A CONCEPTUAL FRAMEWORK: EVENT-BASED CYBERSECURITY RISK ASSESSMENT FOR ORGANISATIONS

WAN AZLENA WAN MOHAMAD[1], NURUL NUHA ABDUL MOLOK[2*], NOOR HAYANI ABD RAHIM[3]

[1,2,3]Department of Information Systems, Kulliyyah of Information and Communication Technology, International Islamic University Malaysia, Gombak, Malaysia

**Corresponding author: nurulnuha@iium.edu.my*

ABSTRACT: The current phenomenon of the interconnected digital world has heightened exposure to cyber risks, emphasising the critical need for robust cybersecurity risk management within organisations. Cybersecurity risk management encompasses identifying, assessing, and mitigating threats to protect individuals, organisations, and nations from cyber risks. Central to this process is the cybersecurity risk assessment, a fundamental exercise aimed at understanding and mitigating potential cyber threats. There are two primary risk assessment approaches: event-based and asset-based approaches. While current literatures are mostly focused on an asset-based approach, this study delves into the event-based approach by exploring potential cyber-attacks that could compromise the confidentiality, integrity, and availability of digital data, posing significant cybersecurity risks to organisations. Despite technological advancements and the increasing complexity of cyber threats, organisations' predominant reliance on an asset-based approach to cybersecurity risk assessment may not adequately address the evolving nature of cyber risks. Furthermore, there is a lack of harmonisation between scholarly and established cybersecurity frameworks based on international standards, such as those by the National Institute of Standards and Technology (NIST) and the International Organisation for Standardization (ISO). This paper synthesises existing frameworks from ISO, NIST and academic research and proposes recommendations to guide organisations in implementing an event-based approach to cybersecurity risk assessment.

KEY WORDS: *Cybersecurity, Information security, Risk management, Risk assessment, Event-based, Framework*

1. INTRODUCTION

In the contemporary digital landscape, the reliance of organisations on technology for operational efficiency, enhanced service delivery, and client engagement has significantly increased. However, this digital transformation has also increased the organisation's exposure to cyber risks (Krishtanosov & Brovko, 2023). As organisations become more reliant on digital infrastructure, the potential for cyber-attacks that could disrupt services, compromise sensitive information, and undermine client trust becomes an urgent concern (National Cybersecurity Agency,

2020). This phenomenon underscores the critical need for robust cybersecurity risk management within organisations.

Cybersecurity risk management encompasses a comprehensive process of identifying, assessing, and mitigating threats to protect individuals, organisations, and nations from cyber risks (Chen et al., 2021; Lau et al., 2021; Sukumar et al., 2023). At the heart of this process lies the cybersecurity risk assessment, a fundamental exercise aimed at identifying and assessing potential cyber threats (ISO/IEC 27005, 2022; NIST SP 800-30, 2012). A robust risk assessment process is essential for devising effective strategies to protect against cyber-attacks and ensure the resilience of public sector operations. There are two primary approaches to risk assessment: the event-based approach and the asset-based approach (ISO/IEC 27005, 2022).

In this context, an "event" refers to any occurrence or change in circumstances that might impact security (ISO/IEC 27005, 2022). The event-based approach to cybersecurity risk assessment focuses on analyzing potential cyber events or incidents that could compromise the confidentiality, integrity, and availability of digital data (ISO/IEC 27005, 2022). This approach involves identifying specific threats, understanding their potential impact, and developing strategies to mitigate those threats (ISO/IEC 27005, 2022). By concentrating on events, this method aims to provide a more dynamic and responsive framework for managing cyber risks, which is particularly important given the rapidly evolving nature of cyber threats.

On the other hand, the underlying concept of an asset-based approach is that risks can be identified and assessed through an inspection of assets, threats and vulnerabilities. The inherently dynamic nature of cybersecurity threats may not be sufficiently addressed by organisations that primarily rely on an asset-based approach to risk assessment. In recent times, cyber-attackers have upskilled their skills through AI techniques to automate attacks, augment their strategies, launch more sophisticated attacks and by implication increase their success (Ukwandu et al., 2020; Zhang et al., 2022). The asset-based approach typically focuses on identifying and protecting critical assets, such as information systems and data repositories. While this method is valuable and more popular than event-based approach, it may fall short in addressing the dynamic and multifaceted nature of modern cyber threats (Bagheri et al., 2023). The asset-based approach tends to emphasize static protection measures, which might not be sufficient in the face of sophisticated and adaptive cyber-attacks (Jung et al., 2023).

The scholarly focus on cybersecurity risk assessment has similarly leaned towards asset-based methods, potentially weakening strategies against emerging cyber threats. For instance, the studies on cybersecurity risk assessment by previous scholars such as (Akbarzadeh & Katsikas, 2023), (Kalinin et al., 2021), (Rea-Guaman et al., 2020), (Mathias Ekstedt et al., 2023) and others are more inclined toward an asset-based approach while less previous scholars focused on the event-based approach.

Moreover, there is insufficient alignment between academic research and established cybersecurity frameworks grounded in international standards, such as those from the NIST and the ISO (Melaku, 2023). These standards provide comprehensive guidelines for managing cybersecurity risks and offer valuable insights into best practices.

This study addresses this gap by proposing an event-based cybersecurity risk assessment framework. The propose framework is developed through a synthesis of the two international standards, ISO/IEC 27005 and NIST SP 800-30, as well as a study by Elmarady & Rahouma This approach seeks to integrate the strengths of these established frameworks with insights from recent scholarly research, creating a comprehensive and practical framework for managing cyber risks in organisations.

2. OVERVIEW OF CYBERSECURITY RISK ASSESSMENT

This section presents the reviews of academic literature and existing standards to understand cybersecurity risk assessment including the definitions, key elements and approaches.

2.1. Definitions of Cybersecurity Risk Assessment

Cybersecurity risk management is defined as the systematic application of management policies, procedures, and practices to the activities of communicating, consulting, establishing the context, and identifying, analyzing, evaluating, treating, monitoring, and reviewing risk (ISO/IEC 27005, 2022). Cybersecurity risk assessment is an important process in the field of cybersecurity risk management, essential for the protection of an organisation's digital information. There are various definitions of cybersecurity risk assessment, although from different sources, share the same objective: to identify, estimate and prioritize information security risks.

According to NIST SP 800-37, cybersecurity risk assessment is central to organisational risk management, emphasizing the protection of operations, missions, reputation, and assets, as well as broader impacts on other organisations and national security (NIST SP 800-37, 2018). This underscores the broad implications of cybersecurity risks and the need for a comprehensive approach. ISO/IEC 27005 defines cybersecurity risk assessment as a process of identifying, analyzing, and assessing risks to make informed decisions that ensure organisational objectives are met (ISO/IEC 27005, 2022). This highlights the strategic role of cybersecurity risk assessment in decision-making and goal alignment.

Meanwhile, NIST SP 800-30 defines it as identifying, estimating, and prioritizing cybersecurity risks by analyzing threats and vulnerabilities, focusing on the analytical aspect of assessing the likelihood and impact of adverse events (NIST SP 800-30, 2012). Whitman et al. describe cybersecurity risk assessment as an integrated approach combining risk identification, analysis, and assessment into a cohesive strategy, simplifying the management of cybersecurity risks (Whitman & Mattord, 2018).

All definitions stress the importance of understanding threats and vulnerabilities to protect digital information. The emphasis varies: NIST SP 800-37 on the broad scope of impacts; ISO/IEC 27005 on aligning risk management with objectives; NIST SP 800-30 on the analytical process; and Whitman et al. on an integrated strategy.

2.2. Key Elements in Cybersecurity Risk Assessment

The key elements in cybersecurity risk assessment encompass three (3) primary processes as presented in Fig. 1.

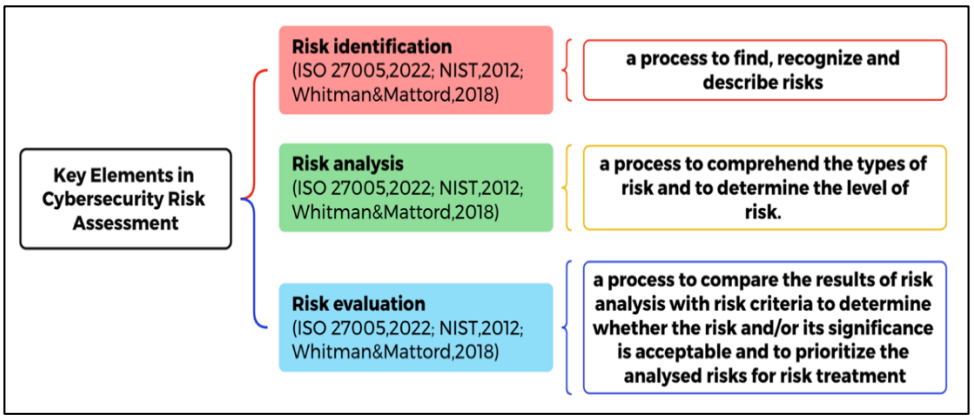

Fig. 1. Key elements in cybersecurity risk assessment

Risk identification is the stage where risks are discovered, acknowledged, and described. It's about spotting potential threats that could negatively impact an organisation's assets and operations (ISO/IEC 27005, 2022; NIST SP 800-30, 2012; Whitman & Mattord, 2018).

During the risk analysis phase, the nature of identified risks is understood, and the level of risk is determined. It involves assessing the likelihood and potential consequences of each risk (ISO/IEC 27005, 2022; NIST SP 800-30, 2012; Whitman & Mattord, 2018).

Risk evaluation involves comparing the risk analysis results against established criteria to determinethe acceptability of the risk. It also prioritizes the risks identified to inform the risk treatment process, which involves deciding on the measures to mitigate, accept, or transfer the identified risks (ISO/IEC 27005, 2022; NIST SP 800-30, 2012; Whitman & Mattord, 2018).

2.3. Approaches in Cybersecurity Risk Assessment

There are two main approaches for assessment: an event-based approach and an asset-based approach (ISO/IEC 27005, 2022).

In an event-based approach, the underlying concept is that risks can be identified and assessed through an evaluation of events and consequences (ISO/IEC 27005, 2022). Events and consequences can often be determined by a discovery of the concerns of top management, risk owners and the requirements identified in determining the context of the organisation (ISO/IEC 27005, 2022).

In an asset-based approach, the underlying concept is that risks can be identified and assessed through an inspection of assets, threats and vulnerabilities (ISO/IEC 27005, 2022). An asset is anything that has value to the organisation and therefore requires protection. Assets should be identified, taking into account that an information system consists of activities, processes and information to be protected (ISO/IEC 27005, 2022).

The event-based approach is contrasted with the asset-based approach to risk identification (ISO/IEC 27005, 2022). In principle, the two approaches differ only regarding the level at which identification is initiated. This study focuses on the event-based approach to cybersecurity risk assessment because it offers a more dynamic and context-specific understanding of risks. This approach aligns with the

necessity for a more adaptive and responsive risk management strategy that addresses not only the technical aspects of cybersecurity but also the broader organizational context and stakeholder concerns (Ganin et al., 2020). Additionally, the event-based approach facilitates a more comprehensive assessment by considering the interplay between different events and their cumulative impact on the organization (Liu et al., 2021). Therefore, developing a framework for event-based cybersecurity risk assessment will provide organizations with a robust framework to assess risks in an increasingly complex digital environment.

3. REVIEW OF EXISTING CYBERSECURITY RISK ASSESSMENT FRAMEWORKS

In the dynamic landscape of information technology, cybersecurity risk management and assessment frameworks serve as essential frameworks for safeguarding digital information. This section presents the reviews of existing cybersecurity risk management and assessment frameworks including the relevant standards and previous studies.

3.1. Comparison of ISO, NIST and ITSRM Cybersecurity Risk Management and Assessment Frameworks

Information security controls, methods and techniques can be applied to manage cybersecurity risks (ISO/IEC TS 27100, 2020). The ISO/IEC 27005 and NIST SP 800-37 stand out as global beacons, widely adopted for their robust approach to managing risk in cybersecurity (Efe A, 2023; ENISA, 2022; Melaku, 2023). Complementing these is the NIST SP 800-30, a risk assessment framework for its event-based approach, which takes into account specific incidents that could potentially disrupt cybersecurity (ENISA, 2022). Additionally, the European Union's IT Security Risk Management Methodology (ITSRM) is known for its process-oriented framework, which meticulously outlines the inputs and outputs associated with each risk management process (ENISA, 2022). A review of these frameworks is presented in Table 1.

Table 1: Comparison of ISO, NIST and ITSRM cybersecurity risk management and assessment frameworks

Parameters	ISO/IEC 27005 (2022)	NIST SP 800-30 (2012)	NIST SP 800-37 (2018)	EU ITSRM2 (2020)
Context Establishment	Yes	No	Yes	Yes
Asset-based / Event-based	• Asset-based • Event-based	Event-based	Asset-based	Asset-based
Risk Treatment	Yes	No	Yes	Yes
Author	ISO	NIST	NIST	EU DIGIT
Compatibility	Any type and size of the organization	Any type and size of the organization	Any type and size of the organization	Any type and size of the organization
Focus Area	Holistic RM	Risk Assessment	Tactical-level RM	Holistic RM
Risk Management Team	Yes	Yes	Yes	Yes
Communication and Consultation	Yes	Yes	Yes	Yes
Monitoring And Review	Yes	Yes	Yes	Yes
Challenges	• Higher costs (Paid access) • Difficulties in implementation for users who are not familiar with ISO/IEC standards	• Focus on Risk Assessment only • Primarily for U.S. federal government entities	Primarily for U.S. federal government entities	Mainly adapted for European organisations

ISO/IEC 27005 provides a comprehensive approach, allowing both asset-based and event-based risk assessments and including context establishment and risk treatment (ISO/IEC 27005, 2022). It is designed for organisations of any type and size, promotes a holistic risk management view, and includes a risk management team, communication, consultation, and monitoring and review processes. However, it can be costly due to paid access and challenging for those unfamiliar with ISO/IEC standards (Melaku, 2023).

NIST SP 800-30 focuses solely on event-based risk assessment (ENISA, 2022) and is specifically tailored for U.S. federal government entities (Efe A, 2023; Melaku, 2023). It lacks context establishment and risk treatment components but includes a risk management team, communication, consultation, and monitoring and review.

NIST SP 800-37 is asset-based (ENISA, 2022) and includes context establishment, risk treatment, a risk management team, communication,

consultation, and monitoring and review. Its focus is on tactical-level risk management, and it is again primarily suited for U.S. federal government entities (Efe A, 2023; Melaku, 2023).

EU ITSRM2 is asset-based, including context establishment, risk treatment, and all the supporting processes, similar to ISO/IEC 27005 (ENISA, 2022). It is adaptable for any organisation size and type, with a holistic risk management focus, designed mainly for European organisations.

All frameworks are compatible with any type and size of the organisation and include a risk management team, communication, consultation, and monitoring and review processes. However, they differ in their approach to risk assessment, focus area, and specific regional applicability.

This study focuses on ISO/IEC 27005 and NIST SP 800-30 in developing an event-based cybersecurity risk assessment framework for organisations with several justifications. ISO and NIST's methodologies are globally recognized and respected (Efe A, 2023; ENISA, 2022; Melaku, 2023). ISO/IEC 27005 offers a comprehensive framework for managing information security risks, allowing both asset-based and event-based assessments. This flexibility is crucial for organizations needing to adapt their risk management approach to specific contexts (Putra & Soewito, 2023). On the other hand, NIST SP 800-30 focuses on event-based risk assessments (ENISA, 2022), which are particularly effective for identifying and evaluating the dynamic nature of cybersecurity threats. This methodology is suitable for organizations aiming to understand and mitigate specific events that could impact their systems (Putra & Soewito, 2023).

Combining ISO/IEC 27005 with NIST SP 800-30 allows leveraging the strengths of both standards. ISO/IEC 27005 offers a holistic view of risk management, while NIST SP 800-30 provides detailed guidance on conducting thorough event-based risk assessments, ensuring a robust and adaptable risk management strategy (Fikri et al., 2019). Therefore, the researchers can develop a robust event-based cybersecurity risk assessment framework that combines comprehensive risk management principles with detailed, context-specific risk assessment practices.

3.2. Comparison of Previous Studies on Cybersecurity Risk Assessment Frameworks

A comparative overview of various cybersecurity risk assessment studies, contrasting their findings, approaches, and scopes is presented in Table 2.

Table 2: Comparison of previous studies on cybersecurity risk assessment frameworks

Authors & Research Title	Research Finding	Risk Assessment Approach	Scope
Rea-Guaman et al. (2020) AVARCIBER: A Framework For Assessing Cybersecurity Risks	Proposed a framework to identify and assess cybersecurity risks to improve the decision-making process regarding the importance and criticality of the risks and countermeasures that must be applied (Rea-Guaman et al., 2020).	Asset-based	Organisations
Elmarady & Rahouma, (2021) Studying Cybersecurity in Civil Aviation, Including Developing and Applying Aviation Cybersecurity Risk Assessment	Identify potential cyber threats to aviation systems and to evaluate their likelihood and risk levels (Elmarady and Rahouma, 2021).	Event-based	Civil Aviation
Kalinin et al. (2021) Cybersecurity risk assessment in smart city infrastructures	Evaluated cybersecurity risks in the dynamic device-to-device networks characteristic of smart city infrastructures (Kalinin et al., 2021).	Asset-based	Smart city infrastructures
Akbarzadeh & Katsikas (2023) Dependency-Based Security Risk Assessment For Cyber-Physical Systems	Propose a dependency-based, domain-agnostic cybersecurity risk assessment method to identify possible attack paths against critical components (Akbarzadeh & Katsikas, 2023).	Asset-based	Cyber-Physical Systems
Ekstedt et. al (2023) Yet Another Cybersecurity Risk Assessment Framework	Introduces a metaframework-based approach named Yet Another Cybersecurity Risk Assessment Framework (Yacraf) which aims to enable comprehensive risk assessment for organizations with more decision support (Mathias Ekstedt et al., 2023).	Asset-based	Organisations
Researchers' Study Event-based Cybersecurity Risk Assessment for Organisations	Proposed an event-based cybersecurity risk assessment framework for organisations	Event-based	Organisations

The comparison reveals that most studies, such as those by Rea-Guaman et al., Kalinin et al., Akbarzadeh & Katsikas, and Ekstedt et al., employ an asset-based risk assessment approach. These studies focus on various scopes including organisations, smart city infrastructures, and cyber-physical systems. In contrast, Elmarady & Rahouma (2021) stand out by using an event-based approach specifically for the civil aviation sector, identifying and evaluating potential cyber threats to aviation systems. This highlights a gap and the potential need for more event-based risk assessment frameworks in organisations to address the evolving nature of cyber threats effectively.

This study focuses on the study by Elmarady & Rahouma on the development of an event-based cybersecurity risk assessment framework for organizations with several justifications. The study by Elmarady & Rahouma specifically utilizes an event-based risk assessment approach, tailored to evaluate potential cyber threats and their likelihood (Elmarady & Rahouma, 2021). This method is highly relevant for dynamic and evolving cyber threat environments, providing a more responsive and adaptive risk management strategy. Furthermore, their research is applied in the civil aviation sector, a high-stakes environment where cybersecurity threats can have severe consequences (Elmarady & Rahouma, 2021). The methodologies and insights gained from this study can be valuable when adapted to other sectors with critical cybersecurity needs, including various organizational contexts. By leveraging the insights and methodologies from Elmarady & Rahouma can significantly enhance the development of an event-based cybersecurity risk assessment framework for organizations, ensuring a comprehensive, dynamic, and adaptable approach to managing cybersecurity risks.

4. PROPOSED FRAMEWORK

This section presents the proposed Event-based Cybersecurity Risk Assessment Framework designed specifically for organizations, outlining its key components and methodologies.

4.1. Adapted Frameworks

The proposed framework of this study adapted three (3) frameworks: ISO/IEC 27005, NIST SP 800-30 and Elmarady & Rahouma to achieve the research objective. The justifications for adapting these frameworks were mentioned in sections 3.1 and 3.2 of this article.

Fig. 2 represents the cybersecurity risk management framework defined by ISO/IEC 27005 while Fig. 3 represents the cybersecurity risk assessment framework defined by NIST SP 800-30. Fig. 4 represents the cybersecurity risk assessment framework defined by Elmarady & Rahouma.

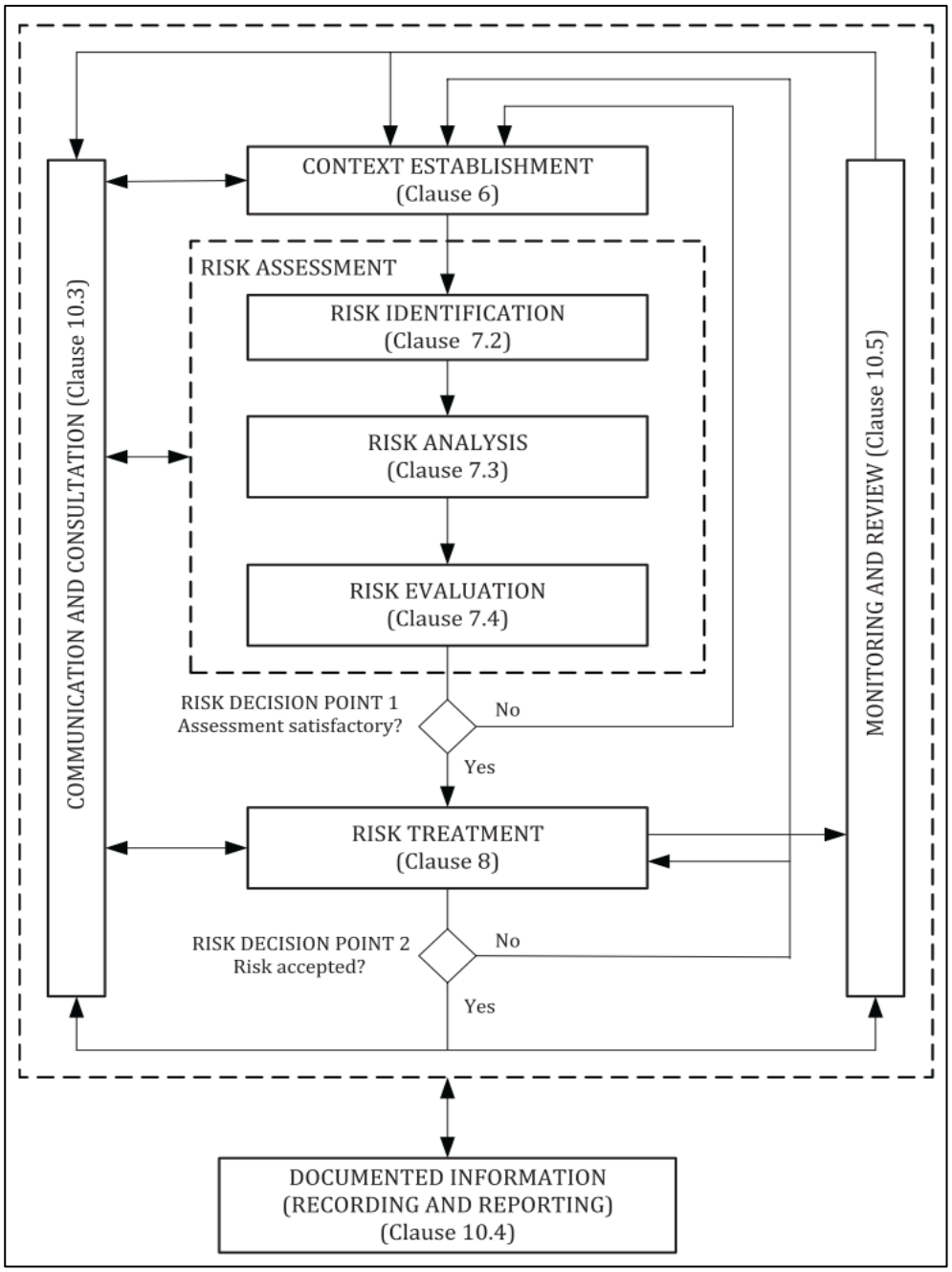

Fig. 2. Framework by ISO/IEC 27005, 2022

The ISO/IEC 27005 framework (ISO/IEC 27005, 2022) prepares for assessment by establishing a risk context in the wider risk management framework, integrating core elements of risk assessment to ensure a comprehensive approach. It systematically identifies events that could pose a risk, the sources of these risks, and the potential impacts, thereby constructing a comprehensive risk profile. The inclusion of likelihood assessment and risk level determination allows organisations to gauge the severity and prioritize their responses effectively. A unique feature of this framework is the identification of a risk owner for each identified risk, ensuring that accountability is assigned and that actions are owned and managed. Despite its thorough approach in these areas, the framework does not explicitly focus on monitoring and review, which may suggest an expectation for these activities to be integrated within the broader organisational risk management processes.

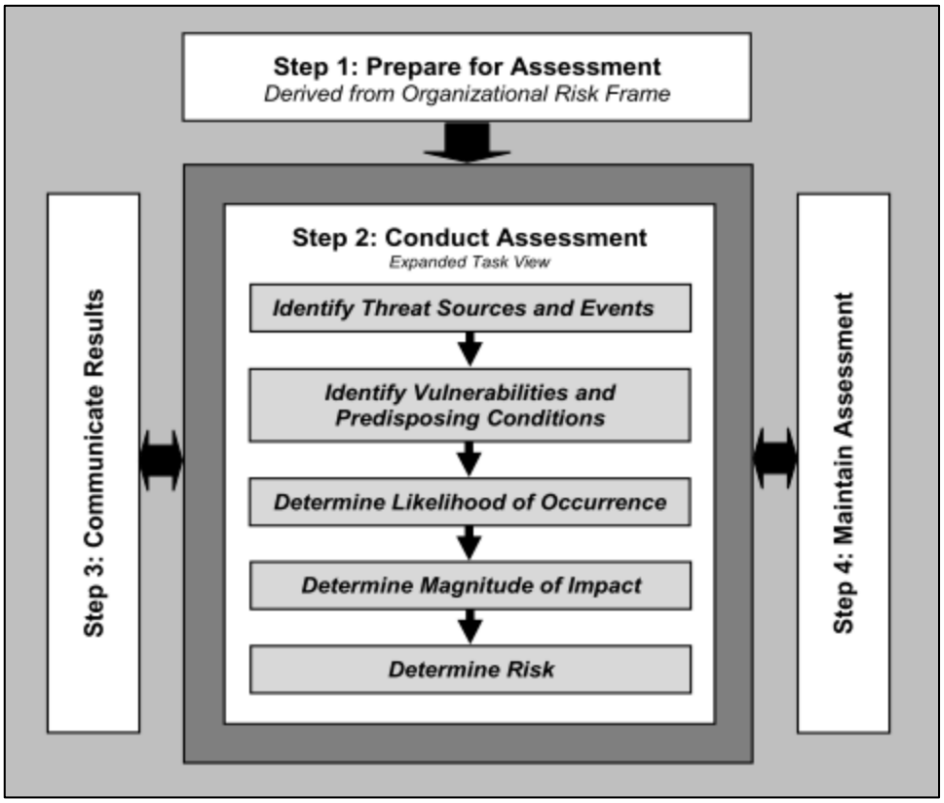

Fig. 3. Framework by NIST SP 800-30, 2012

The NIST SP 800-30 framework (NIST SP 800-30, 2012) emphasizes a more structured approach, beginning with a distinct preparation phase. This suggests a recognition of the importance of setting the stage for a comprehensive assessment by understanding the organisational context and resources at the outset. It shares commonalities with the ISO framework in identifying events, sources, impacts, and likelihoods of risks, demonstrating a consensus on these critical steps in risk assessment. However, it departs from ISO by not assigning a risk owner, perhaps reflecting a preference for a shared responsibility framework or the integration of risk ownership into wider roles. The framework notably includes a dedicated monitoring and review component, indicating a commitment to ongoing risk management and the adaptation to changing threat landscapes over time.

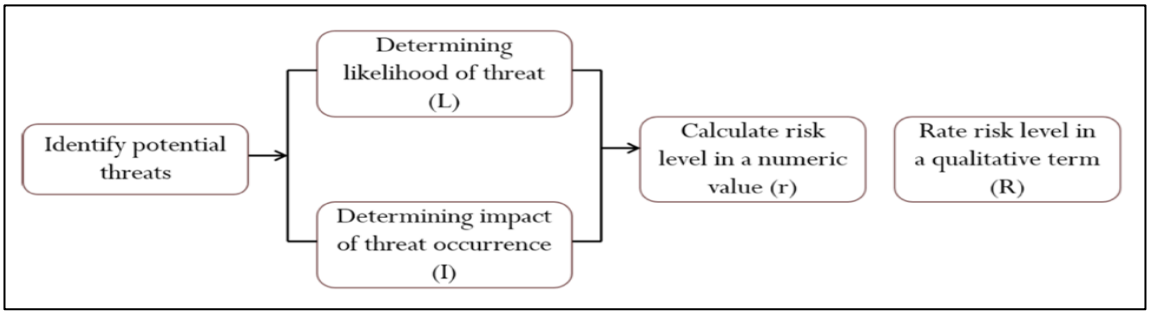

Fig.4. Framework by Elmarady & Rahouma, 2021

The Elmarady & Rahouma framework (Elmarady & Rahouma, 2021) presents a concise event-based approach to risk assessment. It consists of a preparatory phase by identifying the scope of the system that needs to be protected. It bypasses

the identification of risk sources, suggesting a focus on the agile response to threats rather than detailed planning or source tracing. The framework aligns with the others in the identification of events, impacts, and likelihoods, but it does not stipulate the determination of risk owners, pointing towards the framework operating within a pre-defined risk ownership structure. Additionally, the absence of prescribed communication and consultation steps, as well as a lack of a monitoring and review phase, indicates the framework is designed for rapid assessment within the civil aviation environment where other mechanisms provide for these functions.

The comparison of components across three adapted cybersecurity risk assessment frameworks is presented in Table 3. ISO/IEC 27005, NIST SP 800-30 and Elmarady & Rahouma show varying levels of inclusion for different risk assessment components.

Table 3: Components comparison of three adapted risk assessment frameworks

Parameters	ISO/IEC 27005 (2022)	NIST SP 800-30 (2012)	Elmarady et.al (2021)
Prepare for Assessment	Yes	Yes	Yes
Identify Events	Yes	Yes	Yes
Identify Risk Sources	Yes	Yes	No
Identify Impact	Yes	Yes	Yes
Identify Likelihood	Yes	Yes	Yes
Determine Risk Level	Yes	Yes	Yes
Identify Risk Owner	Yes	No	No
Communication & Consultation	Yes	Yes	No
Monitor & Review	Yes	Yes	No

The synthesis of the parameters for ISO/IEC 27005, NIST SP 800-30, and Elmarady & Rahouma frameworks reveals both commonalities and distinctions in their approaches to cybersecurity risk assessment. All three frameworks include the essential step of preparing for assessment, ensuring that organizations establish a structured process before identifying risks. They uniformly emphasize the importance of identifying events, a critical component for understanding potential cybersecurity threats.

When it comes to identifying risk sources, both ISO/IEC 27005 and NIST SP 800-30 recognize this step, highlighting their comprehensive approach to understanding where threats originate (ISO/IEC 27005, 2022; NIST SP 800-30, 2012). In contrast, the framework by Elmarady & Rahouma does not specifically

address identifying risk sources, which might suggest a more streamlined or focused approach within the civil aviation context (Elmarady & Rahouma, 2021).

All three frameworks concur on the importance of identifying the impact and likelihood of events, which are fundamental for evaluating potential risks (Elmarady & Rahouma, 2021; ISO/IEC 27005, 2022; NIST SP 800-30, 2012). This commonality underscores a shared understanding of assessing both the severity and probability of cybersecurity incidents. Consequently, each framework also determines the risk level (Elmarady & Rahouma, 2021; ISO/IEC 27005, 2022; NIST SP 800-30, 2012), providing a quantified measure of the identified risks, essential for prioritizing and managing them effectively.

A significant divergence appears in the identification of risk owners, where ISO/IEC 27005 stands out by assigning responsibility for risk management (ISO/IEC 27005, 2022; NIST SP 800-30, 2012), which is not addressed in the other two frameworks. This element emphasizes accountability and clear delineation of roles within the risk management process. Although NIST SP 800-30 does not suggest organisations identify the risk owner, NIST SP 800-30 suggests organisations identify the information systems owner or business/mission owner (NIST SP 800-30, 2012).

Communication and consultation are integral to both ISO/IEC 27005 and NIST SP 800-30, ensuring that stakeholders are engaged and informed throughout the risk assessment process (ISO/IEC 27005, 2022; NIST SP 800-30, 2012). However, Elmarady & Rahouma do not explicitly include this parameter (Elmarady & Rahouma, 2021), which may reflect a narrower focus on technical assessment over stakeholder engagement.

Finally, the parameter of monitoring and review is included in NIST SP 800-30 (NIST SP 800-30, 2012), ISO/IEC 27005 (Elmarady & Rahouma, 2021; ISO/IEC 27005, 2022) and the Elmarady & Rahouma framework (Elmarady & Rahouma, 2021; ISO/IEC 27005, 2022). The inclusion of monitoring and review highlights the importance of continuous improvement and reassessment in managing cybersecurity risks, ensuring that the risk management process remains dynamic and responsive to new threats.

Each framework presents a different philosophy and set of priorities in cybersecurity risk assessment. ISO/IEC 27005 framework is meticulous and assumes ongoing risk assessment practices; NIST SP 800-30 framework is procedural and continuous; while Elmarady & Rahouma framework is streamlined and potentially embedded within a specific framework. These frameworks underscore that the choice of a risk assessment framework must align with the organisation's risk appetite, operational style, and the specific threats it faces.

4.2. Development of the Proposed Framework

The proposed framework as presented in Fig. 5 includes a sequence of components that outline the risk assessment process. The process starts with the preparation step to implement risk assessment (Elmarady & Rahouma, 2021; ISO/IEC 27005, 2022; NIST SP 800-30, 2012). The key elements in cybersecurity risk assessment are risk identification, risk analysis and risk evaluation (ISO/IEC 27005, 2022; NIST SP 800-30, 2012; Whitman & Mattord, 2018). Therefore, the researchers proposed three (3) main levels of risk assessment: Level 1- Risk

Identification, Level 2- Risk Analysis and Level 3- Risk Evaluation. By referring to ISO/IEC 27005 and NIST SP 800-30, risk communication and consultation are carried out throughout the risk assessment involving the three main levels (ISO/IEC 27005, 2022; NIST SP 800-30, 2012). Monitoring and review are conducted at all three main stages (NIST SP 800-30, 2012).

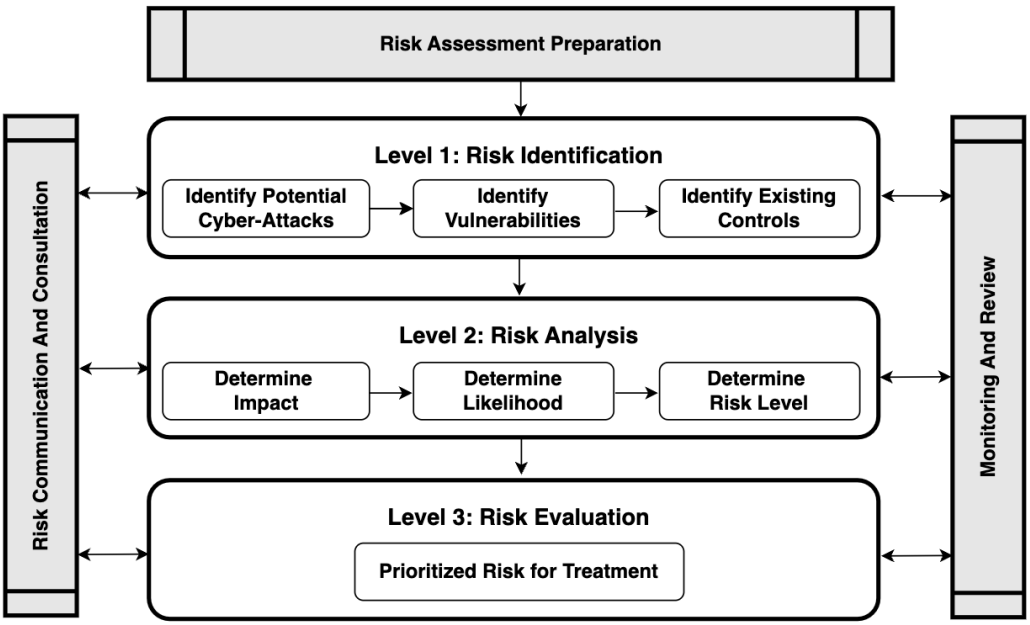

Fig. 5. Proposed Framework

4.2.1. Risk Assessment Preparation

Organisations should establish risk acceptance criteria before conducting a risk assessment (ISO/IEC 27005, 2022). These criteria help determine if a risk is acceptable. The risk acceptance criteria depend on the organization's policies, objectives and goals considering the aspects of business/service reputation, law, technology, finance, operations and social factors (Department of Prime Minister, 2024). Elmarady & Rahouma categorize risks into acceptable, tolerable, and intolerable levels (Elmarady & Rahouma, 2021). Acceptable risks require no further action, tolerable risks need some mitigation measures, and intolerable risks require immediate action to reduce the risk to a tolerable level. Therefore, the researchers proposed specific risk acceptance criteria as presented in Table 4 as guidance for organisations to determine the risk level.

Table 4: Proposed Risk Acceptance Criteria

Risk Level (Elmarady et.al,2021)		Details (Department of Prime Minister,2024)	Risk Acceptance Criteria (Elmarady et.al,2021)
Intolerable	3	Risks that have significant and immediate implications for the organization's functions, services and reputation and involve significant cost increases.	The cybersecurity risk index of the consequences is unacceptable. Immediate actions should be taken to mitigate the risk and reduce the cybersecurity risk index to a tolerable level
Tolerable	2	Risks that have moderate implications as well as additional costs to the organization's functions, services and reputation.	The risk level can be tolerated based on some risk mitigation measures
Acceptable	3	Risks that do not / less affect the organization's functions, services and reputation.	Risk Accepted. No further risk mitigation and control measures are required

4.2.2. Level 1 – Risk Identification

Risk identification aims to generate a list of risks based on those events that can prevent, affect or delay the achievement of cybersecurity objectives (ISO/IEC 27005, 2022). In an event-based approach, risks are identified and assessed by evaluating events and consequences, often determined through top management's concerns, risk owners, and organisational context (ISO/IEC 27005, 2022). Interviews with top management and responsible individuals help identify relevant events, consequences, and risk owners (ISO/IEC 27005, 2022). Elmarady & Rahouma identify potential cyber-attack scenarios that could harm an organisation's services, affecting integrity, confidentiality, and availability (Elmarady & Rahouma, 2021). NIST SP 800-30 states that threats to organisations or those directed through them are identified at the risk identification level (NIST SP 800-30, 2012). Thus, the researchers propose identifying potential cyber-attack scenarios at this stage.

4.2.2.1 Identify Potential Cyber-Attack Scenario

Event-based approaches identify potential cyber-attack scenarios by considering risk sources and their impact on organisations (ISO/IEC 27005, 2022). Both ISO/IEC 27005 and NIST SP 800-30 emphasise that identifying risk or threat sources helps recognise potential cyber threats. Therefore, the researchers suggest organisations identify risk sources based on the examples and typical attack methods from ISO/IEC 27005 as shown in Table 5.

Table 5: The Examples and Usual Methods of Attack by ISO/IEC 27005 (ISO/IEC 27005, 2022)

Risk Source	Examples and Usual Method of Attacks
State-related	States, intelligence agencies
	Method: Attacks generally conducted by professionals, working under a calendar and a method of attack that are predefined. This attacker profile is characterized by its ability to carry out an offensive operation over a long period of time (stable resources, procedures) and to adapt its tools and methods to the topology of the target. By extension, these actors have the means of purchasing or discovering 0-Day vulnerabilities and some are able to infiltrate isolated networks and to conduct successive attacks in order to reach a target or targets (e.g. by means of an attack aimed at the supply chain).
Organized crime	Cybercriminal organizations (mafias, gangs, criminal outfits)
	Method: Online scams or in person, ransom request or attack via ransomware, use of bot-nets, etc. Due in particular to the proliferation of attack kits that are readily available online, cybercriminals are conducting increasingly sophisticated and organized operations for lucrative or fraudulent purposes. Some have the means of purchasing or discovering 0-Day vulnerabilities.
Terrorist	Cyber-terrorists, cyber-militias
	Method: Attacks that are usually not very sophisticated but which are conducted with determination for the purposes of destabilization and destruction: denial of service (aimed for example at making the emergency services of a hospital centre unavailable, untimely shutdowns of an energy production industrial system), exploitation of vulnerabilities of Internet sites and defacement.
Ideological activist	Cyber-hacktivists, interest groups
	Method: The methods of attack and sophistication of the attacks are relatively similar to those of cyber-terrorists but are motivated by less destructive intentions. Some actors conduct these attacks in order to convey an ideology, a message (e.g. massive use of social networks as a sounding board).
Specialized outfits	"Cyber-mercenary" profile with IT capacities that are generally high from a technical standpoint. Because of this, it should be distinguished from script-kiddies with whom it shares however the spirit of a challenge and search for recognition but with a lucrative objective. Such groups can be organized as specialized outfits that propose veritable hacking services.
	Method: This type of experienced hacker is often at the origin of the designing and creating of attack kits and tools that are available online (possibly for a fee) which can then be used "turnkey" by other groups of attackers. There are no particular motivations other than financial gain.
Amateur	Profile of the script-kiddies hacker or who has good IT knowledge; motivated by the quest for social recognition, fun, challenge.
	Method: Basic attacks but with the capacity of use the attack kits that are available
Avenger	The motivations of this attacker profile are guided by a spirit of acute vengeance or a feeling of injustice (e.g. employee dismissed for serious fault, discontented service provider following a contract that was not renewed, etc.).
	Method: This attacker profile is characterized by its determination and its internal knowledge of the systems and organizational processes. This can make it formidable and provide it with substantial power to do harm.
Pathological attacker	The motivations of this attacker profile are of a pathological or opportunistic nature and are sometimes guided by the motive for a gain (e.g. unfair competitor, dishonest client, scammer, and fraudster).

	Method: Here, either attackers have a knowledge base in computing that leads them to attempt to compromise the IS of their target, or they use the attack kits available online, or decide to subcontract the IT attack by calling upon a specialized outfit. In certain cases, attackers can direct their attention to an internal source (discontented employee, unscrupulous service provider) and attempt to corrupt the latter.

4.2.2.2. Identify Vulnerabilities and Existing Controls

Cyber-attacks exploit a vulnerability of an asset or control to compromise the confidentially, integrity and/or availability of corresponding digital information. A vulnerability is a weakness in an asset or control that can be exploited by a risk source, leading to negative consequences (Elmarady & Rahouma, 2021; ISO/IEC 27005, 2022; NIST SP 800-30, 2012). Vulnerabilities can exist in governance structures, such as inadequate risk management strategies, poor communication, and misaligned enterprise architecture. They can also be found in external dependencies, mission processes, and security architectures (NIST SP 800-30, 2012).

Based on identified potential cyber-attacks and vulnerabilities, organisations should identify existing controls to avoid duplication and unnecessary costs (Department of Prime Minister, 2024). Reviewing these controls ensures they are effective. Therefore, the researchers suggest identifying vulnerabilities and existing controls in the risk identification phase.

4.2.3. Level 2 – Risk Analysis

Risk analysis aims to determine the risk level (ISO/IEC 27005, 2022). Activities in risk analysis involve determining impact, likelihood and risk level (Elmarady & Rahouma, 2021; ISO/IEC 27005, 2022; NIST SP 800-30, 2012).

4.2.3.1. Determine Impact

The impact of a threat event is the magnitude of harm from unauthorized disclosure, modification, destruction, or loss of digital information or service availability. Organisations assess impact based on loss value using a loss scale. ISO/IEC 27005 states that impact criteria should specify the damage or harm extent from loss of confidentiality, integrity, and availability of functions, missions, services, and data (ISO/IEC 27005, 2022). Elmarady & Rahouma rate impact on a five-point scale from high to low with descriptions of the impact on operations, services and reputation (Elmarady & Rahouma, 2021). The Department of Prime Minister rates impact on a five-point scale starting from very high, high, medium, low and very low (Department of Prime Minister, 2024) as shown in Table 6.

Table 6: Proposed Ratings of Impact

Scale	Impact Rating (Department of Prime Minister,2024)	Impact on Operations and Services (Elmarady & Rahouma, 2021)	Impact on Reputation (Elmarady & Rahouma, 2021)	Priority Level of Cybersecurity Incidents Handling (Department of Prime Minister,2022)
5	Very High	Serious impact where no operational services can be provided for an extended time period	The reputation cannot be recovered with stakeholders and the organization may not continue in its current form	If occur, priority level of cybersecurity incidents handling is 1
4	High	Major impact where a majority of operational services cannot be provided for some time	The reputation can be affected on capability to provide function services by the majority of the stakeholders	If occur, priority level of cybersecurity incidents handling is 1
3	Medium	Moderate impact where some operational services cannot be provided	The reputation can be affected on organization services and activities by a key stakeholder	If occur, priority level of cybersecurity incidents handling is 2
2	Low	Minor impact where some operational services are degraded	The reputation can be affected by the complaints of a key stakeholder on organization service and activities	If occur, priority level of cybersecurity incidents handling is 2
1	Very Low	Insignificant impact where operational services can be provided as usual	The reputation can be affected by the isolated compalints of individual stakeholder	If occur, priority level of cybersecurity incidents handling is 2

The Department of Prime Minister outlines two priority levels for cybersecurity incident management: Priority Level 1, which includes incidents with high impact on national defense, security, economic stability, reputation, government function, public health, safety, and privacy; and Priority Level 2 includes incidents other than priority level 1 and less impactful (Department of Prime Minister, 2022). The researchers propose incorporating these priority levels into the impact ratings, as demonstrated in Table 6, to aid organizations in accurately determining the impact rating.

4.2.3.2. Determine Likelihood

Likelihood is the chance of something happening (ISO/IEC 27005, 2022). After identifying risk scenarios, analyse the likelihood of each scenario using qualitative or quantitative techniques (ISO/IEC 27005, 2022). Findings from risks, vulnerabilities, and existing controls help in this analysis. Elmarady & Rahouma rate likelihood on a five-point scale with the frequency of occurrence of past similar attacks (Elmarady & Rahouma, 2021). The researchers proposed to rate likelihood based on the five-point scale as determined in the impact rating by the Department of Prime Minister (Department of Prime Minister, 2024) as shown in Table 7.

Table 7: Proposed Ratings of Likelihood

Scale	Likelihood Rating (Department of Prime Minister,2024)	Frequency of occurrence of past similar attacks (Elmarady et.al,2021)
5	Very High	At least once every two weeks
4	High	At least once every three months
3	Medium	Once every three months to a year
2	Low	Once every one to three years
1	Very Low	Once every three years or more

This scale is used to assess and prioritize risks based on their historical frequency, which in turn helps in the allocation of resources to mitigate such risks effectively.

4.2.3.3. Determine Risk Level

Based on the findings from the impact and likelihood assessment, organisations need to assess risk levels by considering (i) the potential impact and (ii) the probability of events (NIST SP 800-30, 2012). According to ISO/IEC 27005, a qualitative risk level matrix should align with the organisation's risk acceptance criteria (ISO/IEC 27005, 2022). Researchers propose determining risk level, *r*, as follows, where *L* is the likelihood scale (1-5) and *I* is the impact rating:

$$r = L\ x\ I$$

Elmarady & Rahouma suggest converting *r* into a qualitative term, *R*, to assess cybersecurity risk tolerability and apply necessary mitigation measures (Elmarady & Rahouma, 2021). The conversion formula is:

$$R = \begin{cases} intolerable, & r \geq 15 \\ tolerable, & 15 > r \geq 5 \\ acceptable, & r < 5 \end{cases}$$

The researchers adapted the cybersecurity risk matrix from Elmarady & Rahouma in which the risk index with acceptable levels is shown in light green, while tolerable levels is shown in yellow and intolerable is shown in red (Elmarady & Rahouma, 2021) as presented in Table 8.

Table 8: Cybersecurity Risk Matrix

Risk Level (*r*)	**Impact (I)**				
Likelihood (L)	Very Low	Low	Medium	High	Very High
Very Low	1	2	3	4	5
Low	2	4	6	8	10
Medium	3	6	9	12	15
High	4	8	12	16	20
Very High	5	10	15	20	25

The researchers adopted the conversion of risk level, *r*, into an equivalent five-point scale from Elmarady & Rahouma as presented in Table 9 (Elmarady & Rahouma, 2021).

Table 9: Five-point scale of risk level (Elmarady & Rahouma, 2021)

Risk Level (r)	**Tolerability of risk (R)**	**Five-point scale of risk level**
$\boldsymbol{r \geq 20}$	$intolerable$	5
$\boldsymbol{20 > r \geq 15}$	$intolerable$	4
$\boldsymbol{15 > r \geq 10}$	$tolerable$	3
$\boldsymbol{10 > r \geq 5}$	$tolerable$	2
$\boldsymbol{r < 5}$	$acceptable$	1

Intolerable risk includes any level $r \geq 15$. Both $r \geq 20$ and $20 > r \geq 15$ are intolerable, scored as 5 and 4 on the five-point scale. Tolerable risk falls between $15 > r \geq 5$, with $15 > r \geq 10$ and $10 > r \geq 5$ corresponding to 3 and 2. Acceptable risk, $r < 5$, is rated as 1. Higher numerical values indicate less tolerable risks, with 5 being intolerable and 1 acceptable.

4.2.4. Level 3 – Risk Evaluation

Risk evaluation compares risk analysis results with risk criteria to determine if a risk is acceptable or tolerable (ISO/IEC 27005, 2022). Applying risk acceptance criteria (Table 1) is essential in this process. Risk evaluation uses insights from risk analysis to recommend actions, focusing on the need for risk mitigation and prioritizing risks based on their level (ISO/IEC 27005, 2022).

4.2.5. Risk Communication and Consultation

Risk Communication and Consultation are continuous, iterative processes for sharing information and engaging with stakeholders on risk management (ISO/IEC 27005, 2022). NIST SP 800-30 emphasizes their importance for ensuring accurate risk assessment inputs, utilizing intermediate results, and providing meaningful inputs for risk response in the risk management process (NIST SP 800-30, 2012). The researchers suggest the process of risk communication and consultation is carried out throughout the risk assessment involving the three main stages.

4.2.6. Risk Monitoring and Maintenance

Potential cyber-attacks, vulnerabilities, existing controls, impact, likelihood, and level of risk are constantly changing, requiring continuous monitoring. According to NIST SP 800-30 maintaining risk assessments involves (NIST SP 800-30, 2012):

- Monitoring identified risk factors and understanding changes; and
- Updating risk assessment components based on monitoring activities.

ISO/IEC 27005 defines monitoring risk-related events using indicators from strategic scenarios, prioritizing events by consequence magnitude and likelihood (ISO/IEC 27005, 2022). Therefore, organisations should regularly review Potential cyber-attacks, vulnerabilities, existing controls, impact, likelihood, and level of risk.

4.2.7. Example of a complete risk assessment (Levels 1 to 3)

Table 10 presents the example of a complete risk assessment of level 1 to 3 of an organisation.

Table 10: Example of a complete risk assessment of levels 1 to 3

LEVEL 1 : RISK IDENTIFICATION			LEVEL 2 : RISK ANALYSIS					LEVEL 3: RISK EVALUATION
Potential Cyber Attack	Vulnerabilities	Existing Control	Impact (*I*)	Likelihood (*L*)	Risk Level (r = *I* x *L*)	Tolerability of Risk	Five-point Scale of Risk Level	
DOS/DDOS	Volumetric Vulnerabilities	deploying firewalls network segmentation intrusion detection systems	Medium-High	Low	4	**Acceptable**	1	No further risk mitigation and control measures are required
	Protocol Vulnerabilities	using secure protocols						
Website defacement	No web application firewalls (WAFs)	using web application firewalls (WAFs)	Medium-Low	High	10	**Tolerable**	3	The risk level can be tolerated based on some risk mitigation measures
	Server Misconfiguration	conducting security audits						
	User Authentication Vulnerabilities	penetration testing, code review						
	SQL Injection Vulnerabilities							
	Cross-Site Scripting (XSS) Vulnerabilities							
	Remote File Inclusion (RFI) Vulnerabilities							
	Outdated Software	regular updates to software						
Ransomware, Data breach	Server Misconfiguration	conducting security audits	High	Medium-High	20	**Intolerable**	5	Immediate actions should be taken to mitigate the risk and reduce the cybersecurity risk index to a tolerable level
	User Authentication Vulnerabilities	penetration testing, code review						
	SQL Injection Vulnerabilities							
	Cross-Site Scripting (XSS) Vulnerabilities							
	Remote File Inclusion (RFI) Vulnerabilities							
	absence of a robust data backup strategy	implement regular data backup strategy						
	Outdated Software	regular updates to software						
Phishing emails	lack of effective email filtering	strengthen the email filtering configuration - block phishing email	Medium-Low	High	**10**	**Tolerable**	3	The risk level can be tolerated based on some risk mitigation measures
Email spoofing	less awareness on email spoofing	monthly regular awareness						
Brute force system access	Weak password	strong password policies						
	No input validtion	provide input validation						
Trojan, Worms, Botnet	outdated software	regular updates to software	Medium-Low	High	**10**	**Tolerable**	3	The risk level can be tolerated based on some risk mitigation measures
	lack of effective email filtering	strengthen the email filtering configuration - block phishing email						
	insecure credential management	secured credential management						
Malware hosting	outdated software	regular updates to software	Medium-High	Low	4	**Acceptable**	1	No further risk mitigation and control measures are required
	lack of effective email filtering	strengthen the email filtering configuration - block phishing email						
	insecure credential management	secured credential management						
Directory listing	improper web server configurations	secured web server configurations	Low	Medium-Low	2	**Acceptable**	1	No further risk mitigation and control measures are required

5. CONCLUSION

In conclusion, as the digital landscape continues to evolve and cyber threats become more sophisticated, it is imperative for organizations to adopt a more dynamic and responsive approach to cybersecurity risk assessment. While the traditional asset-based approach has been widely used, it may not fully capture the complexities of modern cyber risks. This study highlights the benefits of an event-based approach, which focuses on identifying and evaluating specific cyber incidents and their potential impacts on an organization's operations and data integrity. By synthesizing existing frameworks from ISO, NIST, and academic research, this paper provides a comprehensive framework for implementing event-based cybersecurity risk assessments. Adopting this approach can enhance an organization's ability to anticipate, prepare for, and respond to cyber threats, thereby strengthening overall cybersecurity posture. Future research could be expanded by evaluating the approaches in specific sectors with unique cybersecurity challenges contributing to the enhanced cybersecurity posture of organisations.

ACKNOWLEDGEMENT

We acknowledge and thank the Public Administration Department of Malaysia (JPA), for sponsoring this study under the *Hadiah Latihan Persekutuan* program for government officials.

REFERENCE

Akbarzadeh, A., & Katsikas, S. K. (2023). Dependency-based security risk assessment for cyber-physical systems. *International Journal of Information Security*, *22*(3), 563–578. https://doi.org/10.1007/s10207-022-00608-4

Bagheri, S., Ridley, G., & Williams, B. (2023). Organisational Cyber Resilience: Management Perspectives. *Australasian Journal of Information Systems*, *27*. https://doi.org/10.3127/ajis.v27i0.4183

Chen, J., Zhu, Q., & Başar, T. (2021). Dynamic Contract Design for Systemic Cyber Risk Management of Interdependent Enterprise Networks. *Dynamic Games and Applications*, *11*(2), 294–325. https://doi.org/10.1007/s13235-020-00363-y

Department of Prime Minister. (2022). *General Circular Number 4 of 2022: Management and Handling of Public Sector Cyber Security Incidents dated 1 August 2022*.

Department of Prime Minister. (2024). *General Circular Number 3 of 2024: Public Sector Information Security Risk Management Guidelines*.

Efe A. (2023). A Comparison of Key Risk Management Frameworks: COSO-ERM, NIST RMF, ISO 31.000, COBIT. In *Journal of Auditing and Assurance Services* (Vol. 2023, Issue 2). http://orcid.org/0000-

Elmarady, A. A., & Rahouma, K. (2021). *Studying Cybersecurity in Civil Aviation, Including Developing and Applying Aviation Cybersecurity Risk assessment*. https://doi.org/10.1109/ACCESS.2021.3121230

ENISA. (2022). *Interoperable EU risk management framework : methodology for and assessment of interoperability among risk management frameworks and methodologies.*

Fikri, M. Al, Putra, F. A., Suryanto, Y., & Ramli, K. (2019). Risk Assessment Using NIST SP 800-30 Revision 1 and ISO 27005 Combination Technique in Profit-Based Organization: Case Study of ZZZ Information System Application in ABC Agency. *Procedia Computer Science*, *161*, 1206–1215. https://doi.org/10.1016/j.procs.2019.11.234

Ganin, A. A., Quach, P., Panwar, M., Collier, Z. A., Keisler, J. M., Marchese, D., & Linkov, I. (2020). Multicriteria Decision Framework for Cybersecurity Risk Assessment and Management. *Risk Analysis*, *40*(1), 183–199. https://doi.org/10.1111/risa.12891

ISO/IEC 27005. (2022). *Information security, cybersecurity and privacy protection-Guidance on managing information security risks*.

ISO/IEC TS 27100. (2020). *ISO/IEC TS 27100:2020, Information technology — Cybersecurity — Overview and concepts*.

Jung, D., Shin, J., Lee, C., Kwon, K., & Seo, J. T. (2023). Cyber Security Controls in Nuclear Power Plant by Technical Assessment Methodology. *IEEE Access*, *11*, 15229–15241. https://doi.org/10.1109/ACCESS.2023.3244991

Kalinin, M., Krundyshev, V., & Zegzhda, P. (2021). Cybersecurity risk assessment in smart city infrastructures. *Machines*, *9*(4). https://doi.org/10.3390/machines9040078

Krishtanosov, V. B., & Brovko, N. A. (2023). Conceptual-Analytical Approaches to Threats in the Digital Economy. *AlterEconomics*, *20*(1), 216–245. https://doi.org/10.31063/AlterEconomics/2023.20-1.11

Lau, P., Wang, L., Liu, Z., Wei, W., & Ten, C.-W. (2021). A Coalitional Cyber-Insurance Design Considering Power System Reliability and Cyber Vulnerability. *IEEE Transactions on Power Systems*, *36*(6), 5512–5524. https://doi.org/10.1109/TPWRS.2021.3078730

Liu, Z., Zheng, R., Lu, W., & Xu, S. (2021). Using Event-Based Method to Estimate Cybersecurity Equilibrium. *IEEE/CAA Journal of Automatica Sinica*, *8*(2), 455–467. https://doi.org/10.1109/JAS.2020.1003527

Mathias Ekstedt, Zeeshan Afzal, Preetam Mukherjee, Simao Hacks, & Robert Lagerstrom. (2023). *Yet another cybersecurity risk assessment framework | Enhanced Reader*.

Melaku, H. M. (2023). Context-Based and Adaptive Cybersecurity Risk Management Framework. *Risks*, *11*(6). https://doi.org/10.3390/risks11060101

National Cybersecurity Agency. (2020). *Malaysia Cyber Security Strategy 2020-2024*.

NIST SP 800-30. (2012). *NIST SP 800-30:Guide for conducting risk assessments*. https://doi.org/10.6028/NIST.SP.800-30r1

NIST SP 800-37. (2018). *NIST 800-37 : Risk management framework for information systems and organizations*. https://doi.org/10.6028/NIST.SP.800-37r2

Putra, A. P., & Soewito, B. (2023). Integrated Methodology for Information Security Risk Management using ISO 27005:2018 and NIST SP 800-30 for Insurance Sector. *International Journal of Advanced Computer Science and Applications*, *14*(4). https://doi.org/10.14569/IJACSA.2023.0140468

Rea-Guaman, A. M., Mejía, J., San Feliu, T., & Calvo-Manzano, J. A. (2020). AVARCIBER: a framework for assessing cybersecurity risks. *Cluster Computing*, *23*(3), 1827–1843. https://doi.org/10.1007/s10586-019-03034-9

Sukumar, A., Mahdiraji, H. A., & Jafari-Sadeghi, V. (2023). Cyber risk assessment in small and medium-sized enterprises: A multilevel decision-making approach for small e-tailors. *Risk Analysis*, *43*(10), 2082–2098. https://doi.org/10.1111/risa.14092

Ukwandu, E., Farah, M. A. Ben, Hindy, H., Brosset, D., Kavallieros, D., Atkinson, R., Tachtatzis, C., Bures, M., Andonovic, I., & Bellekens, X. (2020). A Review

of Cyber-Ranges and Test-Beds: Current and Future Trends. *Sensors*, *20*(24), 7148. https://doi.org/10.3390/s20247148

Whitman, M. E., & Mattord, H. J. (2018). *Management Of Information Security* (Sixth Edition).

Zhang, Z., Hamadi, H. Al, Damiani, E., Yeun, C. Y., & Taher, F. (2022). Explainable Artificial Intelligence Applications in Cyber Security: State-of-the-Art in Research. *IEEE-Access*, *10*, 93104–93139. https://doi.org/10.1109/ACCESS.2022.3204051