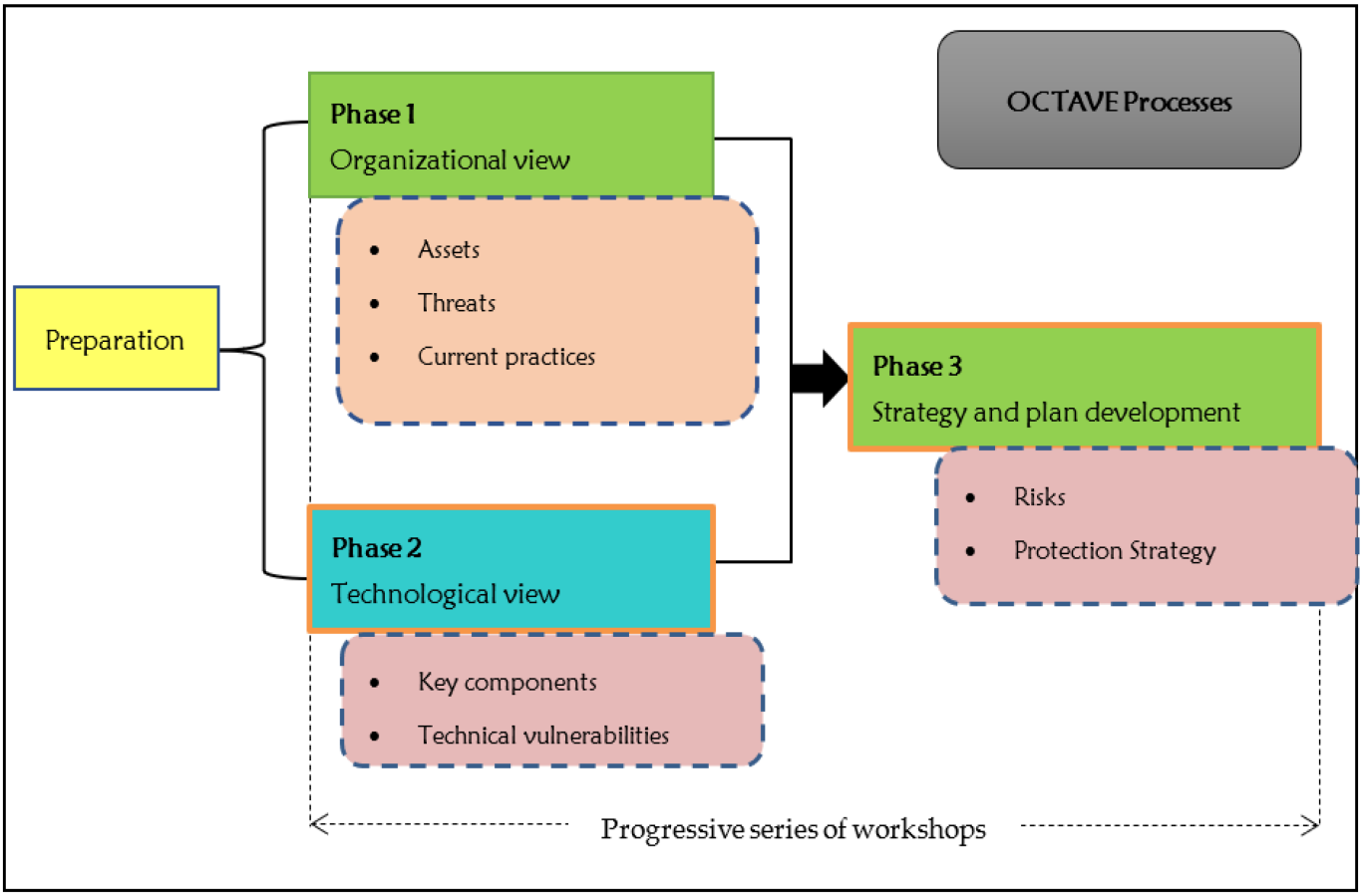

Figure 9. OCTAVE information security risk management framework (Hom et al. 2020).

1.4. Comparison of the Risk Management Frameworks

To compare and analyze the various risk management frameworks, different parameters, such as risk assessment, risk analysis, risk mitigation, cost and ease of implementation, compatibility, and other parameters, are considered (**Table 1** and **Table 2**). According to the analysis made in **Table 1**, the NIST framework is highly likely to be used by any organization that needs tactical-level risk management due to compatibility and ease of availability and use. It was also developed to be consistent with ISO/IEC standards, allowing for simple integration with pre-existing management systems. It is also freely available and accessible from NIST's website for organizations to implement. It has clear, concise, and controlled instructions that enable it to be used alongside other risk assessment toolkits for a multi-faceted approach. However, some of the limitations of the NIST framework are that, since it is based in the USA, most of the documentation is heavily focused on US regulations and legislation.

Table 1. Comparison of different cybersecurity risk management frameworks.

Parameters	NIST	ISO 27005	OCTAVE	COSO	ITIL	COBiT 5	ISO 31000
Risk assessment	√	√	√	√	√	√	√
Risk analysis	√	√	√	×	√	√	√
Risk mitigation	√	√	√	×	√	√	√
Approach	Tactical approach	High-level approach	High-level approach	High-level control capabilities	Holistic approach: customer-focused	Holistic approach	A comprehensive and practice-based approach
Cost	Low cost: free access	High: paid access	Very low cost	Low cost	Higher cost	Free and medium cost	High cost
Implementation	Easy	Easy	Easy	Complex	Complex	Complex	Easy
Compatibility	Any type and size of the organization	Any type and size of the organization	Large organization	Large organization	Any size and type of organization	Simple to complex organizations	Any size and type of organization
Focus area	Tactical-level RM	Holistic RM	Strategic RM	Enterprise RM	End-to-end RM	End-to-end RM	End-to-end RM
Organizational perspective	Allows third-party execution	Assign risk to a third party via outsourcing or insurance	Follows self-directed approach	Allows third-party service provider	Allows third parties such as suppliers	Allows third-party and regulators	None
Technical perspective	√	√	√	√	√	√	×
Assessment team	×	√	√	√	×	×	×
Information gathering	Questionnaires, interviews, document review	Questionnaires, interviews, document review, observation	Workshop based approach	Interviews, workshops, surveys, and benchmarking	Questionnaires, interviews, document review	Questionnaires, interviews, document review	Interviews, workshops, surveys, and benchmarking
Human resources as an asset	×	√	√	√	√	√	√
Software tools used	√	√	√	√	×	√	√

Table 2. ISRM phases for different risk management frameworks (table is adopted from Faris et al. 2014).

ISRM Phases	ISRM Output	NIST	ISO 27005	OCTAVE
Characterization of IS and business process.	List of company's assets that require security and defining the risk appetite and acceptance level	System characterization	Critical asset identification and categorization	Determination of the currently implemented security practice, System characterization and context understanding

ISRM Phases	ISRM Output	NIST	ISO 27005	OCTAVE
Identification of cyber-threat and vulnerability	Identification of cyber-attacks and security vulnerabilities that may affect the already classified assets	List of identified threat intelligence, system vulnerability, and security control analysis	Threat and system vulnerability identification	Threat identification, system vulnerability identification
Analysis and definition of risks	Likelihood determination, impact analysis, and risk analysis and determination	Determination and rating of probability, impact analysis, and determination of risk	Potential impact analysis, likelihood determination, and risk identification	Impact analysis, probability, and risk determination
Analysis of security controls	Cost-benefit analysis and recommendation of various security controls to reduce the risk to an acceptable level	Analysis and recommendation of security controls	Analysis of risks and recommendation of risk reduction techniques	Detail analysis of risk and recommendation of security controls
Evaluation and implementation of security controls	Evaluation, recommendation, and implementation of security controls	Security control recommendation, cost-benefit analysis of security controls, implementation and evaluation of security controls	Recommendation of risk treatment/mitigation methods (reduction, avoidance, transfer, or retention)	Cost-benefit analysis, evaluation, implementation, and planning for the recommended security controls to protect the most critical assets

Moreover, the implementation support services through NIST are specific to US organizations, hence, sourcing appropriate and localized advice may be difficult. The other drawback of NIST is that it focuses on tactical-level risk assessment. However, it does not consider the strategic- and operational-level risk assessment.

In contrast, ISO 27005 aligns directly with ISO/IEC 27001 for information security management systems and provides a toolset that can be adopted around the specified controls. An organization of any type and size can also implement it. It also provides a basis for organizations to implement their risk management framework; however, it is costlier than the other frameworks. Moreover, it is difficult to understand the implementation details if the user is unfamiliar with ISO/IEC and its security controls.

COSO is complex and hence can be implemented by large and complex organizations. However, it does not incorporate risk assessment and analysis processes.

Unlike NIST, which operates at the tactical level of risk management, OCTAVE is a strategic-level risk management framework that can be applied with minimum cost and can be implemented for any type and size of the organization. It is also very well organized and is freely available. Moreover, OCTAVE addresses all aspects of

information security risks from technical, physical, and people perspectives. However, the limitations are that it is complex, and most organizations cannot model the risk. It also follows a qualitative risk management approach.

2. Cybersecurity Risk Mitigation Options

Risk treatment/mitigation is a method used by the top management of an organization to reduce the already assessed cyber-risk (Mazzoccoli and Naldi 2020). Mitigation of the identified risk can be addressed using the methods shown in **Figure 10**.

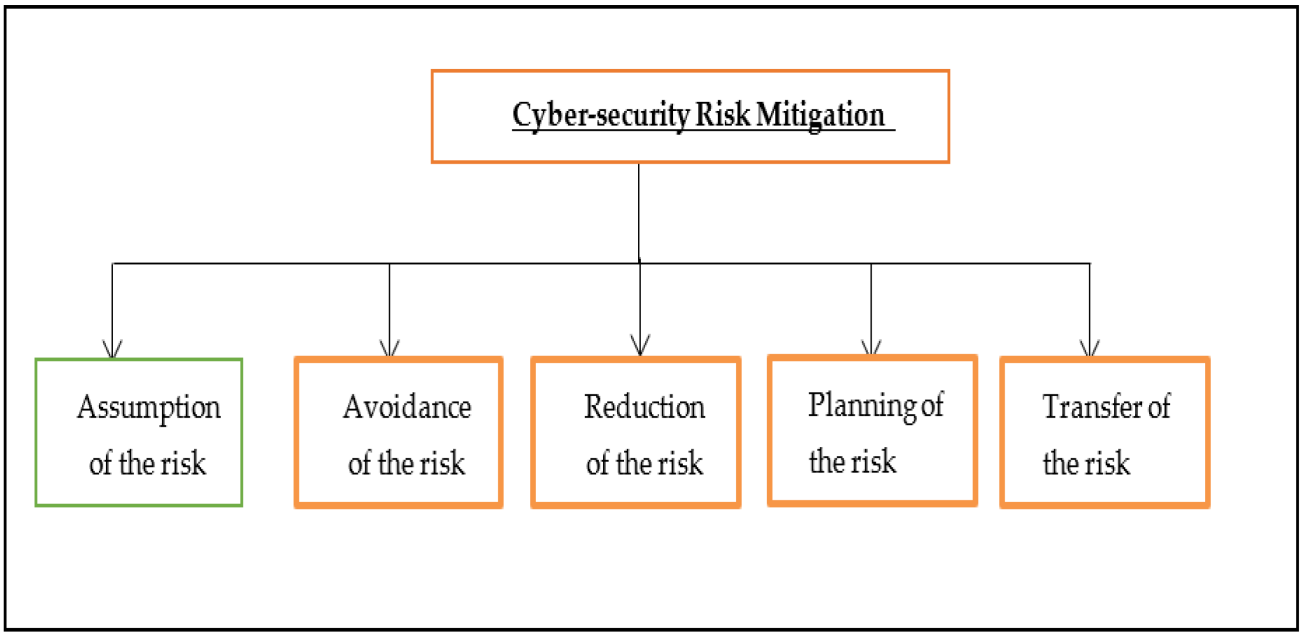

Figure 10. Risk mitigation options.

Risk assumption: This involves agreeing to take the cyber-risk and carry on the operation of the IT system that supports the business operation or to implement recommended security controls that are meant to minimize the cyber-risk to an acceptable risk level known as the risk appetite of the enterprise.

Risk avoidance: This is meant to avoid cyber-risk by removing the risk causes or sources, such as by giving up some of the system functionality and shutting down the system when the risk is identified.

Risk limitation: By implementing security controls such as using preventive, supportive, or detective techniques, limit the potential impact of threat sources that may exploit system vulnerability.

Risk planning is used to manage risks using risk mitigation plans such as IRP, BCP, and DRP.

Risk transfer: To transfer the risk to another third party to gain compensation for losing the company's assets due to a cyber-attack. Some risk transfer techniques are shifting the risk to other assets and processes, or other organizations, purchasing cyber-insurance, and outsourcing to other organizations.

3. Measuring the Cybersecurity Risk Management Framework

Measuring the benefits that the risk management framework brings to an organization is a complex and challenging task. To mitigate this challenge, the measurement of the risk management framework performance should be seen from different perspectives and needs to consider multiple factors.

Capability Maturity Assessment Model: This measures the security program's effectiveness within an organization using industry standards and best practices. One of the first steps to establish a security risk management framework for any type and size of organization is to evaluate the existing risk management program, process, and systems. In light of the above fact, the most efficient mechanism of understanding the current trend and status of the security program and process within a company is by performing and conducting a security capability maturity assessment. The risk management program and process should follow the capability maturity model with five levels, as shown in **Figure 11** below.

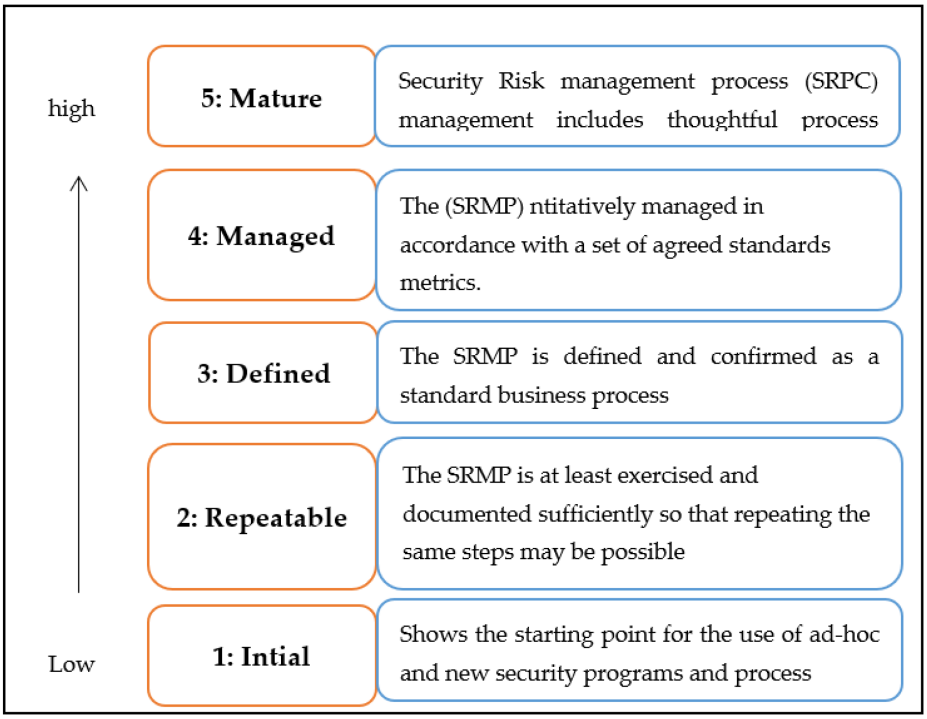

Figure 11. Capability maturity assessment model.

The maturity assessment models can have the subcategories shown in **Figure 12**.

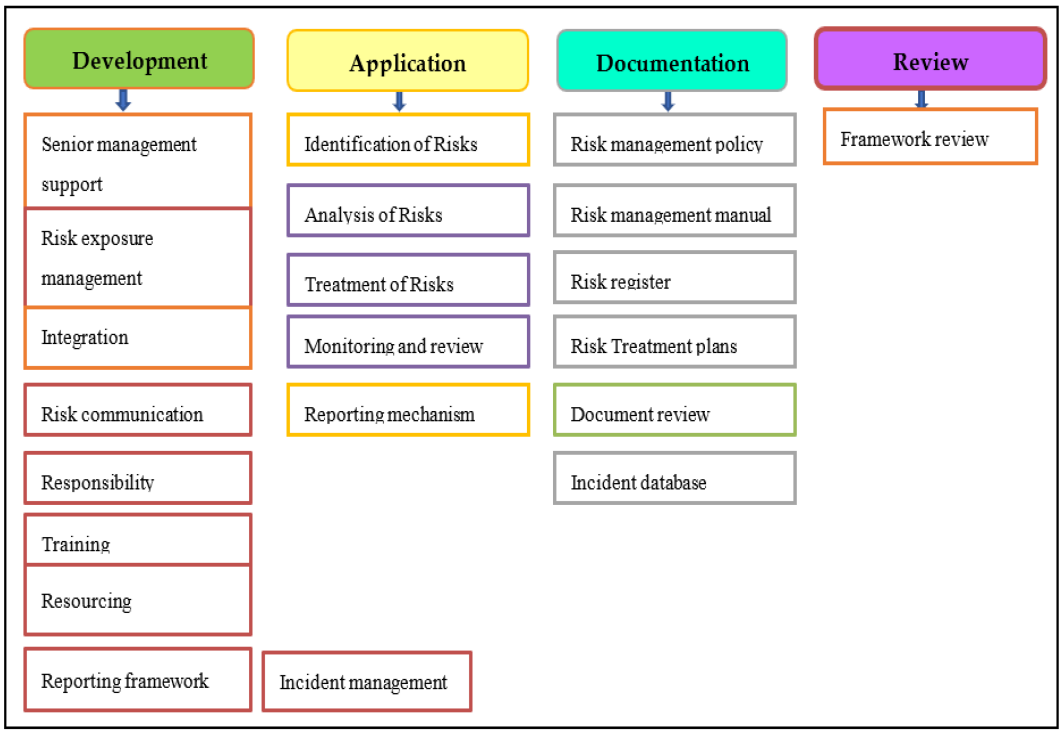

Figure 12. Risk assessment checklists.

Conformance measures whether the organization conforms to its security risk management policy directives. In addition to the maturity assessment techniques, risk management programs should go through conformance auditing. The primary function of conformance auditing is to ensure that the basic security requirements presented in the organization risk management policy are followed. Moreover, the company can also compare itself with other best practices and standards.

Value adds: This measures the extent to which the risk management program contributes to better accomplishing the company's security objectives and outcomes.

References

1. Tranchard, Sandrine. 2018. Risk management: The new ISO 31000 keeps risk management simple. Governance Directions 70: 180–82.
2. Rampini, Gabriel Henrique Silva, Harmi Takia, and Fernando Tobal Berssaneti. 2019. Critical success factors of risk management with the advent of ISO 31000 2018-Descriptive and content analyzes. Procedia Manufacturing 39: 894–903.
3. Shad, Muhammad Kashif, Fong-Woon Lai, Chuah Lai Fatt, Jiří Jaromír Klemeš, and Awais Bokhari. 2019. Integrating sustainability reporting into enterprise risk management and its

relationship with business performance: A conceptual framework. Journal of Cleaner Production 208: 415–25.

4. Kaur, Gurdip, and Arash Habibi Lashkari. 2021. Information Technology Risk Management. In Advances in Cybersecurity Management. Cham: Springer International Publishing, pp. 269–87.
5. Wang, Dayu, Daojun Zhong, and Liang Li. 2022. A comprehensive study of the role of cloud computing on the information technology infrastructure library (ITIL) processes. Library Hi Tech 40: 1954–75.
6. Al-Fatlawi, Qayssar Ali, Dawood Salman Al Farttoosi, and Akeel Hamza Almagtome. 2021. Accounting information security and it governance under cobit 5 framework: A case study. Webology 18: 294–310.
7. Lee, In. 2021. Cybersecurity: Risk management framework and investment cost analysis. Business Horizons 64: 659–71.
8. Goel, Rajni, Anupam Kumar, and James Haddow. 2020. PRISM: A strategic decision framework for cybersecurity risk assessment. Information & Computer Security 28: 591–625.
9. Sulistyowati, Diah, Fitri Handayani, and Yohan Suryanto. 2020. Comparative analysis and design of cybersecurity maturity assessment methodology using nist csf, cobit, iso/iec 27002 and pci dss. JOIV International Journal on Informatics Visualization 4: 225–30.
10. Gordon, Lawrence A., Martin P. Loeb, and Lei Zhou. 2020. Integrating cost–benefit analysis into the NIST Cybersecurity Framework via the Gordon–Loeb Model. Journal of Cybersecurity 6: tyaa005.
11. McCarthy, Charlie, and Kevin Harnett. 2014. National Institute of Standards and Technology (nist) Cybersecurity Risk Management Framework Applied to Modern Vehicles. No. DOT HS 812 073. Washington, DC: National Highway Traffic Safety Administration.
12. Almuhammadi, Sultan, and Majeed Alsaleh. 2017. Information security maturity model for NIST cyber security framework. Computer Science & Information Technology (CS & IT) 7: 51–62.
13. Diamantopoulou, Vasiliki, Aggeliki Tsohou, and Maria Karyda. 2020. From ISO/IEC27001: 2013 and ISO/IEC27002: 2013 to GDPR compliance controls. Information & Computer Security 28: 645–62.
14. Hom, Jane, Boonsri Anong, Kim Beom Rii, Lee Kyung Choi, and Kenita Zelina. 2020. The Octave AllegroMethod in Risk Management Assessmnet of Educational Institute. Aptisi Transactions on Technopreneurishp (ATT) 2: 167–79.
15. Faris, Sophia, Mohamed Ghazouani, Hicham Medromi, and Adil Sayout. 2014. Information security risk assessment—A practical approach with a mathematical formulation of risk. International Journal of Computer Application 103: 36–42.

16. Mazzoccoli, Alessandro, and Maurizio Naldi. 2020. Robustness of optimal investment decisions in mixed insurance/investment cyber risk management. Risk Analysis 40: 550–64.