



UNIVERSITY OF WEST ATTICA

SCHOOL OF ENGINEERING  
DEPARTMENT OF INFORMATICS AND COMPUTER ENGINEERING  
MSC IN CYBERSECURITY

---

**Analysis of framework methods and software tools for information  
security risk management**

---

*Master Thesis*  
*of*  
*Sampanis I. Spiridon*

**Supervisor :** Professor Gritzalis Stefanos

**Examination Committee:** Professor Gritzalis Stefanos  
Professor Yannakopoulos Panayotis  
Adjunct Professor Kogias Dimitrios

Athens, 27 April 2024

This page is intentionally blank.

**Analysis of framework methods and software tools for information  
security risk management**

*Sampanis I. Spiridon*

cscyb21028

**Supervisor :**

**Professor Gritzalis Stefanos**

**Examination Committee:**

**Professor Yannakopoulos Panayotis**

**Adjunct Professor Kogias Dimitrios**

**Examination Date 27/04/2024**

**«DECLARATION OF NON-PLAGIARISM AND ASSUMPTION OF PERSONAL RESPONSIBILITY»**

“I am the author of this thesis and I declare that any help I had in its preparation is fully acknowledged and mentioned in the thesis. I have also cited the sources from which I have made use of data, ideas, or words, whether quoted verbatim or paraphrased. I also certify that this thesis was prepared by me personally specifically for this master’s thesis.””

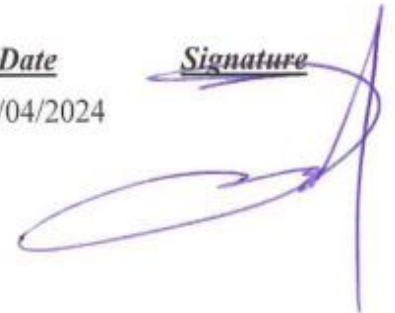
**Full Name of Writer**

Sampanis I. Spiridon

**Date**

27/04/2024

**Signature**

A handwritten signature in blue ink, consisting of a large, stylized loop followed by a vertical line that extends upwards and then curves back down to the right.

## *Acknowledgements*

I would like to express my deepest gratitude to my supervisor, Professor Gritzalis Stefanos, for their invaluable guidance, unwavering support, and endless patience throughout the duration of this research. Their expertise, encouragement, and constructive feedback have been instrumental in shaping this thesis and my academic journey.

I am indebted to the members of my thesis committee, Professor Panayotis Yannakopoulos and Professor Dimitrios Kogias, for their insightful comments, valuable suggestions, and critical evaluation of this work. Their expertise and commitment to academic excellence have greatly enriched the quality of this thesis.

I extend my sincere appreciation to University of West Attica for providing me with the resources and facilities essential for conducting this research. I am grateful for the opportunity to pursue my academic aspirations in such a supportive environment.

I would like to thank my colleagues and friends for their encouragement, camaraderie, and understanding during the ups and downs of the thesis-writing process. Their moral support and shared experiences have been a source of strength and inspiration.

My heartfelt gratitude goes to my family for their unconditional love, unwavering belief in my abilities, and constant encouragement. Their sacrifices and encouragement have been the driving force behind my academic pursuits, and I am forever grateful for their unwavering support.



# *Preface*

Information security has become a critical concern in today's interconnected world, where the proliferation of digital technologies has brought unprecedented opportunities as well as risks. As organizations strive to protect their valuable assets from evolving cyber threats, the need for effective risk management strategies has never been more pronounced.

This master thesis delves into the intricate domain of information security risk management, with a specific focus on analyzing framework methods and software tools. The aim of this research is to provide a comprehensive overview of the existing approaches to information security risk management, evaluate their strengths and limitations, and identify emerging trends and best practices in the field.

The journey of researching and writing this thesis has been both challenging and rewarding. It has been a privilege to explore the depths of information security risk management under the guidance of my esteemed supervisor, Professor Gritzalis Stefanos whose expertise and insights have been invaluable throughout this endeavor.

I am also indebted to the numerous authors, researchers, and practitioners whose pioneering work and contributions form the foundation of this study. Their insights and innovations have served as constant sources of inspiration and enlightenment.

It is my sincere hope that this thesis contributes to the advancement of knowledge in the field of information security risk management and serves as a valuable resource for researchers, practitioners, and organizations striving to safeguard their digital assets in an increasingly complex and interconnected world.

© 2024

of

Sampanis I. Spiridon

Department of Informatics and Computer Engineering

University of West Attica

This page is intentionally blank.



## Table of Contents

<b>Acknowledgements</b> .....	<b>i</b>
<b>Preface</b> .....	<b>ii</b>
<b>Abstract</b> .....	<b>iii</b>
<b>Περίληψη (greek translation)</b> .....	<b>iv</b>
<b>1 Introduction</b> .....	<b>1</b>
1.1 Problem Definition and Framework Analysis .....	1
1.2 Scope of Thesis.....	2
1.3 Overview of the Chapters .....	2
<b>2 Theoretical Background and Related Work</b> .....	<b>5</b>
2.1 Information Security Risk Management: Definition, Importance and Principles .....	5
2.1.1 <i>Definition and Importance</i> .....	5
2.1.2 <i>Process of Information Security Risk Management</i> .....	7
2.1.3 <i>Methods for managing risks in Information Security</i> .....	8
2.2 Literature Review: Current State of Research .....	11
2.2.1 <i>Studies on Information Security Risk Management</i> .....	11
2.2.2 <i>Studies on Risk Management Frameworks and Methodologies</i> .....	12
2.2.3 <i>Studies on Risk Management Tools</i> .....	13
2.3 Gap Analysis: Research Questions .....	15
2.3.1 <i>Research Questions</i> .....	15
2.3.2 <i>Resolving the research questions</i> .....	15
<b>3 Identified Risk Management Frameworks and Methodologies</b> .....	<b>17</b>
3.1 ISO 27005:2022.....	17
3.2 NIST SP 800-37.....	21
3.3 OCTAVE .....	25
3.4 FAIR .....	27
<b>4 Identified Risk Management Software Tools</b> .....	<b>32</b>
4.1 Microsoft Security Assessment Tool 4.0.....	32
4.2 CORAS .....	37
4.3 SimpleRisk.....	41
4.4 SAP GRC.....	45
<b>5 Comparison Evaluation of Framework Methods and Software Tools</b> .....	<b>51</b>

5.1	Criteria for comparison evaluation .....	51
5.1.1	Scalability.....	51
5.1.2	User-Friendliness.....	52
5.1.3	Alignment with Compliance Requirements .....	53
5.1.4	Features .....	53
5.1.5	Resource Optimization.....	54
5.2	Evaluation analysis .....	55
5.2.1	Evaluation analysis of selected ISRM Frameworks.....	55
5.2.2	Evaluation analysis of selected ISRM Tools .....	58
5.3	Discussion.....	61
<b>6</b>	<b>Conclusion and Recommendations .....</b>	<b>66</b>
6.1	Summary of Findings .....	66
6.2	Recommendations.....	67
6.3	Limitations and Future Expansion.....	68
	<b>References .....</b>	<b>69</b>

## List of Figures

<b>Figure 2.1:</b> Process of ISRM (IT Governance UK, 2023) .....	8
<b>Figure 2.2:</b> Methods for managing risks in Information Security (PracticeTests Academy, 2023) .	9
<b>Figure 3.1:</b> Process of Risk Assessment by ISO 27005:2022 framework (ISO, 2022) .....	18
<b>Figure 3.2:</b> Benefits of ISO/IEC 27005 (PECB, 2023).....	20
<b>Figure 3.3:</b> Process of Risk Assessment by NIST SP 800-37 RMF (Cuelogic, 2019) .....	22
<b>Figure 3.4:</b> Process of Risk Assessment by OCTAVE framework (CERT, 2008).....	25
<b>Figure 3.5:</b> Process of Risk Assessment by FAIR framework (Balbix, 2022) .....	28
<b>Figure 3.6:</b> Risk decomposition by FAIR methodology (FAIR Institute, 2023) .....	29
<b>Figure 4.1:</b> MSAT setup for the organization (Microsoft, 2009) .....	33
<b>Figure 4.2:</b> MSAT risk assessment process (Microsoft, 2009).....	33
<b>Figure 4.3:</b> MSAT assessment report produced by risk analysis (Microsoft, 2009) .....	34
<b>Figure 4.4:</b> User-Interface (UI) of CORAS tool (CORAS, 2023) .....	38
<b>Figure 4.5:</b> CORAS asset diagram (Solhaug and Stølen, 2014) .....	38
<b>Figure 4.6:</b> CORAS threat diagram (Solhaug and Stølen, 2014).....	39
<b>Figure 4.7:</b> Decomposed threat scenario using high-level CORAS (Solhaug and Stølen, 2014)...	39
<b>Figure 4.8:</b> Risk management (Insert a new risk) of SimpleRisk tool (SimpleRisk, 2020) .....	43
<b>Figure 4.9:</b> Plan mitigation on SimpleRisk tool(SimpleRisk, 2020) .....	43
<b>Figure 4.10:</b> Reporting feature of SimpleRisk tool (SimpleRisk, 2020).....	44
<b>Figure 4.11:</b> Dynamic reporting on SimpleRisk tool (SimpleRisk, 2020) .....	44
<b>Figure 4.12:</b> SAP GRC capabilities (JNC Consultancy, 2023) .....	46
<b>Figure 4.13:</b> Risk analysis by SAP GRC tool (SAP, 2023) .....	47
<b>Figure 4.14:</b> Risk assessment reporting by SAP GRC tool (SAP, 2023) .....	48
<b>Figure 4.15:</b> Risk management and reporting by SAP GRC (Winterhawk, 2023).....	48

## Acronyms

ISRM	Information Security Risk Management
IT	Infrastructure Technology
AI	Artificial Intelligence
RMF	Risk Management Framework
ISMS	Information Security Management System
ISO	International Organization for Standardization
IEC	International Electrotechnical Commission
GDPR	General Data Protection Regulation
SDLC	Systems Development Life Cycle
HIPAA	Health Insurance Portability and Accountability
GRC	Governance, Risk Management, Compliance
SAP	System Applications and Products

## *Abstract*

With cybersecurity threats on the rise, organizations must implement robust information security risk management (ISRM) measures. This necessitates choosing appropriate ISRM frameworks and tools aligned to their specific requirements and constraints. However, the suitability of these solutions across diverse organizational contexts remains inadequately analyzed. Therefore, this research conducts a comparative evaluation of widely adopted ISRM frameworks including ISO 27005:2022, NIST SP 800-37, OCTAVE and FAIR along with software tools like MSAT 4.0, CORAS, SimpleRisk and SAP GRC.

The study assesses these options across various criteria proposed in this study. The findings reveal those comprehensive solutions like ISO 27005:2022 and SAP GRC suit large enterprises but can overwhelm smaller entities for whom OCTAVE or SimpleRisk may be preferable. Highly regulated industries benefit from ISO and NIST's compliance capabilities whereas modular tools like MSAT and CORAS provide agility. Ultimately, organizations must weigh criteria based on their maturity, strategic needs and risk environments to determine optimal frameworks and tools.

The key contribution is providing a robust comparative analysis to inform ISRM decision-making. It concludes that regular re-evaluation is essential given the dynamic threat landscape. This helps maintain selections aligned to evolving organizational contexts. Further case studies and assessments of emerging solutions can expand insights. Overall, this research enables organizations to make strategic ISRM choices for long-term cyber resilience.

**Keywords:** *Risk Management, Information Security, Methods and Tools, Evaluation, Comparative Analysis, Decision-Making, Cyber Resilience*

## Περίληψη

Με τις απειλές για την ασφάλεια στον κυβερνοχώρο να αυξάνονται, οι οργανισμοί πρέπει να εφαρμόζουν ισχυρά μέτρα διαχείρισης κινδύνου ασφάλειας πληροφοριών (ISRM). Αυτό προϋποθέτει την επιλογή κατάλληλων πλαισίων και εργαλείων ευθυγραμμισμένων με τις συγκεκριμένες απαιτήσεις και τους περιορισμούς τους. Ωστόσο, η καταλληλότητα αυτών των λύσεων σε διάφορα οργανωτικά πλαίσια παραμένει ανεπαρκώς αναλυμένη. Ως εκ τούτου, η παρούσα έρευνα διενεργεί συγκριτική αξιολόγηση των ευρέως υιοθετημένων πλαισίων, συμπεριλαμβανομένων των ISO 27005:2022, NIST SP 800-37, OCTAVE και FAIR, μαζί με εργαλεία λογισμικού όπως τα MSAT 4.0, CORAS, SimpleRisk και SAP GRC.

Η μελέτη αξιολογεί αυτές τις επιλογές με βάση διάφορα κριτήρια που προτείνονται στην παρούσα μελέτη. Τα ευρήματα αποκαλύπτουν ότι οι ολοκληρωμένες λύσεις όπως το ISO 27005:2022 και το SAP GRC ταιριάζουν σε μεγάλες επιχειρήσεις, αλλά μπορούν να επιβαρύνουν τις μικρότερες οντότητες για τις οποίες μπορεί να είναι προτιμότερες οι λύσεις OCTAVE ή SimpleRisk. Οι βιομηχανίες με υψηλή ρύθμιση επωφελούνται από τις δυνατότητες συμμόρφωσης του ISO και του NIST, ενώ τα αρθρωτά εργαλεία όπως το MSAT και το CORAS παρέχουν ευελιξία. Τελικά, οι οργανισμοί πρέπει να σταθμίσουν τα κριτήρια με βάση την ωριμότητα, τις στρατηγικές ανάγκες και τα περιβάλλοντα κινδύνου για να καθορίσουν τα βέλτιστα πλαίσια και εργαλεία.

Η βασική συμβολή είναι η παροχή μιας ισχυρής συγκριτικής ανάλυσης για την ενημέρωση της λήψης αποφάσεων. Καταλήγει στο συμπέρασμα ότι η τακτική επαναξιολόγηση είναι απαραίτητη, δεδομένου του δυναμικού τοπίου των απειλών. Αυτό συμβάλλει στη διατήρηση των επιλογών ευθυγραμμισμένων με τα εξελισσόμενα οργανωτικά πλαίσια. Περαιτέρω μελέτες περιπτώσεων και αξιολογήσεις αναδυόμενων λύσεων μπορούν να διευρύνουν τις γνώσεις. Συνολικά, η παρούσα έρευνα επιτρέπει στους οργανισμούς να κάνουν στρατηγικές επιλογές στην διαχείριση κινδύνου ασφάλειας πληροφοριών για μακροπρόθεσμη ανθεκτικότητα στον κυβερνοχώρο.

**Λέξεις Κλειδιά:** Διαχείριση Κινδύνων, Ασφάλεια Πληροφοριών, Μέθοδοι και Εργαλεία, Αξιολόγηση, Συγκριτική Ανάλυση, Λήψη Αποφάσεων, Ανθεκτικότητα στον Κυβερνοχώρο

# 1

## *Introduction*

### *1.1 Problem Definition and Framework Analysis*

The rapid advancement of technology and the increasing interconnectedness of digital systems have brought about numerous benefits, but they have also introduced significant risks to the security of organizations' information assets. Cyber threats, such as data breaches, unauthorized access, malware attacks and social engineering, have become increasingly sophisticated and pose significant challenges to businesses, governments and individuals worldwide.

Information security risk management (ISRM) plays a crucial role in mitigating these risks and protecting sensitive data, intellectual property, customer information and critical infrastructure. Organizations need to establish robust frameworks and implement effective software tools to proactively identify, assess and manage risks to their information assets.

However, selecting the right frameworks, methodologies and software tools for information security management is not a straightforward task. The evolving threat landscape, industry-specific requirements, compliance regulations and resource limitations further complicate the decision-making process. Organizations often struggle to evaluate and compare the available options, resulting in suboptimal choices or a lack of alignment with their specific needs and goals.

Furthermore, while there are several well-established frameworks and methodologies for information security management, including ISO 27005:2022, NIST SP 800-37, CORAS, FAIR and others, there is a lack of comprehensive analysis and evaluation of these frameworks in a comparative context. Similarly, although there is a wide range of software tools available to assist organizations in implementing and automating their risk management processes, organizations often face challenges in selecting the most suitable tool for their requirements due to a lack of comprehensive analysis and understanding of the available options.

Therefore, the problem addressed in this thesis is the necessity for a thorough analysis of framework methods and software tools for information security management. By conducting a comprehensive evaluation and comparison of these frameworks and tools, organizations can gain valuable insights and make informed decisions regarding their adoption and implementation strategies. This research aims to bridge the gap by providing an in-depth examination of various frameworks, methodologies and software tools, considering their strengths, weaknesses, applicability and suitability for different organizational contexts.

## ***1.2 Scope of Thesis***

This thesis aims to present, compare and evaluate frameworks, methods and tools for information security management. The focus will be on providing a comprehensive analysis of these frameworks, methodologies and software tools to support organizations in making informed decisions regarding their adoption and implementation strategies. The thesis will encompass some of the well-established information security management frameworks and methods like ISO 27005:2022, NIST SP 800-37, OCTAVE and FAIR. Each framework will be analyzed in terms of its purpose, key components, strengths, weaknesses and applicability. Additionally, the thesis will also include an analysis of software tools designed to support information security management processes such as Microsoft Security Assessment Tool 4.0, CORAS, SimpleRisk and SAP GRC. Comparative analysis for both frameworks and methods and tools will be performed to highlight the strengths and limitations of the forementioned frameworks / tools, enabling organizations to select the most suitable tool for their information security management requirements.

The scope of this thesis will cover a broad spectrum of frameworks, methodologies and software tools for information security management. The focus will be on their analysis, comparison and evaluation, providing valuable insights into their respective strengths, weaknesses and applicability. The thesis will not only present these frameworks, methodologies and tools but also provide recommendations for organizations seeking to implement effective information security management strategies.

## ***1.3 Overview of the Chapters***

The thesis will be structured into several chapters, each serving a specific purpose and contributing to the overall investigation of frameworks, methodologies and tools for information security management. Here is an overview of the proposed chapter structure:



## **Chapter 1: Introduction**

This introductory chapter provides an overview of the research topic, problem definition and the scope of the thesis. It highlights the significance of effective information security management and sets the stage for the subsequent chapters.

## **Chapter 2: Theoretical Background and Related Work**

Chapter 2 delves into the theoretical foundations and related work of information security management. It provides a comprehensive overview of the concepts, principles and best practices associated with managing information security risks. The chapter also reviews existing literature, studies and research related to frameworks, methodologies and tools for information security management.

## **Chapter 3: Analysis of Frameworks and Methodologies**

Chapter 3 focuses on the analysis of various frameworks and methodologies for information security management. Each framework is analyzed in terms of its purpose, key components, strengths, weaknesses and applicability.

## **Chapter 4: Evaluation of Risk Management Tools**

Chapter 4 centers on the evaluation of software tools designed to support information security management processes. Each tool is assessed based on its features, functionalities, usability, integration capabilities and cost.

## **Chapter 5: Comparative Analysis and Synthesis**

Chapter 5 provides a comparative analysis and synthesis of the frameworks, methodologies and tools discussed in the previous chapters. It explores the commonalities, differences and complementary aspects among the frameworks and tools.

## **Chapter 6: Conclusion and Recommendations**

The final chapter summarizes the key findings from the research and presents conclusions, it offers practical recommendations for organizations seeking to implement

information security management strategies and discusses the limitations of the research and suggests potential areas for future exploration or improvement.

# 2

## *Theoretical Background and Related Work*

In today's digital landscape, organizations face an ever-growing array of cyber threats and security challenges. The safeguarding of valuable information assets is of paramount importance to ensure business continuity, protect sensitive data and maintain trust among stakeholders. Information security management is the discipline that enables organizations to systematically identify, assess and mitigate risks to their information assets, ensuring their confidentiality, integrity and availability. This chapter delves into the theoretical background and related work of information security management, establishing the necessary foundation for the subsequent analysis and evaluation of frameworks, methodologies and tools.

### *2.1 Information Security Risk Management: Definition, Importance and Principles*

#### *2.1.1 Definition and Importance*

Information security risk management (ISRM) refers to the **ROC**. It involves understanding the potential vulnerabilities and threats that could impact the confidentiality, integrity and availability of sensitive information and implementing appropriate measures to minimize or mitigate those risks (ENISA, 2023; Hopkin 2018).

The importance of ISRM cannot be overstated, especially in today's digital world where information is one of the most valuable assets a business possesses. With the increasing reliance on digital systems, the potential for data breaches, cyber-attacks and other forms of unauthorized access has escalated. Incidents like these can lead to significant financial losses, damage to reputation, legal repercussions and loss of customer trust. Furthermore, regulatory bodies across different sectors are increasingly implementing stringent rules regarding data protection and privacy, making effective ISM not just a strategic necessity but also a legal requirement.

At the heart of ISM are three core principles:

- **Confidentiality:** This principle ensures that sensitive information is only accessible to those authorized to view it. Mechanisms to uphold confidentiality include user authentication, encryption, access controls and secure network design.
- **Integrity:** This principle involves maintaining and assuring the accuracy and consistency of data over its entire life cycle. It ensures that information is not altered in transit and that it is protected from unauthorized changes, whether malicious or accidental.
- **Availability:** This principle ensures that information is accessible to authorized individuals whenever needed. Redundancy, disaster recovery planning and secure, efficient network architecture are measures used to guarantee the availability of systems and data.

Risk management is a structured approach to identifying, assessing and addressing potential threats or risks that could impact an organization's operations, objectives, or reputation (Hopkin 2018). It is a fundamental part of strategic management and a cornerstone of good corporate governance. Risk management plays a crucial role in an organization's information security strategy for several reasons:

- **Prioritization of Resources:** By identifying and prioritizing risks, organizations can better allocate their limited resources to manage the most significant risks. Without proper risk management, organizations may end up spending a lot of resources protecting against low-impact threats while neglecting more serious ones.
- **Compliance with Regulations:** Many industries are subject to regulations that require them to manage risks to their information systems. Proper risk management can help organizations meet these compliance requirements and avoid fines or penalties.
- **Preventing Data Breaches and Attacks:** By identifying vulnerabilities and potential threats, risk management can help prevent data breaches and cyberattacks before they occur.
- **Business Continuity:** By managing risks, organizations can ensure that they can continue their operations even when a risk event occurs. This is especially important in today's world where organizations are heavily reliant on their information systems.

### 2.1.2 Process of Information Security Risk Management

Effective ISRM involves a coordinated approach that integrates these principles into every aspect of an organization's operations, from its business processes and human resources practices to its IT infrastructure and software systems. The aim is to create a resilient environment that can withstand threats, adapt to changing risk landscapes and recover quickly from security incidents.

The primary goal of information security risk management is to enable organizations to make informed decisions and allocate resources effectively to protect their valuable information assets. By proactively managing risks, organizations can reduce the likelihood and impact of security incidents, ensure compliance with relevant regulations and maintain the trust of their stakeholders.

The process of ISRM typically involves the following key steps (Rapid7, 2023), which are presented in Figure 2.1:

- **Risk Identification:** This step involves identifying and documenting the potential risks and threats that could affect the organization's information assets. This may include conducting risk assessments, threat modeling and vulnerability scanning to identify potential vulnerabilities in systems, networks and processes.
- **Risk Assessment:** Once risks are identified, they need to be assessed in terms of their likelihood and potential impact on the organization. This involves evaluating the probability of a risk occurring and the magnitude of its potential consequences. Risk assessment methods may vary depending on the organization's industry, size and specific requirements.
- **Risk Evaluation:** In this step, organizations evaluate the identified risks based on predefined criteria or risk tolerance levels. Risks are prioritized based on their potential impact, likelihood and other factors such as legal or regulatory requirements.
- **Risk Treatment:** After evaluating the risks, organizations develop and implement appropriate risk treatment strategies. These strategies may include risk avoidance, risk mitigation, risk transfer, or risk acceptance. Risk mitigation measures can involve implementing technical controls, adopting security best practices, developing policies and procedures and providing security awareness training.
- **Risk Monitoring and Review:** Risk management is an ongoing process and it requires continuous monitoring and review to ensure that the implemented controls and strategies remain effective and aligned with the evolving threat landscape. Regular assessments and audits are conducted to identify new risks, evaluate the effectiveness of existing controls and make necessary adjustments.

- **Risk Communication and Reporting:** Effective communication of risks and their status is essential to ensure that stakeholders, including management, employees and external parties, are aware of the risks and understand the measures in place to manage them. Regular reporting on risk management activities, incident and mitigation efforts helps facilitate decision-making and accountability. Identified Risk Management Frameworks and Methodologies



*Figure 2.1: Process of ISRM (IT Governance UK, 2023)*

### **2.1.3 Methods for managing risks in Information Security**

In the ever-evolving landscape of cybersecurity, risk management plays a vital role in safeguarding information assets. Managing risks in information security requires a multifaceted approach that combines various methods and strategies. The selection of these methods often depends on organizational needs, the nature of the threats, regulatory requirements and technological infrastructure. This section will explore some of the prominent methods utilized for managing risks in information security, including Forensic Analysis, Malware Analysis, Penetration Testing, Software Security, Digital Resilience and Frameworks (PracticeTests Academy, 2023) as shown in Figure 2.2.

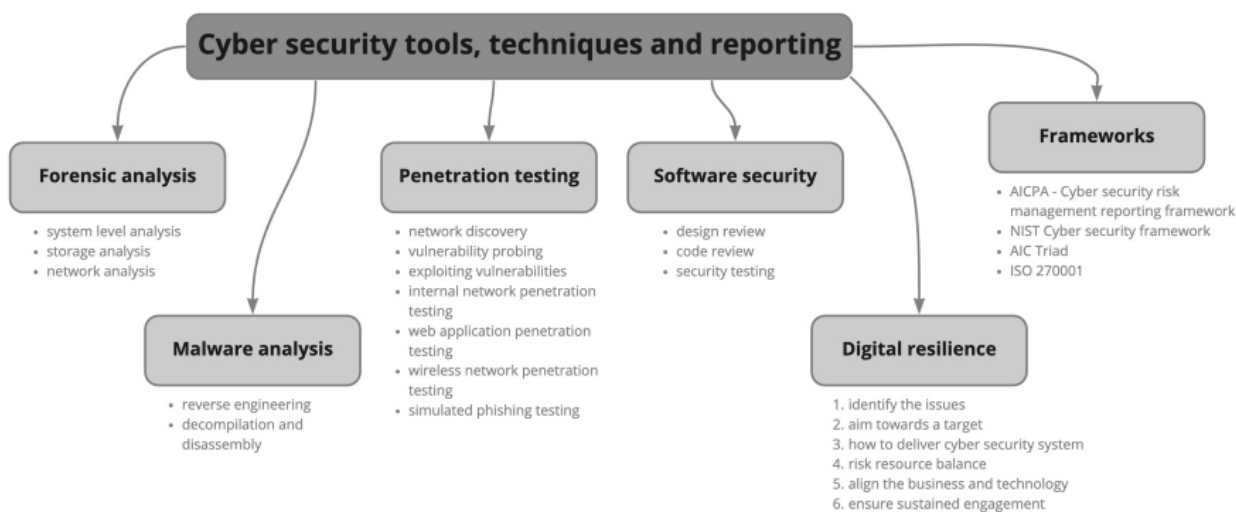


Figure 2.2: Methods for managing risks in Information Security (PracticeTests Academy, 2023)

## Forensic Analysis

Forensic analysis is an integral part of information security, involving the meticulous collection, preservation and analysis of evidence related to cyber incidents. It's applied in the investigation of data breaches, fraud and other cybercrimes, providing detailed insights into attack vectors and facilitating legal action. While offering valuable prevention strategies, forensic analysis may be time-consuming and requires specialized skills. It may also face challenges with encryption or data loss.

## Malware Analysis

Malware analysis examines the functionality, origin and impact of malicious software. This process is crucial in understanding how malware operates, allowing security professionals to develop countermeasures and protections. It contributes to early detection and mitigation of malware-based threats. However, evolving malware techniques can render analysis complex, necessitating specialized tools and expertise.

## Penetration Testing

Penetration testing, or pen testing, simulates cyberattacks on systems to discover vulnerabilities that could be exploited by malicious entities. This proactive approach identifies weak points in

security systems, applications and networks. Though effective in finding vulnerabilities, the success of penetration testing is tied to its scope and there can be potential disruptions to normal operations.

### **Software Security**

Software security emphasizes preventive measures during software development to avert vulnerabilities leading to security breaches. By embedding security within the development lifecycle, it helps in building secure applications. While reducing risks associated with software flaws, integrating these measures into the development process might slow down timelines.

### **Digital Resilience**

Digital resilience refers to an organization's robustness in withstanding and recovering from cyber incidents. Ensuring continued operation during and after a cyber incident, this approach enhances the ability to bounce back from attacks, thus minimizing downtime and financial losses. However, achieving digital resilience requires comprehensive planning and investment in resilient technologies.

### **Frameworks**

Frameworks such as ISO 27005:2022, NIST SP 800-37 and others offer structured approaches to risk management in information security. These guide risk assessment, mitigation and overall management processes, providing a systematic approach based on industry standards. While highly beneficial, these frameworks may need customization to align with specific organizational contexts.

The blend of these methods forms the cornerstone of a strong security posture. Through proactive testing, secure development, incident response, adherence to established frameworks and resilience strategies, organizations can build comprehensive defences against cybersecurity threats. The effective integration of these various methods requires strategic alignment with the organization's specific threats, regulations and business objectives, underlining the importance of a dynamic and adaptable approach to risk management in information security.



## ***2.2 Literature Review: Current State of Research***

### ***2.2.1 Studies on Information Security Risk Management***

In recent years, the realm of ISRM has seen significant attention in the academic field due to the proliferation of digital technologies and increasing cybersecurity threats. Recognized as a key business activity, ISRM involves the process of identifying, assessing and managing risks associated with an organization's information assets (Dhilon & Backhouse, 2001).

Von Solms R. and B. (2004) made a critical contribution by emphasizing the role of top management in ISRM. They highlighted that without the commitment and active participation of top-level management, effective risk management cannot be achieved. Their study demonstrated that ISRM should not be confined to IT departments but should be an organization-wide responsibility that aligns with overall business objectives.

Shedding light on the human aspect of ISRM, Albrechtsen and Hovden (2010) explored the impact of cultural and behavioural factors on the effectiveness of ISRM. They found that fostering a security-conscious culture is vital for reducing the likelihood of security breaches. In their study, they presented an intervention method to improve information security awareness and behaviour within an organization, thereby promoting a proactive rather than reactive approach to information security.

Adding to this line of research, Bulgurcu et al. (2010) carried out a study to understand the factors influencing employees' compliance with information security policies. They found that perceived benefits, organizational commitment and the seriousness of potential security risks significantly influenced employee behaviour.

On the practical side, Fernandez-Aleman et al. (2013) studied the impact of implementing GDPR compliance tools in healthcare organizations. Their work highlighted the crucial role of these tools in managing data privacy risks, showcasing how specific sectors require tailored risk management solutions.

More recent studies, like the one from Alcantara and Melgar (2016), provide a systematic review of the literature of ISMR and found that there are various approaches to risk analysis, including the use of artificial intelligence. They also mention a new approach to governance of information security called the "4th wave," which involves creating an inventory of information systems, conducting risk assessments and developing business continuity plans.

However, the process of implementing ISMR into an organization seems to be a difficult task that contains various challenges. More precisely, Bergström et al. (2019) examine information

security risk management challenges in public sector organizations. Through in-depth interviews and analysis, the study finds that there are managerial and organizational concerns that go beyond the technical aspects of security. These concerns impact the social build-up of knowledge in information security work. The study offers actionable advice to practitioners and highlights the importance of understanding actual practices in risk management.

In the modern era, with the vast amount of information and interconnectivity between IoT devices Big Data play a crucial role in the communication and cybersecurity field. Yang (2022) presents the importance of information security in the context of big data and the Internet. It emphasizes the need for effective risk management to protect the information security of big data. The article proposes a novel information security risk management model based on existing models, with a focus on risk assessment. It also introduces a fuzzy comprehensive assessment method as the core algorithm for risk assessment. The article concludes by highlighting the importance of effective risk management in ensuring the information security of big data.

Finally, the continuous evolution of Smart Cities, IoT and Artificial Intelligence (AI) can support the risk management and protection of organizations in the Infrastructure Technology (IT) sector. More specifically, reports from Deloitte (2019) present that smart cyber solutions may create predictive, actionable insights by using AI and sophisticated analytics to massive volumes of internal and external data. The AI tools may also assist in detecting and responding to attacks more quickly by monitoring the cyber environment with the speed and accuracy that only machines can deliver. By leveraging the benefits of AI, ISMR can be a very simplistic procedure, easy to implement and fast to deliver reports of information security risks.

### ***2.2.2 Studies on Risk Management Frameworks and Methodologies***

The body of literature on risk management frameworks and methodologies is expansive and continues to grow as new models and approaches are developed. These frameworks and methodologies aim to provide systematic and consistent ways of identifying, assessing and mitigating risks.

A substantial amount of research has been focused on ISO 27005:2022, which provides guidelines for information security risk management. Junior and Arima (2023) conducted a systematic literature review of ISO 27005:2022. The study identified the motivations and goals for adopting the ISO 27005:2022 standard in productive systems. The results of the review suggest that organizations adopt ISO 27005:2022 to improve processes related to information security management, risk assessment and meet legal requirements and stakeholder expectations.

The NIST Risk Management Framework (RMF) has also been a subject of intense scrutiny (NIST, 2012). Guidance on conducting risk assessments of federal information systems and organizations has been continuously studied from the scope of NIST RMF. The primary focus of the studies is cost-benefit analysis, residual risk, risk assessment, risk management, risk mitigation, security controls, threat vulnerability and various control families.

The OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation) methodology is another risk management approach extensively studied in academia. Alberts et al. (2002) proposed this methodology that emphasizes self-directed assessments, making it particularly suitable for organizations that understand their operational risks better than external parties.

More recently, studies have turned their focus to emerging methodologies such as the FAIR (Factor Analysis of Information Risk) model. This quantitative risk management framework has been lauded for its ability to provide monetary values for potential risk scenarios, aiding in the decision-making process (Freund and Jones, 2014).

The evolution on ISMR has led to the invention and utilization of new frameworks and methodologies to handle risk. However, the literature depicts that combination of two or more frameworks can lead to great results and high amount of risk avoidance. Al Fikri et al. (2019) studied the application of NIST SP 800-30 Revision 1 and ISO 27005 combination technique in risk assessment in a profit-based organization, using the case study of ZZZ Information System Application in ABC Agency. The key findings of this study include the successful implementation of the combined technique in the organization, the identification of potential risks and vulnerabilities in the information system and the recommendation of appropriate risk mitigation strategies. The study also highlights the importance of stakeholder involvement and continuous monitoring in the risk assessment process.

Overall, the academic literature reflects an ongoing debate on the comparative merits of different risk management frameworks and methodologies. The effectiveness of these models often depends on the context of the organization and the nature of the risks it faces, underlining the need for a context-specific, adaptable approach to risk management.

### ***2.2.3 Studies on Risk Management Tools***

A variety of risk management tools have been developed over the years, with their effectiveness and utility being a central focus of research. These tools are used for identifying, assessing and managing risks in the context of information security, with each tool having unique features and advantages.

Fray (2012) made significant contributions by comparing several risk management tools in terms of their efficiency. In his article, a comparative study of different risk assessment methods in information systems is presented. He developed a new formal mathematical model of risk assessment (FoMRA) and compared it with two widely used methods, MEHARI and CRAMM. The study verified the correctness of the model and provided examples of computations related to a specific unit of public administration in Poland. The article also includes a list of references for further reading on risk assessment in information systems.

In a similar vein, Karabacak and Sogukpinar (2005) developed the ISRAM (Information Security Risk Analysis Method), a tool aimed at providing a systematic and repeatable process for risk management. Their research highlighted ISRAM's ability to integrate qualitative and quantitative aspects of risk management, providing a comprehensive view of an organization's risk landscape.

In addition to comparing and developing new tools, studies have also focused on improving existing ones. For instance, the study by Zargar et al. (2013) proposed a new vulnerability assessment tool for the open-source security testing methodology manual (OSSTMM). This study highlighted the importance of continuously updating and refining tools to keep up with the evolving threat landscape.

Moreover, the implementation of these tools within organizations has been an area of study. Siponen et al. (2006) discussed the challenges related to the implementation of risk management tools, such as the need for specialized skills and the difficulty of integrating these tools with existing systems.

To efficiently create systems that contain all the important key features to manage the risks in information security is a complex task. However, there are several guidelines that support this task. NIST organization (2012) provide such guidelines to create robust systems and programs that effectively handle ISRM.

While there are numerous studies on risk management tools, the literature suggests that the effectiveness of a tool largely depends on the specific needs and context of the organization. There's an emphasis on the importance of aligning the tool with the organization's overall risk management approach and ensuring the tool is adaptable to changing conditions. As the field of risk management evolves, recent studies continue to probe into the efficacy and innovation of risk management tools. These tools play a crucial role in identifying, assessing and managing risks, thus becoming the focal point of ongoing research.

## 2.3 *Gap Analysis: Research Questions*

The field of risk management in information security is rapidly evolving. However, there exist gaps in understanding and applying various frameworks, methodologies and tools. The gap analysis aims to identify these areas, posing research questions that guide future inquiry and development.

### 2.3.1 *Research Questions*

To successfully achieve the thesis goal and present all the aforementioned frameworks, methodologies and tools the research question must be explored and presented as a practical guide to the implemented research that is presented in the next chapters. Some of the questions that are going to be answered in detail are shown below.

- How Effective are current frameworks and methodologies?
- What are the limitations of current tools?
- How are frameworks and tools aligned with emerging threats?
- How effective are the frameworks and tools to reduce the information security risks?
- What are the criteria for evaluation of the various frameworks and tools?

### 2.3.2 *Resolving the research questions*

To adequately answer the research questions the following plan will be followed:

#### **1) Presentation of Risk Management Frameworks and Methodologies:**

Connecting to the first and third research questions, a comprehensive presentation of various risk management frameworks and methodologies, such as ISO 27005:2022, NIST SP 800-37, OCTAVE and FAIR, must be explored. The focus should be on their effectiveness, adaptability ability to align with emerging threats. Comparative studies may reveal the strengths and weaknesses of these frameworks in various organizational contexts.

#### **2) Presentation of Risk Management Tools:**

Aligned with the second research question, a detailed analysis of risk management tools, including Microsoft Security Assessment Tool 4.0, CORAS, SimpleRisk and SAP GRC must be undertaken. Evaluation criteria could include usability, scalability, integration capabilities and alignment with various frameworks. A robust examination will provide insights into the limitations and potential improvements needed in these tools.

### **3) Comparison of Frameworks and Tools and Overall Evaluation**

To address all research questions holistically, a comparison evaluation across frameworks, methodologies and tools is vital. The focus should be on understanding how each fits into different scenarios, sectors and technological landscapes. A meta-analysis might provide a unified view, identifying areas where enhancements are needed and where current practices excel.

By understanding the effectiveness, limitations, alignment and customization of frameworks, methodologies and tools, the field can progress towards more robust, adaptable and context-sensitive risk management strategies. Further studies that explore these research questions in depth will contribute significantly to the understanding and application of risk management in the ever-changing cybersecurity landscape.

# 3

## *Identified Risk Management Frameworks and Methodologies*

In an era where information and cybersecurity are paramount to organizational success, the role of risk management tools and frameworks has become more critical than ever. From small enterprises to multinational corporations, the constant threats to information integrity and security necessitate the adoption of comprehensive strategies to identify, assess and mitigate risks. This section delves into four highly recognized and influential risk management frameworks that have been instrumental in shaping the landscape of ISRM, which are ISO 27005:2022, NIST SP 800-37, OCTAVE and FAIR tools.

### **3.1 ISO 27005:2022**

ISO/IEC 27005:2022 is part of the ISO 27000 series of standards, focusing on information security risk management (ISO, 2022). Established by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), it provides guidelines for risk management principles and practices in the context of an Information Security Management System (ISMS). ISO 27005:2022 is a cornerstone framework in the realm of information security risk management. A globally recognized standard, it provides a comprehensive methodology for organizations to manage information security risks, regardless of their size, nature, or industry.

The ISO 27005 risk assessment framework is crucial for organizations seeking to manage their information security risks in a systematic, consistent, and repeatable manner. By providing structured guidelines for identifying, analyzing, evaluating, treating, and monitoring risks, the framework helps organizations protect their valuable information assets, ensure business continuity, and maintain compliance with legal and regulatory requirements. Adopting ISO 27005 enhances

organizational resilience against cyber threats and other information security vulnerabilities, ultimately safeguarding both reputation and stakeholder trust.

ISO 27005:2022 is based on the process presented in Figure 3.1 and analyzed in the next paragraphs in detail. It's important to mention that ISO 27005:2022 is a risk treatment iterative process.

The process includes the following steps:

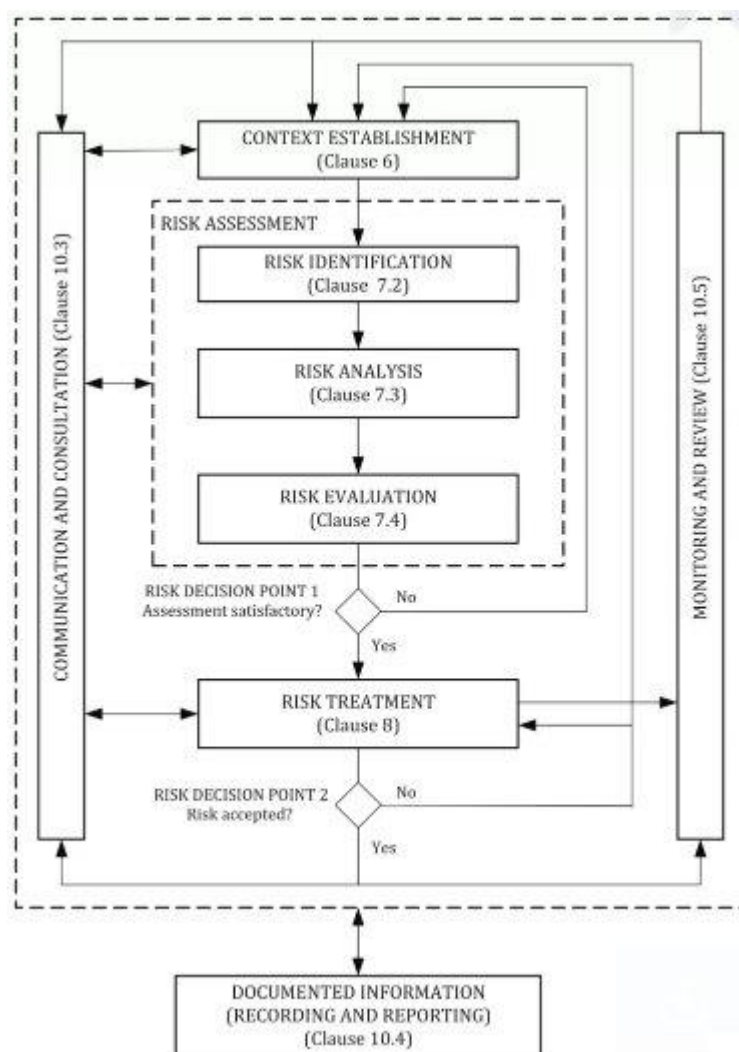


Figure 3.1: Process of Risk Assessment by ISO 27005:2022 framework (ISO, 2022)

- 1. Risk Identification:** This involves identifying and documenting potential risks to the organization's information security. Risks can be identified through various methods such as risk assessments, threat assessments, vulnerability assessments and analysis of the external and internal context.



2. **Risk Analysis:** Once risks are identified, they need to be analyzed to assess their potential impact and likelihood. This step involves evaluating the factors that contribute to the risk, including the severity of potential consequences, the likelihood of occurrence and the level of vulnerability.
3. **Risk Evaluation:** The analyzed risks are then evaluated based on predetermined risk criteria. Risk criteria are the terms of reference against which the significance of a risk is evaluated. This step helps prioritize risks based on their potential impact and the organization's risk tolerance.
4. **Risk Treatment:** After evaluating the risks, organizations need to develop and implement risk treatment plans. Risk treatment involves selecting and applying appropriate controls and measures to mitigate, transfer, accept, or avoid the identified risks. The aim is to reduce the risks to an acceptable level based on the organization's risk appetite.
5. **Risk Communication:** Effective communication is crucial throughout the risk management process. Organizations need to communicate the identified risks, their analysis and the selected risk treatment options to relevant stakeholders. Clear communication ensures that all parties involved understand the risks and their associated actions.
6. **Risk Monitoring and Review:** Risk management is an ongoing process and risks need to be monitored and reviewed regularly. This step involves tracking the effectiveness of implemented risk treatment measures, reassessing risks based on changes in the internal or external context and updating risk management plans accordingly.

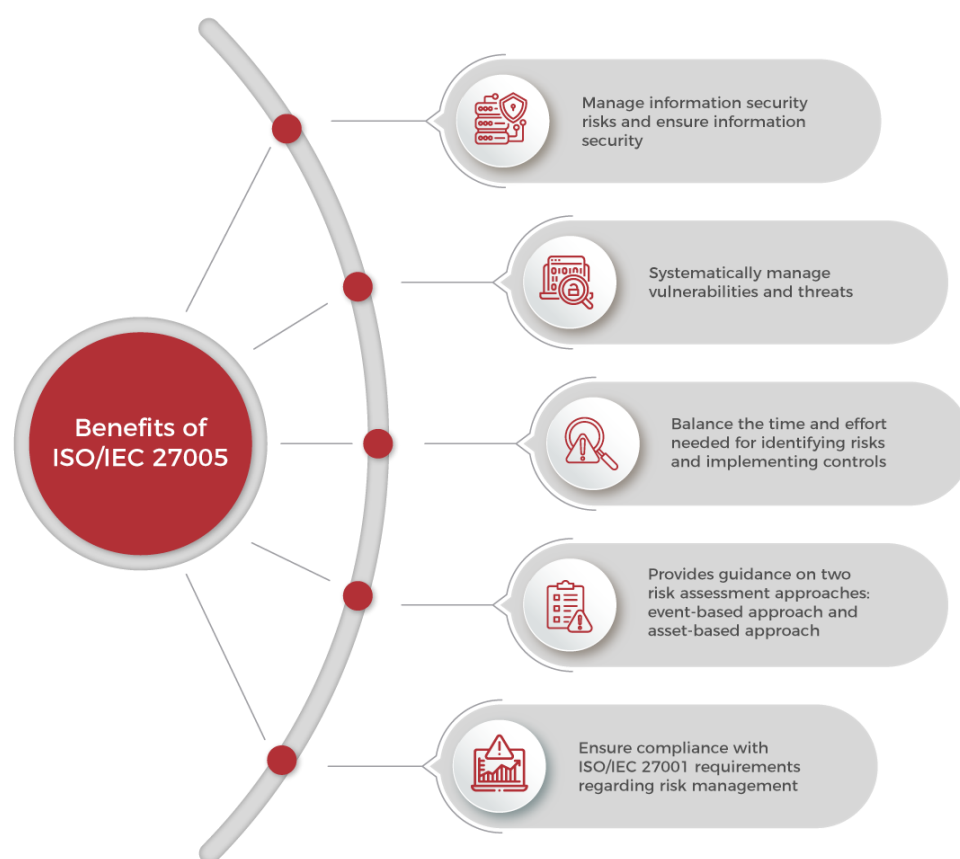
### Key Characteristics of ISO 27005:2022

- **Comprehensive Approach:** The framework offers a comprehensive approach to risk management, encompassing the full lifecycle of risk, from identification to ongoing monitoring.
- **Alignment with Other Standards:** The guidance text in ISO 27005:2022 has been aligned with the latest editions of ISO/IEC 27001 and ISO 31000 to ensure consistency and compatibility.
- **Flexibility:** Its structure allows for application across various industries, accommodating different organizational needs and regulatory requirements.
- **Focus on Continuous Improvement:** The iterative nature of the framework encourages ongoing refinement and improvement of risk management practices.

- **Risk Scenario Concepts:** The concept of risk scenarios has been introduced in ISO 27005:2022, which refers to the sequence or combination of events leading from the initial cause to the unwanted consequence. This helps organizations understand and assess risks more comprehensively.
- **Supports Regulatory Compliance:** The standard provides a systematic approach that can assist organizations in meeting regulatory and legal compliance requirements related to information security.

ISO 27005:2022 offers a multifaceted approach to information security risk management, providing tangible benefits that support both the strategic and operational needs of modern organizations. Its adaptability, comprehensiveness and focus on continuous improvement make it an asset for organizations striving to navigate the complex landscape of information security risks.

In Figure 3.2, the most significant benefits of ISO 27005:2022 framework can be shown.



**Figure 3.2:** Benefits of ISO/IEC 27005 (PECB, 2023)

The ISO 27005 framework offers a robust approach to managing information security risks, focusing on both vulnerabilities and threats in a systematic manner. By categorizing and prioritizing

risks based on their potential impact and likelihood, organizations can more effectively allocate resources to treat vulnerabilities and counteract threats. This leads to a more resilient security posture, reducing the likelihood of successful cyber-attacks or data breaches. The framework also supports both event-based and asset-based approaches to risk assessment, allowing for a multi-dimensional understanding of risks. An event-based approach looks at possible events that could cause security incidents, while an asset-based approach focuses on the information assets that could be compromised. This dual focus ensures a comprehensive and nuanced risk picture that guides more effective security controls.

Moreover, the framework helps organizations balance the time and effort required for identifying risks and implementing controls. By following a standardized approach, organizations can ensure they're not over-allocating resources on low-impact risks or under-preparing for high-impact risks. This leads to more efficient and effective security measures, without overburdening staff or exceeding budgets. One of the additional advantages of ISO 27005 is its compatibility with other standards in the ISO 27000 series, such as ISO 27001 (ISMS requirements) and ISO 27002 (guidelines for controls). This compatibility enables organizations to integrate their risk management processes smoothly across different aspects of information security, creating a cohesive and comprehensive security program that meets global standards.

### **3.2 NIST SP 800-37**

The National Institute of Standards and Technology's Special Publication 800 series (NIST SP 800-37) is a comprehensive set of guidelines and best practices designed to help organizations manage and secure their information systems. It is a set of documents that describe the United States federal government's recommendations and guidelines for information security. The series is highly respected and widely used, both within the public sector and increasingly in the private sector, to establish best practices for various areas of information security and risk management (Force, 2018).

Within this series, several documents specifically address risk management, such as NIST SP 800-30 (Guide for Conducting Risk Assessments), NIST SP 800-37 (Risk Management Framework for Information Systems and Organizations), and NIST SP 800-39 (Managing Information Security Risk). These guidelines are widely used across government agencies, the private sector, and educational institutions for establishing strong risk management processes.

The NIST Risk Management Framework (RMF) is a six-step cyclical process, which is mainly outlined in NIST SP 800-37, that begins with preparation and moves through the other six steps, which are displayed in Figure 3.3 and analyzed in the next paragraphs. These steps are designed to

be iterative and adaptable, allowing organizations to maintain security postures that are in line with evolving threats and organizational changes. The preparation phase, which is the setup of the organization's risk management strategy and guidelines, involves laying the foundation for effective risk management across the organization. It is important to mention that each of these steps is iterative and dynamic, allowing for feedback and adjustments as new vulnerabilities, threats, or business requirements emerge. By



Figure 3.3: Process of Risk Assessment by NIST SP 800-37 RMF (Cuelogic, 2019)

The six-step process of this framework is described below:

- 1. Categorize Information Systems (Step 1):** During this step, the organization categorizes its information systems and the data it processes. This categorization is often based on impact levels such as low, moderate, or high, and is essential for identifying what kind of security controls are necessary.
- 2. Select Security Controls (Step 2):** Based on the categorization, security controls are selected to mitigate the identified risks. These controls are picked from NIST SP 800-53, which provides an exhaustive list of security controls categorized by family (e.g., Access Control, Audit and Accountability).

- 3. Implement Security Controls (Step 3):** After the controls are selected, the next step is to implement them. This could involve a variety of tasks, such as configuring hardware or software, changing administrative practices, or educating users. Documentation of the implementation is crucial for later steps.
- 4. Assess Security Controls (Step 4):** Once the controls are in place, they must be tested to ensure they are functioning as expected. This usually involves developing and implementing assessment plans to evaluate the controls. The results of these assessments are then reported for decision-making purposes.
- 5. Authorize Information Systems (Step 5):** After the assessment, a senior official reviews all the documentation and assessments to decide whether the risks are at an acceptable level to grant system authorization. If the risks are too high, it's back to the drawing board, otherwise, the system is authorized for operation.
- 6. Monitor Security Controls (Step 6):** The final step in the RMF is continuous monitoring. Security is a moving target, and the risk environment can change quickly. Regular audits, reviews, and assessments are necessary to ensure that the controls remain effective and up to date. Any changes or compromises are fed back into the initial steps of the RMF to update the system's risk posture.

### Key Characteristics

NIST SP 800-37 provide a wide variety of characteristics, which makes the framework widely respected and adopted for risk management in the realm of information security. Its comprehensive yet flexible nature allows organizations to tailor their risk management processes in a manner that best suits their specific needs while still adhering to recognized best practices.

- **Comprehensive Lifecycle Approach:** The RMF offers a full lifecycle approach to risk management. It starts from the initial stages of system planning and extends into the ongoing operations and even decommissioning. The framework is not a one-off or linear process but is intended to be cyclical, to adapt to changing environments and requirements.
- **Customizability:** NIST SP 800-37 is inherently flexible and allows for customization to fit organizational needs, priorities, and resources. Organizations can adapt the framework to their specific risk tolerance levels and business objectives, which makes it versatile across different industries and organizational structures.
- **Standardized and Flexible Controls:** One of the most significant advantages is the standardized set of security controls provided by NIST SP 800-53. These controls serve as

a well-vetted starting point for organizations but are not prescriptive. Organizations can tailor these controls to fit their specific needs, allowing a blend of standardization and flexibility.

- **Role-Based Responsibilities:** The RMF clearly delineates roles and responsibilities at each step, from the C-level executives to the system administrators.
- **Detailed Documentation:** Documentation is a cornerstone of the RMF. From system categorization to monitoring, every decision, action, and assessment is documented. This rigorous documentation assists in audits and compliance checks and provides historical data that can be invaluable for future risk assessments and decision-making.
- **Integration with Existing Processes:** The RMF is designed to integrate seamlessly into an organization's existing Systems Development Life Cycle (SDLC), making it easier to adopt without having to overhaul current procedures.

### **Benefits of NIST SP 800-37 RMF**

The benefits of using the NIST SP 800-37 RMF are manifold and serve to enhance an organization's approach to managing information security risks. These benefits are presented below:

- **Regulatory Compliance:** For organizations in the United States, especially federal agencies and businesses that collaborate with the government, compliance with NIST standards is often a prerequisite. Even internationally, NIST compliance can be considered a mark of rigorous security measures and is often accepted as a proxy for robust security practices.
- **Risk-Driven Approach:** One of the critical benefits is the framework's risk-driven approach. By continuously identifying and assessing risks, organizations can make more informed decisions about where to allocate resources, thus ensuring that high-risk areas receive the attention they require.
- **Methodological Consistency:** Using a framework like NIST's RMF provides a structured, repeatable process for managing risks. This methodological consistency makes it easier to train staff, perform audits, and even explain the organization's risk management strategies to external stakeholders.
- **Enhanced Accountability and Transparency:** The framework demands thorough documentation and clearly defined roles and responsibilities. This provides an accountability track, which is beneficial for both internal management and external audits.
- **Strategic Integration:** The framework is not just a set of IT guidelines but integrates with broader organizational processes and objectives. This helps to ensure that information

security risk management is not a siloed function but part of the broader organizational strategy.

- **Cost-Effectiveness:** By concentrating on the most significant risks first and providing a systematic approach for evaluating the costs and benefits of different security controls, the RMF helps organizations to use their resources more efficiently. This cost-effective approach is especially beneficial for organizations with limited resources for security initiatives.

### 3.3 OCTAVE

The Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE) is a risk management framework designed to identify, assess and mitigate information security risks in organizations. OCTAVE is distinguished by its focus on organizational risk and its flexibility to adapt to any type of organizational structure. By combining a focus on both organizational objectives and technological assets, engaging multiple stakeholders and providing a scalable and iterative methodology, OCTAVE offers organizations a balanced and comprehensive tool for risk management (Caralli et al., 2007).

In Figure 3.4 process of OCTAVE risk assessment is depicted.

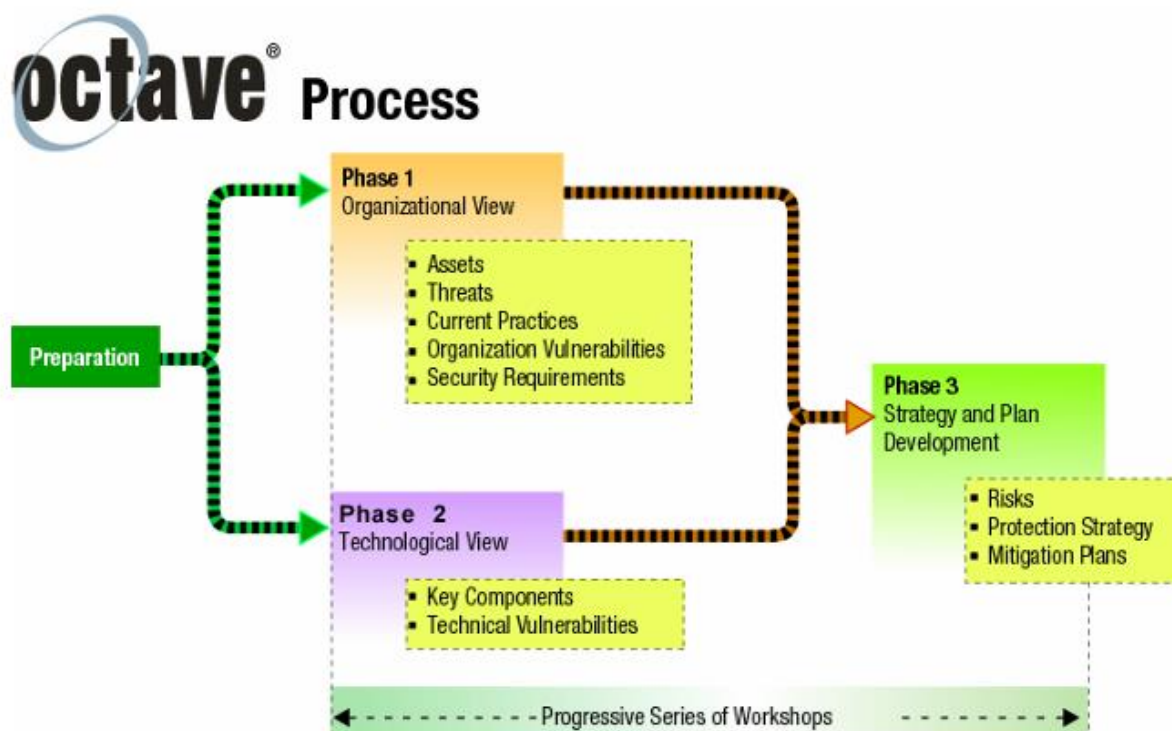


Figure 3.4: Process of Risk Assessment by OCTAVE framework (CERT, 2008)

OCTAVE involves a three-phased approach. Each phase is characterized by workshops, assessments and iterative feedback loops, making the approach very interactive and collaborative:

- 1. Organizational View (Phase 1):** This phase centers around building a risk-based profile for the organization. It considers organizational objectives, current risk areas and security requirements.
- 2. Technological View (Phase 2):** In this phase, data assets are identified and their importance to the organization's objectives is determined. Potential threats and vulnerabilities are then evaluated.
- 3. Strategy and Plan Development (Phase 3):** The final phase develops strategies for mitigating identified risks, typically by selecting appropriate security measures and planning their implementation.

### **Key Characteristics**

- 1. Holistic Approach:** OCTAVE considers both organizational and technical aspects, ensuring a comprehensive risk management strategy.
- 2. Self-Directed:** It is designed to be a self-directed approach, meaning that organizations can implement OCTAVE without the need for external experts, though expert consultation can be beneficial.
- 3. Stakeholder Involvement:** OCTAVE stresses the importance of involving a broad array of stakeholders, ensuring a more balanced and well-informed risk assessment.
- 4. Asset-Centric:** Unlike some other frameworks that focus primarily on vulnerabilities, OCTAVE starts with identifying critical assets, making it particularly useful for organizations that want to align their risk management strategies closely with business objectives.
- 5. Scalable and Flexible:** OCTAVE is adaptable to a wide range of organizational sizes and types, from small businesses to large enterprises.
- 6. Iterative and Repeatable:** The framework is designed to be an ongoing process, not a one-off project. This aligns well with the continuous risk management and improvement model that is considered the best practice in modern cybersecurity.
- 7. Adaptable to Emerging Threats:** Like many risk management frameworks, OCTAVE can be adapted to account for new and evolving risks, thanks to its focus on continuous evaluation and iterative process.



## Benefits of OCTAVE

- 1. Risk-Centric Approach:** One of the standout benefits of OCTAVE is its focus on identifying and evaluating risks from a business perspective. This ensures that risk management activities are aligned with organizational objectives, providing a more contextual and impactful strategy.
- 2. Reduced Complexity:** The self-directed nature of OCTAVE allows organizations to streamline the risk assessment process without the mandatory involvement of external experts, reducing the overall cost and complexity of the process.
- 3. Holistic View:** OCTAVE provides a comprehensive, multi-faceted view of an organization's risk profile. It looks at people, processes and technology, providing a balanced and all-encompassing approach.
- 4. Inclusion of Stakeholders:** The framework encourages involving stakeholders from different departments and roles. This ensures that the risk assessment is well-rounded and considers multiple perspectives.
- 5. Asset-Based Evaluation:** OCTAVE's focus on critical assets means that the most important elements of the organization are secured first. This focus ensures that the security measures employed will have the greatest impact.
- 6. Customizable and Scalable:** OCTAVE's flexible methodology can be adapted to meet the organization's specific needs. This makes it a scalable solution for risk management across various industries and organizational sizes.
- 7. Continuous Improvement:** The iterative nature of the OCTAVE process allows for continuous improvement and adaptation. This is particularly useful in today's rapidly evolving cyber threat landscape.

## 3.4 FAIR

FAIR is a leading framework for understanding, analyzing and quantifying information risk in financial terms. Developed by Jack Jones, FAIR breaks down risk into its underlying components and provides a structured, consistent method for assessing them. FAIR provides a powerful tool for modern risk management. Its data-driven, component-based approach allows organizations to address risk in a more structured, objective and ultimately effective manner (FAIR Institute, 2023).

The framework provides a structured approach to evaluating risks across four primary stages. The process of FAIR framework is displayed in Figure 3.5 and described below.

## Four stages of the FAIR methodology risk assessment



*Figure 3.5: Process of Risk Assessment by FAIR framework (Balbix, 2022)*

- 1. Identify Risk Scenarios (Stage 1):** In the FAIR framework, this stage is crucial for setting the stage for a detailed risk analysis. You begin by identifying the assets that are at risk and the potential sources of threats or threat communities. The focus is on defining what could go wrong and how. Knowing what assets you have, how valuable they are, and who might want to compromise them is foundational in FAIR's risk assessment process. This is where you identify the variables that you'll be evaluating in subsequent stages.
- 2. Evaluate Loss Event Frequency (Stage 2):** Once the assets and threats have been identified, FAIR allows for a detailed evaluation of Loss Event Frequency (LEF). This involves gathering data and making educated estimations about various factors like Threat Event Frequencies (TEF), Threat Capability (TCAP), Resistance Strength (RS), and Vulnerability (Vol). FAIR is especially strong in this aspect as it quantifies these elements in a way that allows for a nuanced understanding of how often a loss event is likely to occur.
- 3. Evaluate Loss Magnitude (Stage 3):** After understanding how often a loss event could occur, the next step in FAIR is to assess how severe such a loss event would be. You'd evaluate both the primary and secondary loss magnitudes. FAIR enables organizations to identify and quantify the various forms of loss, from reputational damage to monetary loss, thereby providing a comprehensive view of the potential impact. The framework uses structured methods to collect data and estimate the scale of the damage.
- 4. Derive and Articulate Risk (Stage 4):** The final stage involves synthesizing all the gathered data to quantify and articulate the risk. FAIR employs computational models to establish the relationship between the different variables identified and evaluated in the earlier stages. One of the key benefits of FAIR is its ability to utilize advanced statistical methods, like Monte Carlo simulations, for risk analysis. This provides a nuanced, probabilistic

understanding of risk, which can be communicated in financial terms, thus making it easier for decision-makers to understand and act upon.

To further comprehend the FAIR framework, the model is displayed in a tree-based representation shown in Figure 3.6. The risk is an evaluation function of the Loss Event Frequency and Loss Magnitude. The former is based on Vulnerability and Threat Event Frequency, which are associated with the repetition of the threat itself. The latter examined the size of the loss for the organization and the secondary risks that may appear with the occurrence of the first risk.

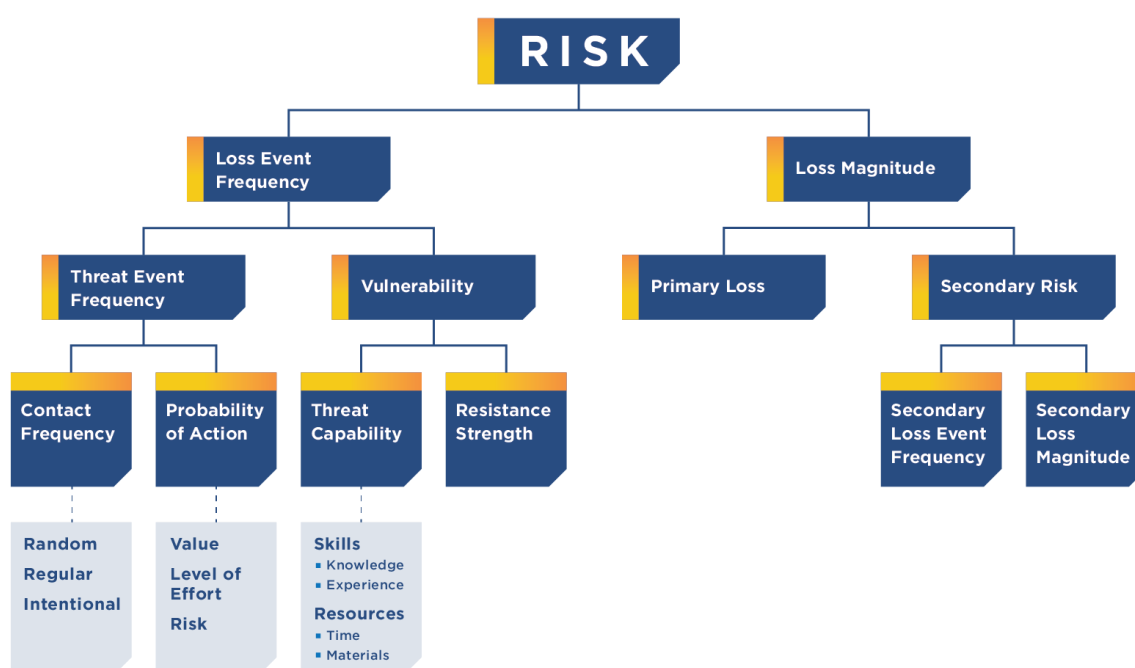


Figure 3.6: Risk decomposition by FAIR methodology (FAIR Institute, 2023)

### Key Characteristics of FAIR:

- 1. Quantitative Analysis:** Unlike many frameworks that offer qualitative assessments, FAIR focuses on quantifiable outcomes. This involves metrics and calculations designed to provide an exact or range-based financial figure, enhancing the rigor and repeatability of risk assessments.
- 2. Financial Orientation:** FAIR translates all risk factors into financial terms, thereby aligning the language of cybersecurity or information risk with the language of business. This makes

it easier to gain C-suite attention and make risk discussions part of broader strategic business decisions.

3. **Component-Based:** FAIR breaks down the often-nebulous concept of risk into discrete, understandable components such as "Loss Event Frequency" and "Loss Magnitude", as shown in Figure 3.6. By understanding the individual elements that contribute to risk, organizations can target interventions more effectively.
4. **Standardized Terminology:** Lack of standardized terminology can often make risk assessments confusing. FAIR addresses this by providing a uniform set of terms and definitions, making it easier for different departments within an organization—or even different organizations—to communicate effectively about risk.
5. **Versatile and Scalable:** FAIR can be applied to a variety of risk scenarios and organizational sizes, making it a flexible option for risk management. FAIR's framework is designed to scale according to the needs of the organization.
6. **Complementary:** While FAIR is a stand-alone framework, it can also complement other methodologies, providing a quantitative aspect that other qualitative frameworks may lack. This makes it a versatile tool that can fit into various risk management strategies.

### **Benefits of FAIR**

Through its unique features and advantages, FAIR offers organizations a robust, data-centric view of information risk, enabling more effective and economically sound decision-making. Its financial orientation and component-based analysis set it apart as a modern tool for mature risk management. These benefits (Balbix, 2022) are described below.

1. **Data-Driven Decisions:** The quantitative nature of FAIR enables organizations to make data-driven decisions, enhancing the overall efficacy and efficiency of their risk management programs.
2. **Strategic Alignment:** By converting risk metrics into financial terms, FAIR allows risk assessments to be integrated into broader business strategies. This can lead to more effective prioritization and resource allocation, thereby maximizing ROI (Return-On-Investment) on security investments.
3. **Resource Optimization:** FAIR helps organizations focus their resources where they will be most effective by quantifying the probable impact of risks. FAIR helps organizations to understand not just the presence of risk, but the potential financial impact of that risk. This

enables more focused spending on security measures that will offer the greatest risk reduction per dollar spent.

- 4. Improved Communication and Enhanced Reporting:** The standardized terminology and quantitative output facilitate better communication among stakeholders and higher management. This clarity makes it easier to report risk to executive levels and facilitates compliance reporting, both internally and for regulatory purposes.
- 5. Compliance:** The framework offers a consistent and repeatable method for assessing risk, aiding in regulatory compliance.

# 4

## *Identified Risk Management Software Tools*

### *4.1 Microsoft Security Assessment Tool 4.0*

The Microsoft Security Assessment Tool (MSAT) 4.0 is a risk assessment application designed to provide information and recommendations about best practices for security within an information technology (IT) infrastructure (Microsoft, 2009). By offering a systematic process for security assessment based on industry standards and best practices, MSAT 4.0 provides organizations with a solid starting point for enhancing their IT security. Its user-friendly interface, customizable scope and detailed reporting make it a versatile tool suitable for a variety of business types and sizes.

The process of MSAT 4.0 typically involves the below features and are presented in Figures 4.1, 4.2 and 4.3:

- 1. Initial Setup:** The tool starts by asking the user to define the scope of the assessment, which could range from an entire organizational IT network to a specific system.
- 2. Data Gathering:** Users fill in a questionnaire based on their current security measures and practices. This questionnaire is divided into multiple sections that cover various aspects of IT security.
- 3. Analysis:** MSAT 4.0 processes the answers to provide an initial assessment of the current security posture.
- 4. Recommendation Generation:** The tool then generates recommendations based on the analyzed data. These recommendations adhere to Microsoft's best practices and industry standards.
- 5. Reporting:** Finally, the tool creates detailed reports that not only highlight vulnerabilities but also offer guidance on improving the organization's security infrastructure.

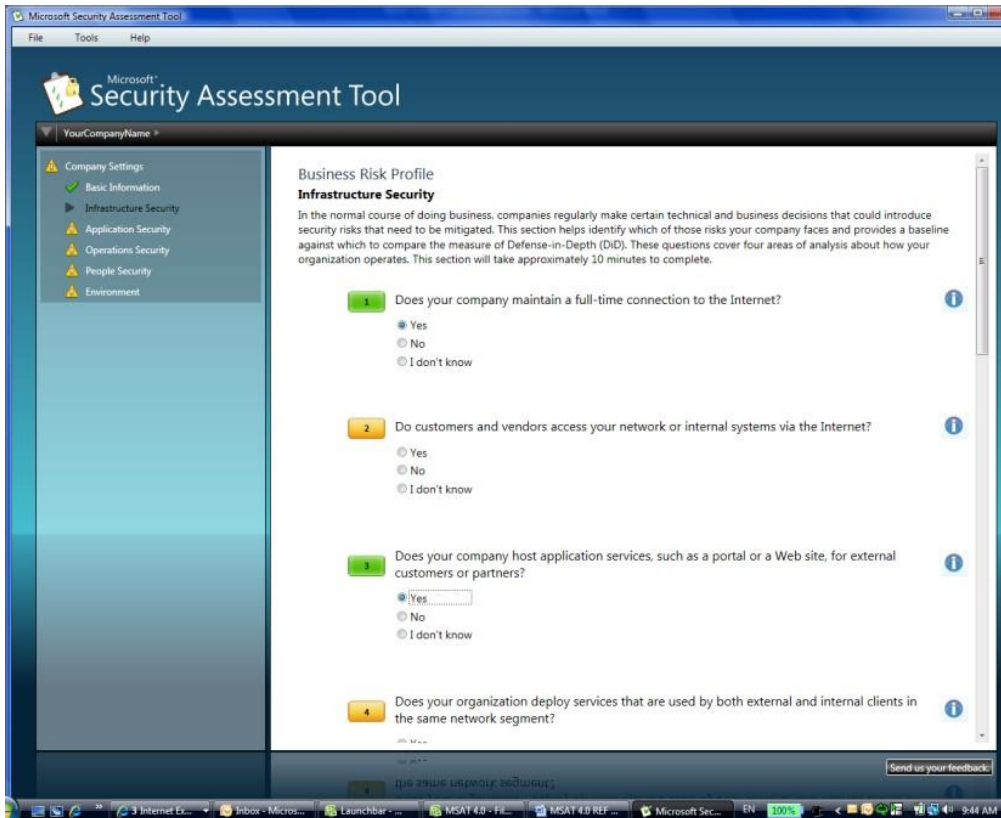


Figure 4.1: MSAT setup for the organization (Microsoft, 2009)

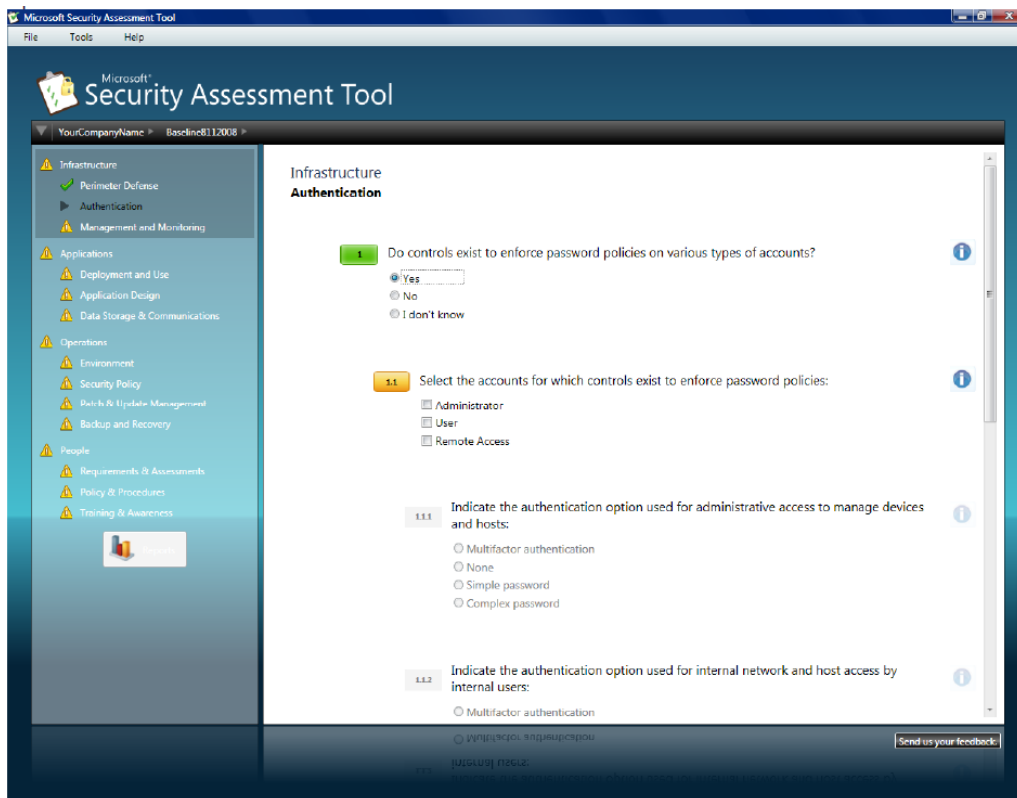


Figure 4.2: MSAT risk assessment process (Microsoft, 2009)

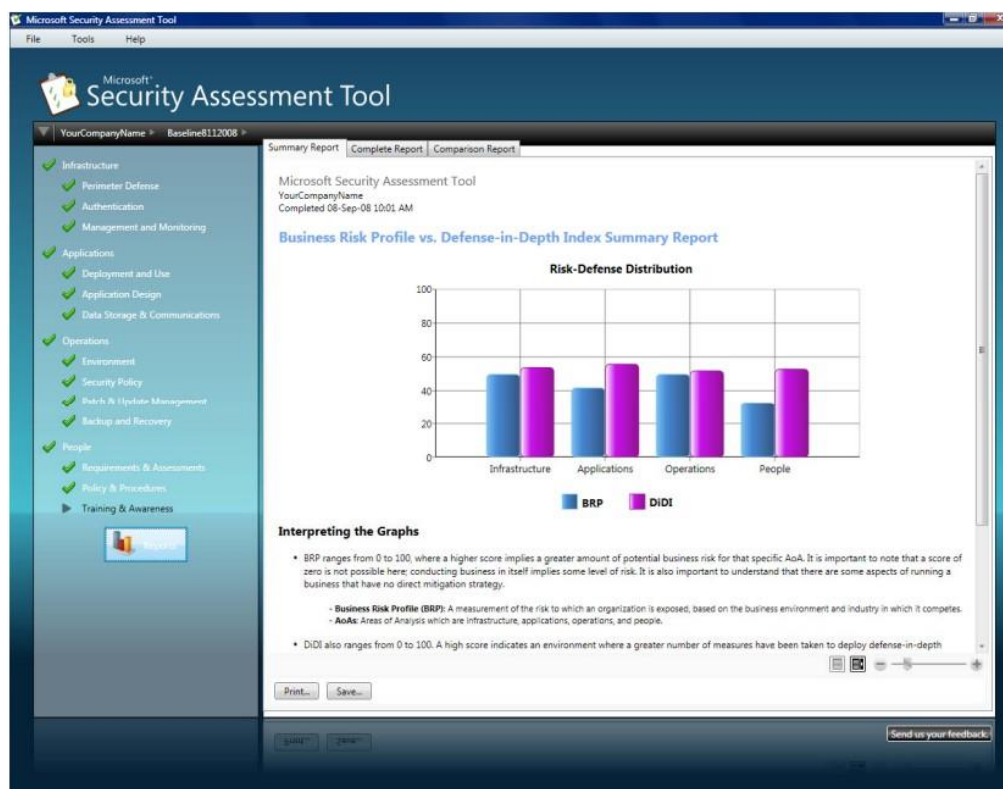


Figure 4.3: MSAT assessment report produced by risk analysis (Microsoft, 2009)

## MSAT's Tool Features

- **Security Benchmarking:** MSAT helps businesses compare their security policies against standard best practices and to other companies in similar industries.
- **Risk Assessment:** The tool evaluates the company's risk profile based on its current security infrastructure, policies and procedures.
- **Custom Recommendations:** MSAT produces a detailed report with specific recommendations tailored to the organization's unique risk profile.
- **Compliance Mapping:** MSAT can map its recommendations to compliance standards like ISO 27001, helping organizations align their security policies with industry standards.
- **User-Friendly Interface (UI):** A straightforward questionnaire aids the user in quickly understanding and completing the assessment.
- **Categorization:** Risks are categorized into areas like Operational Risk, Privacy Risk and Compliance Risk for easier interpretation and action.



## Key Characteristics

- 1. User-Friendly Interface:** MSAT 4.0 offers a GUI-based interface that is intuitive, making it easy even for non-technical staff to navigate through the assessment process. The tool's user-friendly interface ensures that even individuals with limited technical skills can navigate the assessment process. This facilitates broader organizational involvement in security assessments.
- 2. Based on Industry Standards:** Recommendations generated by MSAT 4.0 generally adhere to industry standards and best practices, making the advice trustworthy and actionable.
- 3. Customizable Scope:** The tool allows users to define the scope of the assessment, making it versatile for different organizational sizes and requirements. MSAT 4.0 allows users to customize the scope of the assessment, tailoring the questionnaire to specific organizational needs or requirements. This makes the tool flexible and adaptable.
- 4. Comprehensive Questionnaire:** MSAT 4.0 employs a comprehensive questionnaire to probe various facets of an organization's security, from data protection protocols to network security measures. This ensures a broad-based evaluation and covers multiple security dimensions. The questionnaire is designed to cover a wide range of security topics, from data protection to physical security, ensuring a holistic view of the organization's security posture.
- 5. Detailed and Dynamic Reporting:** The reports generated are thorough and can be used for internal review as well as for compliance documentation. MSAT 4.0 offers real-time reporting features. As soon as the questionnaire is completed, the tool immediately analyzes the results and generates a series of reports. These reports can range from summary-level overviews to deep-dive analyses.
- 6. Risk and Vulnerability Focus:** The tool is designed to identify both vulnerabilities and risks. While vulnerabilities are weak points that could be exploited, risks are the broader potential impacts that could result. MSAT 4.0 helps you understand both. Additionally, it provides actionable insights rather than providing just a list of problems, MSAT 4.0 delivers actionable insights. These are practical steps that can be taken to improve the security posture of the organization.

## Benefits of MSAT 4.0

MSAT 4.0's key characteristics and benefits make it an extremely valuable tool for any organization concerned with enhancing its information security posture. From its comprehensive questionnaire to its actionable insights and reports, it offers a range of features that support both immediate and long-term security planning, which are presented below.

- 1. Cost-Effective:** As a free tool provided by Microsoft, MSAT 4.0 offers a cost-effective way for organizations to assess their security posture. As a free tool, it allows organizations of any size to conduct comprehensive security assessments without worrying about budget constraints.
- 2. Timesaving:** The tool is designed to be fast and efficient, thereby reducing the time it takes for organizations to identify and address vulnerabilities. Traditional risk assessments can be time-consuming. MSAT 4.0 streamlines this process, offering rapid insights that can be immediately acted upon, thereby saving both time and effort.
- 3. Improves Security Awareness:** The comprehensive questionnaire educates users about various facets of security, thus improving overall organizational awareness of IT security matters. By covering a wide range of security topics, MSAT 4.0 offers a more holistic view of an organization's security posture. This is particularly useful for organizations that are looking to address multiple areas of vulnerability but are not sure where to start.
- 4. Strategic Planning:** Detailed reports can be used for strategic planning and budgeting for security measures, as they highlight the areas most in need of improvement or investment. The detailed reports generated by MSAT 4.0 can be an invaluable resource for strategic planning. By identifying weaknesses and suggesting improvements, the tool helps in formulating short-term and long-term security strategies.
- 5. Compliance Aid:** The tool helps organizations prepare for various compliance requirements by providing a structured approach to assessing security risks.
- 6. Educational Purpose:** The questionnaire itself serves as an educational tool. By completing it, team members become more aware of the various aspects of security and why they are important. This educational aspect can be key in fostering a culture of security within the organization.

## 4.2 CORAS

The CORAS Tool is a specialized software system developed to assist organizations in conducting information security risk assessments. It is based on the CORAS model-driven risk management methodology and aims to provide a comprehensive and structured approach to risk management (Solhaug and Stølen, 2014).

By providing a structured, model-driven approach to risk assessment, the CORAS Tool offers organizations a robust and efficient means of evaluating and mitigating potential security risks. Its unique features, such as graphical notation and alignment with international standards, make it a valuable tool for any risk assessment exercise.

The process of CORAS tool is described below.

- 1. Initial Identification:** The tool starts by helping users define and identify the assets that are important to the organization and which could be potentially at risk.
- 2. Threat and Risk Identification:** The tool facilitates the identification of threats and risks associated with the assets.
- 3. Risk Analysis:** CORAS employs a structured approach to analyze the identified risks, usually by considering factors like potential impact, likelihood and vulnerability.
- 4. Recommendation Generation:** Based on the risk analysis, the CORAS Tool produces a set of recommendations tailored to mitigate the risks identified.
- 5. Reporting:** Comprehensive reports are generated, offering insights into the organization's risk profile and proposed mitigation strategies.

### Features of CORAS

- **Risk Modeling:** Allows for detailed modeling of risk scenarios based on assets and threats.
- **Graphical Representations:** Offers diagrammatic representation of threats and vulnerabilities, aiding in the understanding and communication of risks.
- **Customizable Templates:** CORAS has customizable risk evaluation templates that can be adapted to specific business needs.
- **Quantitative and Qualitative Analysis:** Supports both numerical and descriptive risk analysis methods.
- **Integration Capabilities:** It can be integrated with other enterprise systems for more comprehensive risk management.

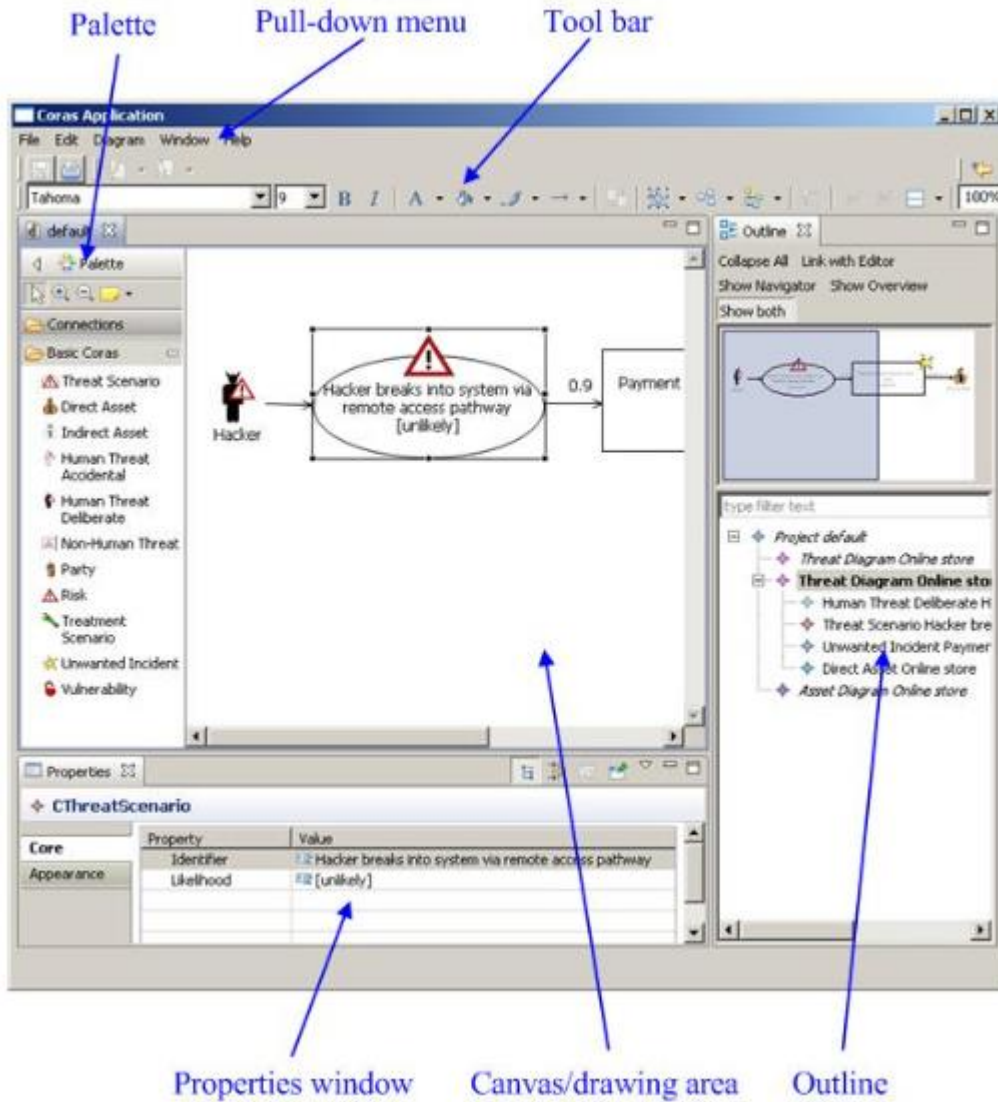


Figure 4.4: User-Interface (UI) of CORAS tool (CORAS, 2023)

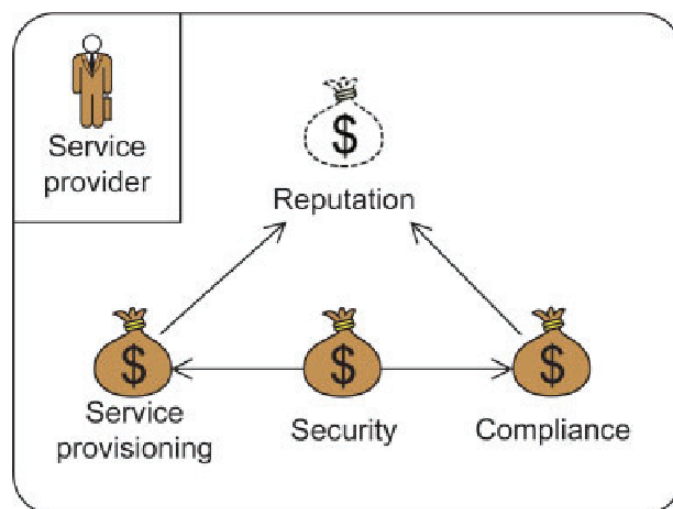


Figure 4.5: CORAS asset diagram (Solhaug and Stølen, 2014)

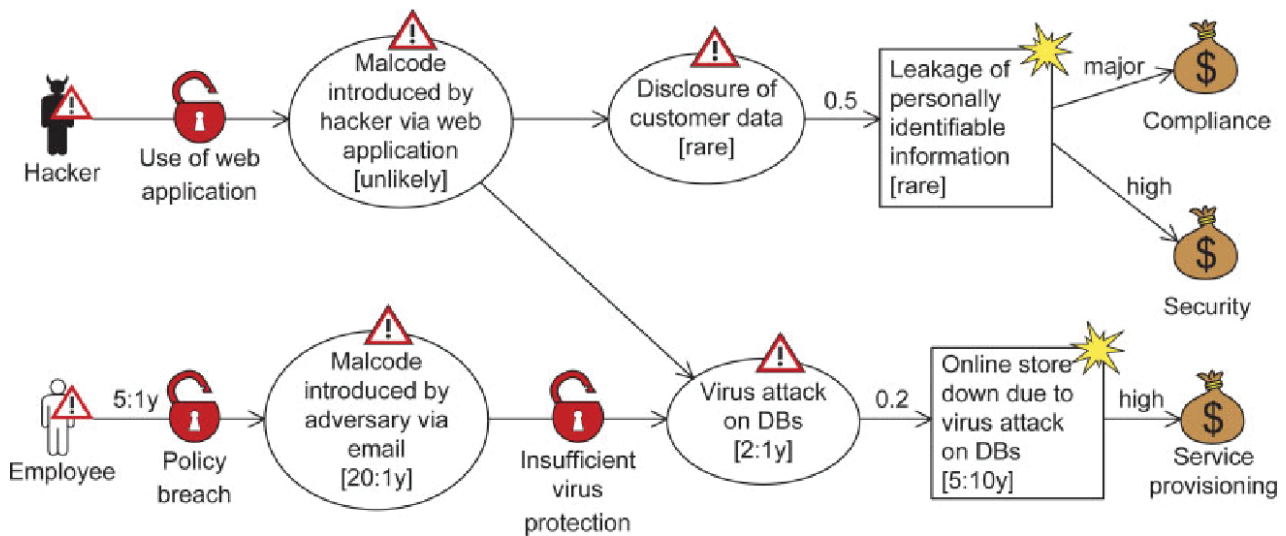


Figure 4.6: CORAS threat diagram (Solhaug and Stølen, 2014)

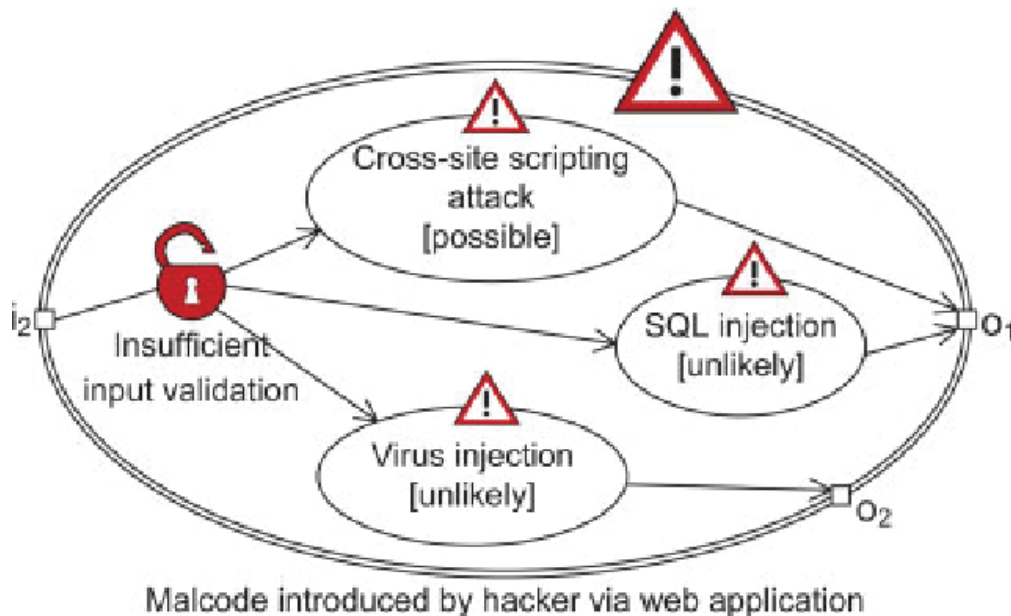


Figure 4.7: Decomposed threat scenario using high-level CORAS (Solhaug and Stølen, 2014)

In Figure 4.3 the UI of CORAS tool is presented which is used to assess the risk in an organization. It provides a wide variety of features aligned with the best practices and standards. In Figures 4.4, 4.5 and 4.6 a threat scenario by intrusion of a hacker into the organization’s systems is depicted. These figures display the asset diagram of the organization, the threat diagram of the hacker’s attack and the high level of the decomposed threat respectively.

The key characteristics and benefits of the CORAS Tool make it an invaluable asset for organizations looking to implement a robust, efficient and standardized approach to risk assessment. Its model-driven methodology, coupled with its customization features and alignment with international standards, offering a comprehensive package for effective risk management. Below the key characteristics and benefits of CORAS are presented.

### **Key Characteristics**

- 1. Model-Driven approach:** One of the standout features of CORAS is its model-driven approach, which makes it easier to visualize the risk assessment process and outcomes. At its core, CORAS is built around a model-driven methodology. This means it provides a visual representation of the risk assessment, aiding in the understanding of complex scenarios.
- 2. Graphical Representations:** The tool offers graphical notations to represent threats and risks, thus aiding comprehension and facilitating communication among stakeholders. This is particularly useful for visual learners and helps in explaining complex risk scenarios to stakeholders.
- 3. Compliance-Friendly:** The tool aligns well with international standards like ISO 27005:2022, making it easier to maintain compliance while conducting risk assessments.
- 4. Extensive Libraries:** CORAS has built-in libraries of common assets, threats and risks, making the initial stages of the risk identification process more streamlined. These pre-loaded libraries speed up the risk identification process and ensure that nothing critical is overlooked.
- 5. Customization:** CORAS offers customization options to better align with specific organizational processes or standards. The tool can be customized to align with the specific needs and policies of an organization. Furthermore, it can be scaled up or down depending on the size of the project or the organization itself.

### **Benefits of CORAS**

- 1. Structured and Standardized Assessment:** The methodology behind CORAS ensures that risk assessments are structured and comprehensive, leaving little room for oversight. The well-structured assessments make the process repeatable and consistent across various departments or projects within the organization.

2. **Efficiency:** The model-driven and graphical approach speeds up the process of risk assessment, making it more efficient. The built-in libraries and customizable templates mean that risk assessments can be performed more quickly, allowing organizations to react swiftly to identified risks. Additionally, the detailed reports and actionable insights empower decision-makers with the information they need to allocate resources more effectively and prioritize security efforts.
3. **Effective Communication:** The graphical notations used in CORAS make it easier to communicate complex risk scenarios to stakeholders, including those who may not be technically proficient.
4. **Compliance Management:** Since CORAS aligns with international standards, it can significantly aid in the compliance management processes of an organization. Because CORAS aligns with international standards, it can be quickly updated or customized to adapt to new or changed regulations. In such way, organizations stand a better chance of fulfilling compliance requirements, thus reducing the risk of penalties or legal issues.
5. **Scalability:** Whether for small projects or organization-wide assessments, the CORAS Tool can be scaled to suit the size and complexity of any risk assessment task.

### 4.3 *SimpleRisk*

SimpleRisk is a web-based risk management tool designed to facilitate the identification, assessment, and mitigation of risks. It is often lauded for its simplicity and user-friendly interface, as well as its ability to adapt to the needs of various organizations. It is a GRC tool that can be used for Governance, Risk Management and Compliance tasks (SimpleRisk, 2020).

The features of SimpleRisk's tool are intended to guarantee that management recognizes, analyzes, and responds correctly to risks that may jeopardize an organization's ability to achieve its business objectives. Each risk's reaction is determined by the chance of occurring and the nature of this risk. According to these parameters, the organization can decide whether to accept, mitigate or transfer to another party the specific risk. The tool is designed for efficient resource optimization and prioritization of the risks that have the greatest impact on the organization's operations.

The process of SimpleRisk typically involves the following:

- **Risk Identification:** The first stage involves defining and identifying the potential risks affecting an organization's assets. SimpleRisk provides a structured approach to list all potential risks and assets, which can be customized according to the organization's requirements.

- **Risk Analysis and Scoring:** SimpleRisk uses a scoring system to evaluate the severity of risks. Users can choose between different risk scoring methodologies, including DREAD, CVSS, and custom scoring options.
- **Risk Treatment and Mitigation Plans:** The tool allows for the creation of detailed treatment and mitigation plans, which can then be assigned to specific team members for implementation.
- **Monitoring and Reporting:** SimpleRisk provides real-time risk reporting capabilities. Users can view a dashboard that gives an overview of the risk landscape, including the status of risk mitigation plans and ongoing activities.

### Features of SimpleRisk

- **Dynamic Risk Register:** SimpleRisk's risk register allows users to log all identified risks, rate them based on severity and assign ownership. It also supports tagging for easier categorization.
- **Customizable Risk Scoring:** The platform offers customizable scoring methods, such as DREAD, CVS and custom formulas, allowing organizations to adopt the scoring method that best suits their industry or requirements.
- **Workflow Automation:** SimpleRisk allows for automated risk workflows, streamlining the process of risk management from identification to resolution.
- **Real-time Dashboards and Reporting:** Customizable dashboards provide a real-time snapshot of an organization's risk posture, with widgets that can display critical metrics and KPIs. Various reports can be generated with a few clicks and the system supports exporting reports to formats like PDF and Excel.
- **Third-party Integration:** SimpleRisk integrates seamlessly with other tools like JIRA, Slack and many cybersecurity tools, allowing for a more cohesive and automated approach to risk management.
- **Multi-user Support and Role-based Access Control:** Multiple users can work on the platform simultaneously and role-based access ensures that sensitive data can be viewed only by authorized personnel.
- **Incident Management:** A built-in incident management module assists in logging, categorizing and managing security incidents.



- **Governance, Risk and Compliance (GRC) Modules:** Additional modules for governance and compliance management can be added, enabling organizations to manage multiple GRC requirements within the same platform.

In the following Figures, the features of SimpleRisk tool are presented:

Figure 4.8: Risk management (Insert a new risk) of SimpleRisk tool (SimpleRisk, 2020)

Figure 4.9: Plan mitigation on SimpleRisk tool(SimpleRisk, 2020)

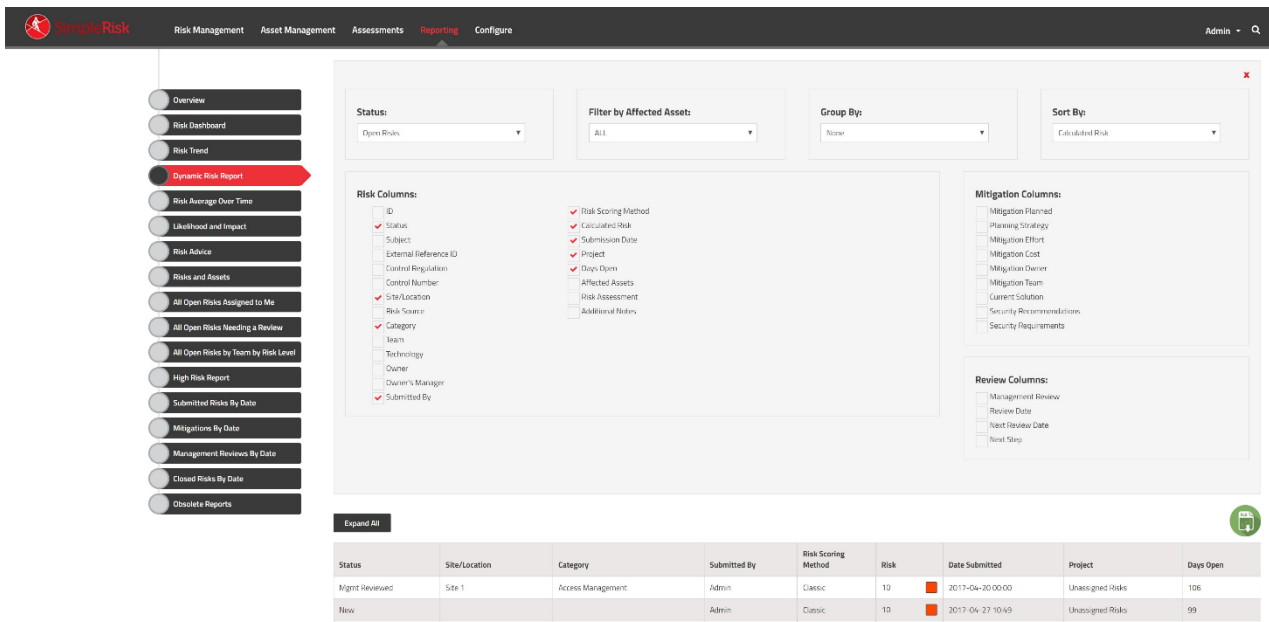


Figure 4.11: Dynamic reporting on SimpleRisk tool (SimpleRisk, 2020)

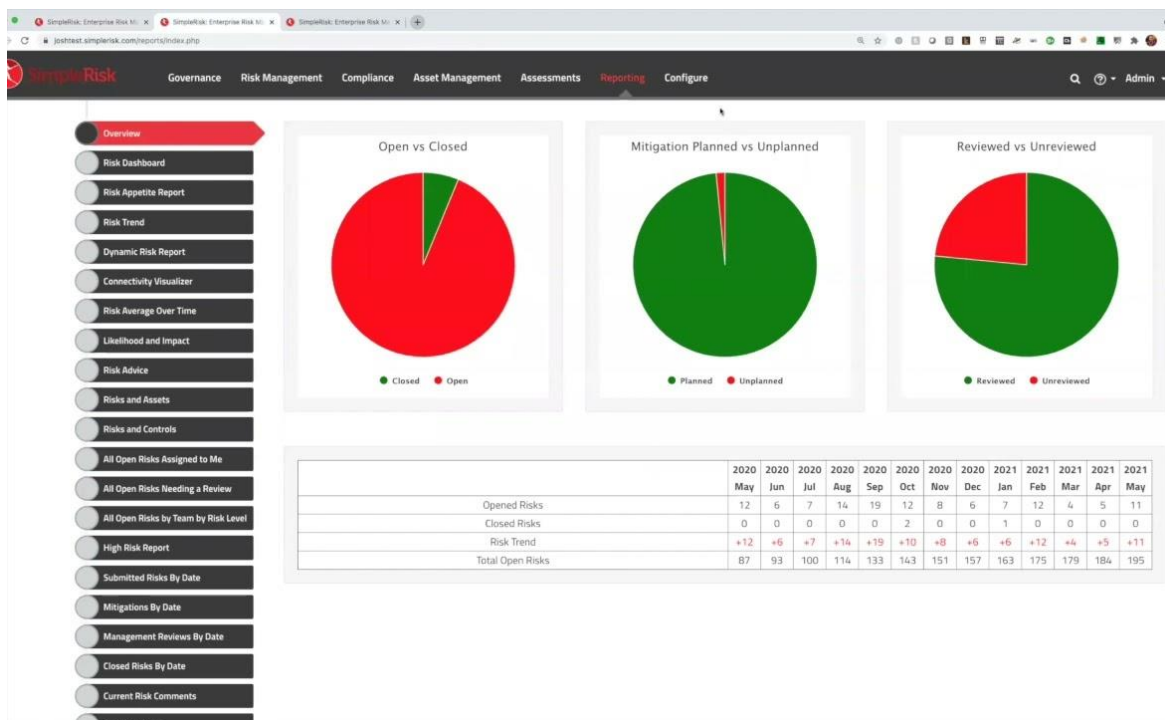


Figure 4.10: Reporting feature of SimpleRisk tool (SimpleRisk, 2020)

## Key Characteristics of SimpleRisk

1. **Usability:** SimpleRisk's user interface is designed to be intuitive, making it simple for users at all levels to navigate through its various modules and features.

2. **Scalability:** The tool can adapt from small teams to large enterprises, making it versatile for a variety of business sizes and industries.
3. **Flexibility:** From risk scoring to dashboards, everything in SimpleRisk can be customized to fit an organization's unique requirements.
4. **Improved Security:** With features like two-factor authentication and role-based access control, SimpleRisk places a high emphasis on securing sensitive data.
5. **Collaboration-Focused:** Given its multi-user support and real-time dashboards, SimpleRisk is designed to promote collaboration among team members.

### **Benefits of SimpleRisk**

1. **Streamlined Risk Management:** The automation features, such as workflow automation and reporting, significantly reduce the time needed to perform various risk management activities.
2. **Cost-Efficiency:** SimpleRisk offers a free community version and tiered pricing options, catering to both budget-conscious small businesses and larger enterprises.
3. **Enhanced Decision-Making:** Real-time data and customizable reports provide actionable insights that aid in decision-making.
4. **Compliance Readiness:** The built-in GRC modules can help organizations stay ahead of compliance requirements, making it easier to adhere to various industry standards and regulations.
5. **Remote Access and Collaboration:** Being a web-based solution, it enables remote teams to work together efficiently, enhancing collaboration and facilitating quicker risk mitigation.
6. **Business Continuity:** Effective risk management through SimpleRisk can contribute to better business continuity planning, helping organizations prepare for and mitigate against various types of risks.

## **4.4 SAP GRC**

SAP GRC is a module within SAP's business software suite that helps organizations manage governance, risk and compliance processes. It is a tool to automate and integrate governance, risk and compliance processes across an organization and provides a centralized platform to manage policies, risks, controls and compliance processes across an organization (SAP, 2023). This includes

things like financial compliance, IT compliance, operational risk management, access controls, fraud management, etc.

It integrates with other SAP modules like ERP, CRM, SCM etc. This allows GRC processes to leverage data from those systems. Additionally, there are pre-configured content packs for regulations like SOX, Basel II, etc. This allows faster implementation and reduces compliance project costs. It provides, also, various workflows, notifications, dashboards and reports to help manage GRC processes. Key users like internal auditors, compliance managers, risk managers can access relevant information.

SAP GRC process typically involves the following:

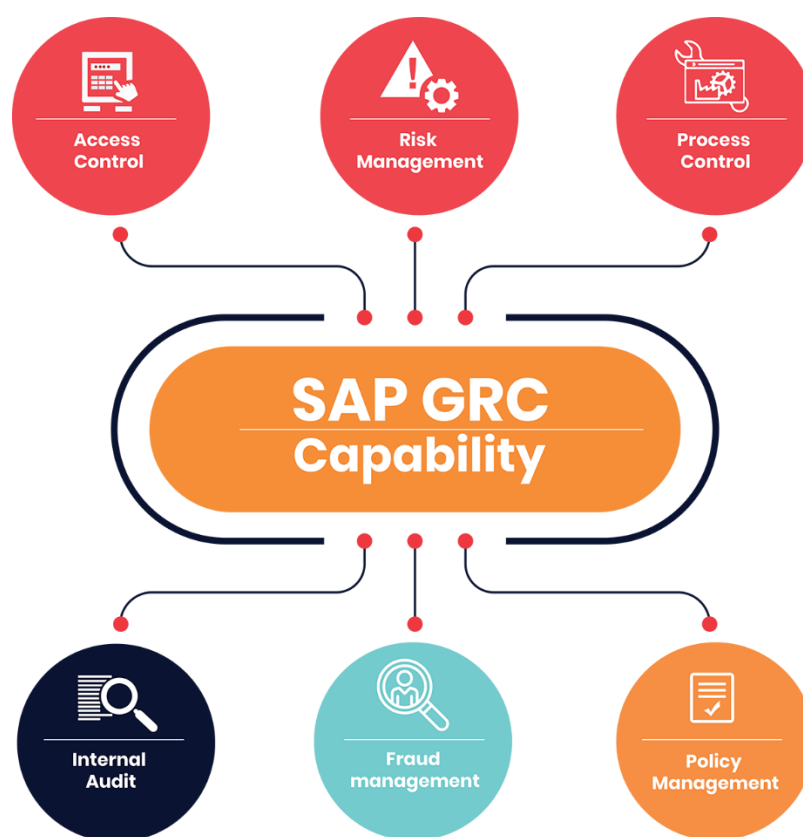


Figure 4.12: SAP GRC capabilities (JNC Consultancy, 2023)

- **Risk Management:** Identification, analysis, evaluation, treatment and reporting of risks. Includes IT risks, market risks, operational risks and more.
- **Audit Management:** Planning, execution, reporting and follow up on internal, external and SOD audits.
- **Policy Management:** Centralized policy library, policy certification, testing and exception management.

- **Access Controls:** Managing access requests, certification and periodic access reviews. Pre-configured rulesets.
- **Compliance Management:** Tracking compliance with regulations like SOX, GDPR, PCI DSS etc.
- **Incident Management:** Recording and managing incidents, violations, fraud and misconduct.

## Features of SAP GRC

SAP GRC provides a wide variety of features presented below:

- Pre-configured content for major regulations (SOX, HIPAA etc.) and risk frameworks.
- Workflow automation for processes like risk assessments, audits, access requests.
- Notifications and alerts for critical risks, policy violations, access issues etc.
- Centralized repository for risks, controls, audits, compliance data and reports.
- Dashboards, reports and visualizations providing insights into GRC data.
- Integration with SAP and non-SAP systems to pull necessary data.

In the following Figures, some of the features of SAP GRC tool are displayed.

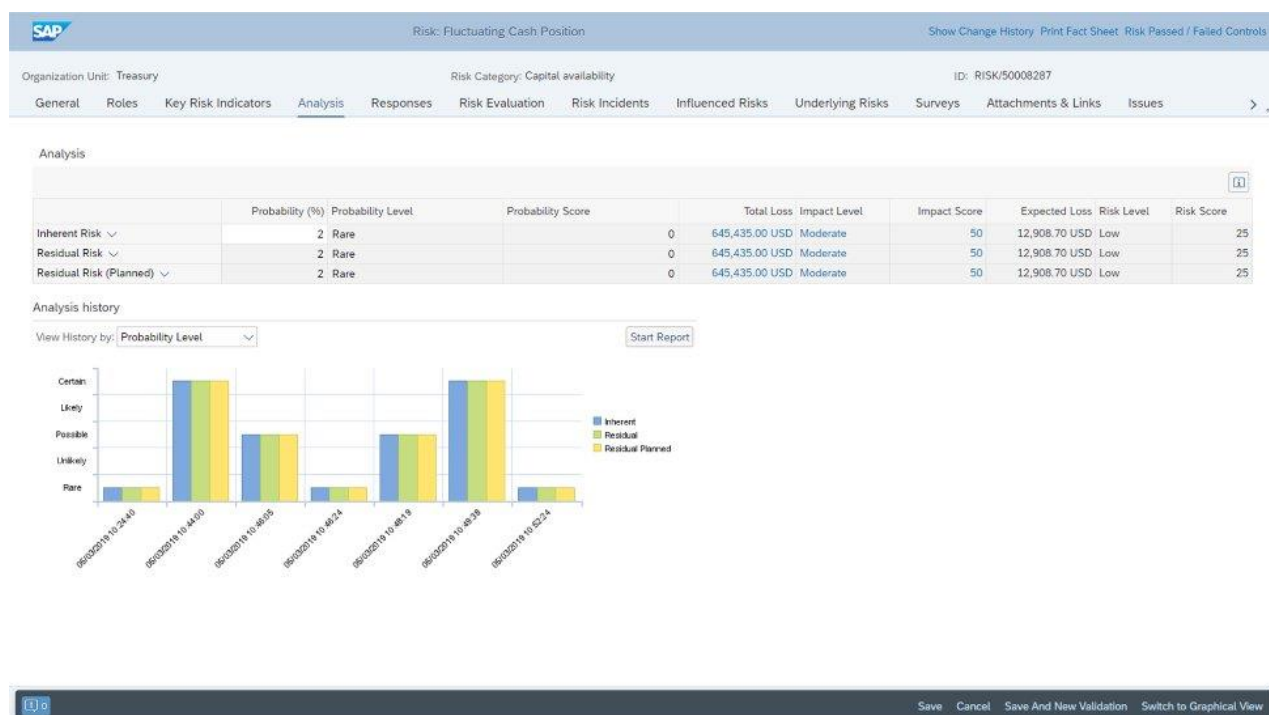


Figure 4.13: Risk analysis by SAP GRC tool (SAP, 2023)

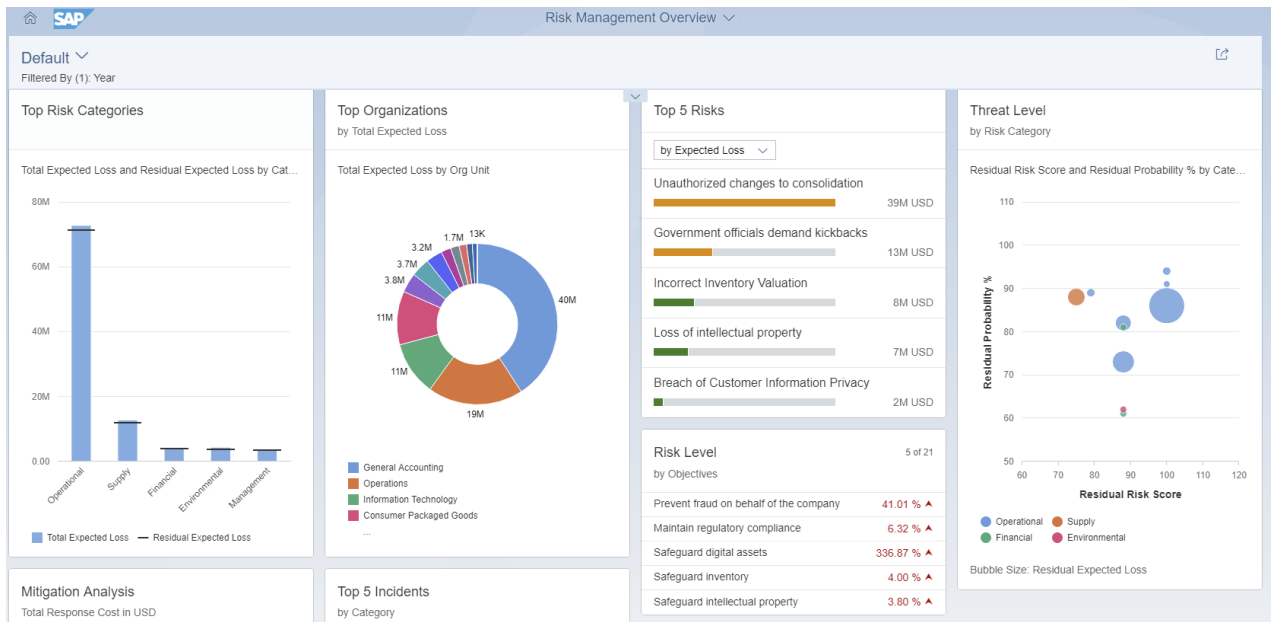


Figure 4.15: Risk management and reporting by SAP GRC (Winterhawk, 2023)

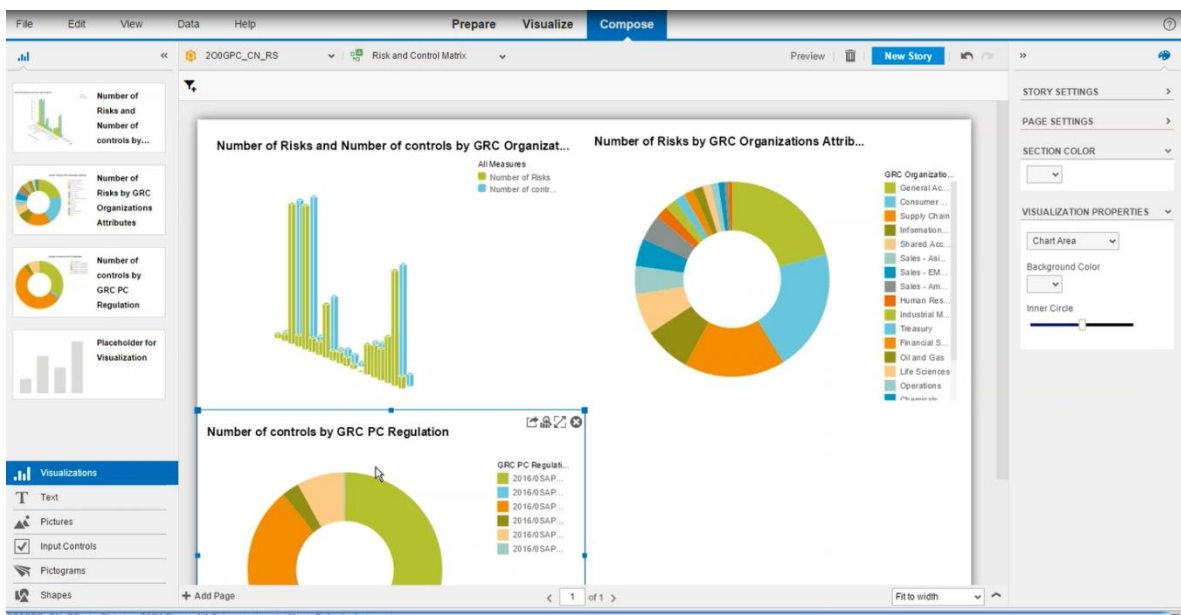


Figure 4.14: Risk assessment reporting by SAP GRC tool (SAP, 2023)

## Key Characteristics of SAP GRC

- Unified GRC platform:** SAP GRC provides a unified, integrated platform to manage multiple governance, risk and compliance processes. Rather than using disparate tools and systems, organizations can centralize all GRC activities within a single solution. This enables a consolidated view of risks, audits, policies and compliance across the enterprise.

- **Organization-wide transparency:** SAP GRC gives organization-wide transparency into GRC data and activities across business units, departments and systems. Executives can get a bird's eye view of compliance status, operational risks, audit issues, and more. This aids risk-based decision-making and resource allocation.
- **Automation of GRC processes:** The software automates and streamlines repetitive, manual GRC processes like risk assessments, control testing, policy certifications and more. Workflows, notifications and integrated data reduce the effort required for GRC activities. This results in greater efficiency and lower compliance costs.
- **Flexibility and configurability:** SAP GRC is highly flexible and configurable to adjust to an organization's changing GRC needs. As regulations change or expand, the system can be adapted without requiring extensive customization. New data sources, risk categories or audit programs can be incorporated to support evolving requirements.
- **Role-based access and permissions:** User access and permissions are managed through roles that reflect organizational responsibilities. Access to risks, reports, and other data can be precisely controlled to maintain segregation of duties. This prevents unauthorized access and enhances security.
- **Integration capabilities:** SAP GRC readily integrates data from SAP ERP, CRM, SRM and other systems to create a single source of truth. It also integrates with non-SAP systems like databases, HR systems, SMTP servers etc. This enables consolidated GRC processes across technologies.

### Benefits of SAP GRC

- **Reduced risk exposure:** SAP GRC helps organizations identify, evaluate, and mitigate risks across business areas. This reduces overall risk exposure arising from unidentified gaps and siloed risk management.
- **Lower compliance costs:** Automating compliance activities like testing and certification reduces manual effort and cost of compliance. Pre-built regulatory content also lowers compliance project costs.
- **Increased visibility:** Real-time dashboards and reports provide visibility into risk, audit and compliance data across the enterprise. This enables proactive management.
- **Accelerated audits:** Centralized audit work papers and findings reduce audit response time. Automated workflows also accelerate the remediation of audit issues.

- **Better data integrity:** Integration eliminates redundant data entry across systems. All GRC data is managed from a single source. This improves data quality and integrity.
- **Standardized GRC processes:** GRC activities are standardized across the organization leading to consistency, efficiency and auditability.
- **Enhanced decision making:** Consolidated organization-wide GRC data enables executives to make more risk-aware decisions aligned to business objectives.
- **Lower Total Cost of Ownership (TCO):** It provides a unified platform with integrated data and automation capabilities lowers the total cost of ownership for enterprise GRC activities.



# 5

## *Comparison Evaluation of Framework Methods and Software Tools*

With the proliferation of cybersecurity threats, adopting a risk management framework and tool has become essential for organizations. This study aims to provide a comparative analysis of selected frameworks and tools, namely ISO 27005:2022, NIST SP 800-37, OCTAVE, FAIR for frameworks and MSAT 4.0, CORAS, SimpleRisk and SAP GRC for tools. This analysis is based on five evaluation criteria, which are scalability, available features, user-friendliness, alignment with compliance requirements and resource optimization, which are described in detail in this chapter.

### *5.1 Criteria for comparison evaluation*

To conduct a comprehensive comparative analysis of various risk management frameworks and tools, it's essential to set forth a robust set of evaluation criteria. The chosen criteria for this study were developed to address the primary concerns and needs of organizations with varying sizes, specializations and regulatory requirements. This section will delve into the five selected evaluation criteria, which are analyzed in the next sub-sections.

#### *5.1.1 Scalability*

Scalability in risk management tools refers to the tool's ability to adapt to an organization's growth in size, complexity, or both. In today's dynamic business environment, scalability is non-negotiable for any tool that wishes to remain relevant. When evaluating a risk management tool for scalability, it's vital to consider not just how well it performs in each situation, but how easily it can accommodate more users, greater data complexity, or even global operations as the organization evolves. Furthermore, scalability also means the tool's capability to integrate with other software

solutions as the need arises, thereby preserving the investment and avoiding the complexity of migrating to a new solution entirely.

Scalability isn't just a matter of handling increased workload; it's also about how smoothly a tool can be upgraded to include new features or accommodate changes in regulatory requirements. For instance, a tool may initially appear inexpensive but may require costly upgrades or customizations to stay current with evolving needs. Thus, it is essential to consider future costs and potential limitations when determining scalability. Another factor is the tool's architecture, whether it's cloud-based or on-premises, as this can influence both scalability and the associated costs.

Finally, scalability is not just a technical criterion but also has a human aspect. A scalable tool must be user-friendly enough to ensure that an increasing number of users can easily adapt to it. The complexity of training required the intuitiveness of the interface and the availability of customer support are factors that can impact the human aspect of scalability. While immediate needs may be a driving force behind the choice of a risk management tool, scalability ensures that this choice remains relevant and effective as needs and numbers change.

### ***5.1.2 User-Friendliness***

User-friendliness is a critical factor for ensuring that a tool is used effectively across the organization. A user-friendly interface can significantly speed up the risk assessment process by making it easier to input data, generate reports and understand results. When evaluating a tool for user-friendliness, consider whether the tool is intuitive and straightforward enough that someone with minimal training can use it effectively. This is especially important for organizations with diverse teams, where not everyone may have technical expertise in information security or risk management.

However, user-friendliness should not compromise the functionality and complexity that a robust risk management process demands. The tool should offer a balance, providing advanced features for expert users while also enabling less technical users to accomplish basic tasks without undue hassle. Consideration should also be given to how easily the tool allows for the exporting and importing of data, the generation of automated reports and customization. In organizations where risk management is a collaborative effort involving multiple departments, the ease with which data can be shared and understood is paramount.

The human aspect of user-friendliness is also a key consideration. With a complete series of non-exhaustive training and user must be capable of adapting to changes or updates in the proposed

method or tool. This becomes particularly relevant in large or growing organizations where new employees will regularly need to be brought up to speed with the risk management tools in place. Accessibility features, such as multilingual support or provisions for visually impaired users, can also add to a tool's user-friendliness, ensuring that it is inclusive and accessible to all employees.

### ***5.1.3 Alignment with Compliance Requirements***

In a world of ever-changing regulations and stringent compliance needs, the alignment of a risk management tool with compliance requirements is a critical evaluation criterion. Organizations often operate under multiple regulatory frameworks and a tool that simplifies the process of compliance can save time, effort and financial resources. When assessing a tool for this criterion, it's essential to look at how thoroughly it incorporates various compliance standards and whether it is updated regularly to reflect changes in these standards. The tool should facilitate reporting and documentation processes that are often mandatory for regulatory compliance.

However, compliance standards do not fit in every case scenario or in every organization because what is essential for a healthcare organization under HIPAA (Health Insurance Portability and Accountability) may not be the same for a financial institution under the GDPR (General Data Protection Regulation). Thus, a tool's adaptability to specific regulatory environments and its ability to allow for customization in compliance reporting are valuable features. It is important that each method or tool can be modified and adapted to match different compliance templates with specific regulations.

Another dimension is the forward-looking aspect of compliance. Regulations and compliance requirements are rarely static; they evolve in response to technological advancements, geopolitical shifts and changes in public policy. Therefore, a good risk management tool should not just be compliant with current regulations but should also be agile enough to adapt to future changes. The availability of regular updates, expert customer support and a strong community of users can often be indicators of how well a tool can adapt to changing compliance landscapes.

### ***5.1.4 Features***

Features are the functionalities and capabilities that a risk management tool offers and they are a significant criterion for evaluation. These features can range from basic functionalities like data input and report generation to more advanced capabilities like real-time analytics, predictive modelling and integration with other organizational tools. When evaluating a tool based on its features, one must consider not just what it offers but also how these features align with the

organization's specific needs and objectives. Each tool should offer a comprehensive dashboard for real-time monitoring and should automate workflows to streamline the risk management process.

However, a tool that offers an exhaustive list of features is not necessarily better. It's essential to balance feature richness with usability. Too many features, particularly those that are not useful for the specific needs of the organization, can clutter the interface and make the tool less user-friendly. It's also important to consider how these features are updated and enhanced over time. It is crucial that the frequency of updates genuinely add value to the existing setup and do not complicate the tool's usage.

Another critical aspect to consider under features is the customization capability of the tool. Every organization is unique in its operations, scale and risk profile and a tool should be flexible enough to accommodate these unique traits. It is important for each tool to enable the users to configure custom fields, create their own risk assessment templates, or integrate with other tools according to the organization's policies and methodologies. Customization not only allows the tool to fit better with the organization but also often extends its lifespan, as it can adapt to evolving requirements.

### ***5.1.5 Resource Optimization***

Resource optimization as an evaluation criterion pertains to how efficiently a risk management tool utilizes both human and computational resources. Given that these tools often require an investment in training, installation and maintenance, the ROI needs to be significant. Users should be able to reduce manual work involved in risk assessment or compliance reporting, which also makes the organization susceptible to more frequent human errors and should provide automation features that can save time and thereby reduce operational costs.

When evaluating a tool's efficiency in resource optimization, it's vital to consider the total cost of ownership, not just the upfront cost. This includes looking at the resources needed for regular updates, the time employees spend using the tool and any additional hardware or software requirements that might be needed for optimal functionality. It's also useful to evaluate how the tool impacts the daily activities of those who will use it. Thus, employees should spend less time struggling with a complicated interface and more time focusing on meaningful work.

Another aspect of resource optimization is how well the tool can integrate into the existing infrastructure. A tool that requires significant changes to the current systems may end up consuming more resources than it optimizes. Conversely, a tool that can easily integrate with existing systems—

be it HR systems for employee training data or IT systems for vulnerability assessments—can significantly improve resource optimization.

## **5.2 Evaluation analysis**

### **5.2.1 Evaluation analysis of selected ISRM Frameworks**

#### **5.2.1.1 Scalability:**

When assessing the scalability of various risk management frameworks, it becomes apparent that each has its unique strengths and limitations. ISO 27005:2022, for instance, scales well in larger corporations with complex operations but may be less agile for rapidly evolving startups. Its emphasis on process-oriented risk management can also be a hindrance to fast scaling, especially in dynamic industries. On the other hand, NIST SP 800-37 scores high on scalability due to its modular approach and adaptability. Its flexibility allows for tailored risk management strategies, making it a good fit for organizations of any size, including those in fast-paced sectors.

OCTAVE also presents scalability advantages, particularly for organizations that are in the scaling phase and still building their risk management practices. Its adaptability and focus on organizational aspects make it suitable for incremental implementation, although it may suffer from consistency issues in larger, decentralized settings. FAIR stands out for its quantitative, data-driven approach to risk management, which scales well in terms of data complexity. However, it could pose challenges for smaller organizations that lack statistical analysis capabilities, acting as a barrier to scale efficiently.

#### **5.2.1.2 Features**

The features criterion is instrumental in distinguishing how well a framework meets the specific needs of an organization. ISO 27005:2022 excels in its comprehensive approach to identifying, assessing and mitigating risks. The framework comes packed with templates and guidelines that facilitate a methodical approach to risk management. However, its extensive set of features may be overwhelming for smaller organizations or those with simpler risk landscapes. NIST SP 800-37, on the other hand, offers a modular set of features that can be tailored to an organization's unique needs. Its emphasis on continuous monitoring and real-time assessment provides added layers of defence, making it particularly suited for environments where risks evolve rapidly.

OCTAVE stands out for its focus on the organizational aspects of risk management, emphasizing features like strategic planning and internal collaboration. While these features are less

technical in nature, they offer a holistic approach to managing risks that extends beyond IT and cybersecurity to cover broader organizational vulnerabilities. FAIR distinguishes itself with its quantitative risk assessment features. The framework allows for data-driven decision-making through its unique set of analytical tools. However, these features might require specialized training or expertise in statistical analysis, which could be a hurdle for some organizations.

#### *5.2.1.3 User-Friendliness*

User-friendliness is a critical aspect to consider when evaluating risk management frameworks, as ease of use directly impacts the efficiency and effectiveness of risk mitigation efforts. ISO 27005:2022, while comprehensive, may seem cumbersome and challenging to navigate for those unfamiliar with its intricacies. However, it often comes with detailed documentation and training materials that somewhat mitigate this limitation. NIST SP 800-37 generally fares better in terms of user-friendliness due to its modular approach. Organizations can selectively implement sections of the framework that are most relevant to their operations, thus easing the learning curve and increasing the framework's accessibility.

OCTAVE scores reasonably well on the user-friendliness criterion because of its intuitive, organization-focused approach. Its less technical nature means that staff at various organizational levels, including management, can engage with it more readily. However, this can be a double-edged sword, as its broad focus may make it difficult to pin down specific actions without prior expertise. FAIR is more specialized and thus can be less user-friendly for those without a background in data analysis or risk assessment. Its strengths in quantitative assessment require a level of expertise that may necessitate specialized training or even hiring of dedicated staff, posing a hurdle for smaller organizations.

#### *5.2.1.4 Alignment with Compliance Requirements*

Alignment with compliance standards is a pivotal criterion in evaluating the suitability of risk management frameworks, especially for organizations subject to regulatory scrutiny or contractual obligations. ISO 27005:2022 often stands as a gold standard in this context, given that it is internationally recognized and provides a comprehensive set of guidelines aligned with various global regulations. Organizations adhering to this framework are generally well-placed to meet most regulatory requirements, such as GDPR for data protection or HIPAA for healthcare information security.

NIST SP 800-37 also shines in this area, particularly for organizations operating in or with the United States. Given that it is a framework developed by a U.S. federal agency, its guidelines are often cited in or aligned with U.S. federal regulations, such as FISMA. For organizations primarily concerned with U.S. regulations, NIST SP 800-37 offers a streamlined path to compliance. OCTAVE, while not as universally recognized for compliance as ISO 27005:2022 or NIST SP 800-37, provides valuable guidelines for risk-based strategic planning, which can be useful for meeting the governance and planning aspects of various compliance standards.

FAIR is somewhat of a specialized case in terms of compliance. While it doesn't directly map to specific regulations, its data-driven approach to quantifying risk aligns well with the evidence-based requirements of many regulatory frameworks. This makes it easier for organizations to justify their risk management strategies and actions during compliance audits. However, this also means that FAIR is often used in conjunction with other frameworks that provide more comprehensive compliance coverage.

#### *5.2.1.5 Resource Optimization*

Resource optimization is a critical criterion for evaluating risk management frameworks, particularly for organizations with limited resources or those looking to maximize the efficiency of their risk management initiatives. ISO 27005:2022, while exhaustive in its coverage, often requires a significant investment in both human and technological resources. From hiring specialized staff to ongoing training and system upgrades, adhering to ISO 27005:2022 can be resource-intensive, potentially straining the budgets of smaller organizations.

NIST SP 800-37, on the other hand, offers a more modular approach, allowing organizations to tailor the framework to their specific needs. This modularity can lead to more efficient resource allocation as organizations can focus on implementing only the most relevant sections. However, even this tailored approach may require a considerable time investment for proper configuration and maintenance, depending on the complexity of the organization's operations.

OCTAVE's focus on organizational risk rather than technological specifics can sometimes lead to better resource optimization, especially for smaller organizations. Its strategic, top-down approach allows for the possibility of implementing risk management strategies without necessarily requiring high-end technological solutions. This makes it an attractive option for organizations with limited IT resources.

FAIR's strength lies in its quantitative analysis of risk, but this comes at the cost of requiring specialized expertise in data analytics and statistical modeling. For organizations that already have such expertise in-house, FAIR can offer a highly efficient way to optimize risk management resources. However, the cost and time associated with training staff or hiring experts can be a significant resource burden for others.

## ***5.2.2 Evaluation analysis of selected ISRM Tools***

### *5.2.2.1 Scalability*

MSAT provides a modular approach, allowing small and medium-sized enterprises to implement the tool without massive upfront costs. You can start with a basic package for risk assessment and then add more features or user licenses as required. However, the tool is not without its limitations. It is primarily a standalone system and integrating it with other third-party security tools or systems can be cumbersome. The tool doesn't offer a native Application Programming Interface (API) for easy integration, meaning that it may struggle to keep up with the growing complexities of larger, multi-faceted organizations.

CORAS offers excellent scalability options, because the tool is designed to grow along with the organization. The pricing model allows for adding new users and features seamlessly, which is a boon for rapidly expanding companies. CORAS also offers a robust API for easy integration with other software systems and security tools. This makes CORAS an ideal choice for larger enterprises that have a complex technology stack and need to integrate multiple functions like incident response, compliance tracking and real-time risk assessment.

SimpleRisk offers scalability but in a limited context. Designed with smaller organizations in mind, it can handle a moderate increase in user numbers and assets. However, its features are not as comprehensive as some of the other tools, which might lead to a point where it no longer satisfies the requirements of a growing enterprise. While it offers some API functionalities for integration, the capabilities are somewhat restricted, which can limit its applicability in complex IT environments.

SAP GRC scores highly on scalability. The suite is designed to accommodate the needs of both small and large organizations. Whether you're running a small business with minimal compliance requirements or a large enterprise with a complex governance structure, SAP GRC can adapt to your specific needs. Moreover, it can easily integrate with other SAP products and even non-SAP systems, providing a scalable solution for organizations at different stages of growth.



#### *5.2.2.2 Features*

In the landscape of risk management tools, the range of features offered can significantly influence an organization's ability to manage and mitigate risks effectively. In this context, we find that Microsoft Security Assessment Tool 4.0 (MSAT) offers essential functionalities like basic risk assessment templates and rudimentary vulnerability scanning. While it does provide a foundational level of security assessment reporting, MSAT's features are not as comprehensive as some other tools available in the market. For instance, it lacks advanced customization options in reporting and has a limited scope in compliance tracking.

In contrast, CORAS emerges as a more feature-rich tool designed for comprehensive risk management. It enables advanced risk modeling and real-time monitoring of risks, setting it apart from basic tools like MSAT. Additionally, CORAS provides extensive reporting capabilities that can be customized for various stakeholders. Its ability to integrate with other tools via robust APIs also makes it a scalable solution for larger enterprises. Moreover, it has a comprehensive compliance tracking system, supporting multiple standards and making it ideal for organizations that need to adhere to various regulatory requirements.

SimpleRisk, on the other hand, offers a simplified approach aimed primarily at small to medium-sized enterprises (SMEs). Though it covers basic risk assessment functionalities, the tool does not allow for much customization. The reporting capabilities, while serviceable, are basic and best suited for smaller organizations with less complex needs. The interface is user-friendly, making it accessible for teams with limited technical expertise, but its compliance tracking features are relatively rudimentary.

Finally, the feature set of SAP GRC is comprehensive, covering everything from Audit Management to Cybersecurity. Its modular design allows organizations to choose the features they need, which can be integrated smoothly into the existing IT landscape. The availability of advanced features like automated process control and risk mitigation tools makes it a standout option for comprehensive governance, risk, and compliance management.

#### *5.2.2.3 User-Friendliness*

The user-friendliness of a risk management tool is often a crucial factor that influences its adoption and effectiveness within an organization. In the realm of the tools under discussion, Microsoft Security Assessment Tool 4.0 (MSAT) offers a straightforward interface but might require some initial training for complete mastery. The tool comes with built-in templates and a relatively easy-to-navigate dashboard, but the usability ends there. Complex tasks can become

cumbersome due to the lack of intuitive design elements, making it a mixed bag in terms of user-friendliness.

CORAS, by contrast, places a strong emphasis on user experience. It features an intuitive interface that is easy to navigate, even for individuals who are not experts in risk management. With drag-and-drop functionalities and a host of templates, CORAS makes it simple for users to perform complex risk assessments and modeling tasks. This user-centered design makes it a highly accessible tool, cutting down on the training time and costs typically required to bring staff up to speed.

SimpleRisk lives up to its name by offering a user-friendly, simplified interface aimed specifically at smaller organizations with fewer technical resources. Its straightforward layout and guided processes make it extremely easy for users to execute basic risk assessments and generate reports. However, this simplicity comes at the expense of more advanced features, which may limit its usability for more experienced risk managers.

While SAP GRC offers a plethora of advanced features, user experience can sometimes suffer due to its complexity. However, for users familiar with SAP's ecosystem, the user interface can be quite intuitive. Also, given its enterprise-level capabilities, some degree of complexity is to be expected. Overall, SAP offers training and support to help users get acclimated, making it reasonably user-friendly for its target audience.

#### *5.2.2.4 Alignment with Compliance Requirements*

The alignment of a risk management tool with compliance requirements is an essential aspect that organizations must consider, especially those bound by legal and regulatory obligations. Microsoft Security Assessment Tool 4.0 (MSAT) offers basic functionalities that assist in meeting some general compliance standards. However, it does not offer specific modules or features tailored to individual compliance frameworks like GDPR, HIPAA, or PCI-DSS, potentially requiring additional tools or customization for full compliance.

In contrast, CORAS provides in-depth features specifically designed to align with various compliance requirements. Its library includes templates and workflows that are modeled after regulatory frameworks such as GDPR and Hopland FISMA. This ensures that risk assessments are compliant with current legal guidelines, making CORAS a strong choice for organizations that need to maintain stringent compliance standards.

SimpleRisk, while user-friendly, has limited built-in compliance capabilities. Although it offers generic tools for risk assessment that can be manually tailored to meet specific regulations, it doesn't

offer predefined compliance modules. Organizations looking for out-of-the-box compliance solutions may find SimpleRisk lacking in this aspect.

As for SAP GRC, one of the primary strengths of the tool is its strong alignment with compliance requirements. It offers specialized modules for different kinds of audits, compliance reporting, and policy management. Whether your organization needs to comply with local laws or international standards, SAP GRC offers the features to ensure that compliance is maintained.

#### *5.2.2.5 Resource Optimization*

Resource optimization is a crucial consideration when selecting a risk management tool, as organizations aim to maximize functionality while minimizing costs and resource allocation. Microsoft Security Assessment Tool 4.0 (MSAT) is lightweight and does not demand significant computational resources, making it a cost-effective solution for small to medium-sized organizations. However, the limited features may necessitate supplementary tools, potentially increasing the overall resource expenditure.

CORAS stands out for its robustness and modularity, allowing organizations to select only the features they need, thereby optimizing resource utilization. While it demands a moderate level of computational power, its scalability ensures that resource use can be adjusted in accordance with organizational growth. Yet, CORAS may require a dedicated team for maintenance and updates, which could increase the human resource commitment.

SimpleRisk is designed for smaller organizations and requires minimal setup and maintenance. This low resource requirement makes it ideal for companies with restricted budgets and less technical manpower. However, the trade-off comes in terms of advanced functionalities, which are limited in SimpleRisk, possibly requiring additional tools for more complex risk assessment needs.

Implementing SAP GRC can be resource-intensive in terms of both time and cost. However, once implemented, the suite helps in optimizing various governance and compliance-related resources by automating routine tasks and providing detailed insights into risk factors. This can result in long-term savings and operational efficiencies, outweighing the initial implementation resources required.

### **5.3 Discussion**

Taking into consideration the benefits and drawbacks of each Security Risk Management framework and tool, a nuanced perspective emerges based on the provided evaluation criteria.

When examining the scalability of different Security Risk Management frameworks and tools, there are noticeable distinctions that make each better suited for different types of organizations. ISO 27005:2022 and NIST SP 800-37 stand out as highly scalable options, capable of being applied to both small and large organizations. However, this scalability often comes with a level of complexity and resource intensiveness that may deter smaller organizations with limited resources. On the contrary, OCTAVE and FAIR provide a more tailored approach, allowing for scalability in smaller or specialized environments, but they lack the comprehensive nature of ISO and NIST, potentially making them less suitable for larger organizations seeking an all-encompassing solution. In terms of tools, SAP GRC offers exceptional scalability, catering to the needs of any size of organization with its broad focus on governance, risk, and compliance. However, like ISO and NIST, its comprehensive nature might necessitate considerable resources for effective implementation. MSAT 4.0 is designed primarily for broader enterprise risk assessments and, while scalable in that context, might not be the best fit for smaller or specialized organizations. CORAS, though highly scalable, introduces the caveat of requiring specialized expertise in model-driven security, making it less accessible for smaller organizations or those without the necessary expertise. SimpleRisk, however, provides a straightforward solution that is easily scalable, especially for smaller organizations or those looking to implement a risk management tool without a steep learning curve or resource commitment.

When evaluated based on features, each framework and tool in the landscape of Security Risk Management offers something unique, catering to different organizational needs and preferences. NIST SP 800-37 stands out for its modular design, which allows organizations to adjust their risk management strategies as requirements change or new vulnerabilities emerge. This modularity can be a significant advantage for organizations that need a framework adaptable to change. ISO 27005:2022 is also feature-rich but could be considered overwhelming due to its exhaustive list of elements to consider for information security risk management. Its robustness is its strength but could also serve as a limitation for organizations looking for a less comprehensive solution. In the realm of tools, SAP GRC offers a wide array of features, from risk analytics to compliance monitoring, making it a complete solution platform for organizations' governance, risk, and compliance needs. However, its exhaustive feature set, like that of ISO 27005:2022, can be overwhelming for some organizations, especially those without a dedicated GRC team. MSAT 4.0 offers powerful reporting capabilities but lacks some of the specialized risk modelling functionalities that a tool like CORAS provides. CORAS distinguishes itself with a unique visual language for threat and risk modelling, making it an excellent tool for organizations that prefer

model-based risk assessments. SimpleRisk, on the other hand, offers a balanced feature set suitable for organizations that require straightforward risk assessment capabilities without the complexity that comes with more feature-rich tools.

The user-friendliness of a Security Risk Management framework or tool is often a critical factor for organizations, as it directly impacts the learning curve and the efficiency of implementing risk management processes. When it comes to frameworks, NIST SP 800-37 offers extensive guidelines and resources, but these can be daunting for newcomers or smaller teams who may find the depth of the documentation overwhelming. ISO 27005:2022, while globally recognized, also suffers from a similar challenge, which requires a certain level of expertise to navigate its comprehensive guidelines effectively. Turning our attention to tools, SAP GRC is powerful but can be complex, often requiring specialized training or even a dedicated team to manage its suite of features. This could be a drawback for smaller organizations or those without a dedicated GRC unit. MSAT 4.0, while robust in features, offers a more user-friendly interface compared to SAP GRC, making it accessible for teams with varying levels of expertise. CORAS is highly specialized and its model-based approach requires a significant level of expertise in model-driven security. SimpleRisk provides a user-friendly experience for those who need straightforward risk management capabilities without the complexities often associated with more comprehensive tools.

Compliance alignment is a key consideration for organizations when selecting a Security Risk Management framework or tool, especially when they are subject to various industry regulations or standards. In this regard, ISO 27005:2022 and NIST SP 800-37 are often seen as the gold standards. They are widely accepted frameworks that align well with various international and national regulations, making them top choices for organizations that need to demonstrate compliance rigorously. However, their extensive nature can be seen as both a boon and a bane. They provide comprehensive compliance roadmaps but also necessitate a high level of commitment and resource allocation to ensure full compliance. On the tools side, SAP GRC excels in the compliance category, offering robust capabilities to align with numerous compliance requirements and standards. This makes it a preferable option for larger enterprises with complex compliance landscapes. MSAT 4.0, while comprehensive, does not offer as many built-in compliance features as SAP GRC but is highly configurable to align with various regulatory needs. CORAS, on the other hand, is more specialized and may require additional configuration to fully meet compliance standards. SimpleRisk, while not as feature-rich in the compliance department, offers basic functionalities that can be tailored to meet the compliance needs of smaller organizations or specific projects.

Finally, the efficient use of resources is a critical factor for organizations in selecting a Security Risk Management framework or tool, as both time and financial constraints play a significant role in the success of any risk management program. In terms of frameworks, ISO 27005:2022 often requires a significant commitment of both time and skilled personnel to implement effectively, given its comprehensive and globally recognized nature. It can be resource-intensive, especially for smaller organizations. NIST SP 800-37, while also robust, offers a modular approach that can be somewhat less taxing on resources if applied strategically. OCTAVE and FAIR, being more specialized, can often be implemented more quickly but may require expertise in specific areas, such as data analytics for FAIR, that could necessitate specialized training or consultants. When it comes to tools, SAP GRC is an enterprise-level solution that offers a host of functionalities but often at a premium price point and with a steep learning curve. It's well-suited for larger organizations that have the budget and personnel to make the most of its capabilities. MSAT 4.0, while extensive, can also be resource-intensive when it comes to customization and alignment with specific compliance standards. CORAS, with its model-based approach, requires expertise in model-driven security, which might necessitate additional training or the hiring of specialists. SimpleRisk, however, offers a simpler, more straightforward solution that can be effective for smaller organizations or individual departments, thereby requiring fewer resources for both implementation and ongoing management.

In conclusion, the choice of risk management frameworks and tools is highly contextual and must be tailored to the organization's specific needs, goals and constraints. Organizations must balance the scales of scalability, feature richness, user-friendliness, compliance alignment, and resource optimization in making their selections. Larger, more resource-rich organizations may gravitate toward ISO 27005:2022, NIST SP 800-37, or SAP GRC. In contrast, smaller or more specialized entities may find the tailored approaches of OCTAVE, FAIR, or SimpleRisk more aligned with their needs.

The landscape of information security risk management is not static and as such, a periodic reassessment of the chosen frameworks and tools effectiveness and relevance is essential for maintaining robust security postures. Therefore, organizations should not only consider the immediate benefits and limitations but also the long-term viability and adaptability of their selected framework. The best tool for any given organization will depend on a complex array of factors including the size of the organization, the expertise of its staff, its specific security needs and the regulatory landscape it operates. As with frameworks, the dynamic nature of the cybersecurity

landscape means that ongoing assessment and adjustment are necessary to ensure that the selected tool remains optimal for an organization's evolving needs.

# 6

## *Conclusion and Recommendations*

### *6.1 Summary of Findings*

This research conducted an in-depth examination of major framework methods and tools applicable to information security risk management. The core objective was to evaluate their respective strengths, limitations and suitability for varied organizational contexts through a robust comparative analysis. The findings reveal that while all the analyzed frameworks and tools offer value, each has distinct characteristics that make them preferable based on an organization's size, sector, risk landscape and resource constraints.

In terms of frameworks, ISO 27005:2022 and NIST SP 800-37 stand out for their comprehensive coverage of risk management processes based on internationally recognized standards. However, this same extensive scope also makes them potentially overwhelming, especially for smaller entities. OCTAVE's emphasis on organizational risk provides an alternative tailored for internal collaboration, but isn't as extensive on the technical aspects. FAIR's quantitative data-driven approach is unmatched but calls for statistical expertise.

Among the tools, SAP GRC leads in enterprise-grade integration, automation and compliance capabilities. Yet these advanced functionalities result in complexity that may warrant dedicated personnel. MSAT 4.0 excels in assessment-focused features but has limitations in compliance alignment and integration. CORAS is exceptional for model-based risk analysis but necessitates specialized skills and SimpleRisk prioritizes ease-of-use for streamlined risk management.

When evaluated on the metrics of scalability, available features, user-friendliness, compliance alignment and resource optimization, each framework and tool exhibits areas of strength and weakness and we can conclude that there is no universal optimal choice. ISO 27005:2022 and NIST SP 800-37 score highly on compliance alignment but are intensive on resources. SAP GRC offers



gold-standard features but has a steep learning curve. SimpleRisk simplifies the user experience but lacks advanced capabilities.

Moreover, the changing cyber risk landscape means frameworks and tools must evolve continually to remain effective. The research highlights that organizations must weigh these criteria based on their unique priorities, constraints and risk environments when selecting frameworks and tools. Regular re-evaluations are key to ensure the selections remain optimally aligned. By combining diligent assessments with a clear focus on strategic needs, organizations can leverage the most suitable framework and tools for their specific context. This research provides a robust basis for making such risk management decisions through its comparative analysis.

## **6.2 Recommendations**

When selecting information security risk management frameworks and tools, organizations must engage in a holistic evaluation process weighing multiple criteria of relevance to their specific context. For large enterprises with extensive resources and complex operations, the unparalleled comprehensiveness of ISO 27005:2022, NIST SP 800-37 and SAP GRC offer the strategic maturity to manage risks with rigor based on globally recognized standards. However, their sophistication necessitates investments in personnel and systems to extract their full value. Small and medium-sized companies often benefit from streamlined solutions like OCTAVE, FAIR and SimpleRisk that simplify training and implementation while providing essential risk management capabilities. Highly regulated sectors such as finance and healthcare, where compliance is paramount, should give priority to frameworks and tools with robust alignment to their specific regulatory environment, making ISO 27005:2022, NIST SP 800-37 and SAP GRC strong choices. For fast-paced industries where agility and adaptability are critical, modular solutions like NIST SP 800-37 and CORAS allow adjustment as threats and regulations evolve.

An organization's existing resources, expertise and technologies also guide appropriate tool selection, with firms possessing complex IT systems and data environments favoring tools like SAP GRC and CORAS for their integration and customization abilities. However, those lacking specialized skills may find options like SimpleRisk more accessible. Regardless of organizational characteristics, integrating periodic re-evaluation of selected frameworks and tools is essential, given the constantly evolving threat landscape. By taking a strategic approach that objectively balances organizational priorities against solution sophistication, entities can determine optimal frameworks and tools for their unique risk profile and resources. This research offers a foundation

to guide such informed decisions through robust, criteria-based comparative analysis of widely used information security risk management frameworks and tools.

### ***6.3 Limitations and Future Expansion***

While the research presented a comprehensive analysis of major information security risk management frameworks and tools, certain limitations provide avenues for future exploration. Firstly, the scope encompassed only select prominent frameworks and tools, excluding newer or more specialized solutions that may offer alternative capabilities. With the continuous evolution of the domain, more frameworks and tools can emerge warranting evaluation. Secondly, the optimality of frameworks and tools can vary based on specific organizational risk profiles, threat environments, regulatory landscapes and business objectives. Additional real-world case studies across different industries could provide further context-specific insights. Thirdly, the rapidly evolving nature of cyber threats necessitates regular re-evaluation of existing frameworks and tools to assess alignment with emerging risks. Longitudinal studies can illuminate how the threat landscape has changed and correspondingly how frameworks and tools have adapted.

As technologies like cloud computing, mobile devices and IoT become ubiquitous, new attack vectors and information security paradigms may develop that call for different risk management approaches. By expanding assessments to encompass innovations in frameworks, tools and organizational contexts, future research can provide wider perspectives. Developing evaluation metrics tailored to emerging technologies could also highlight new selection criteria beyond traditional considerations. Overall, treating risk management selection as a dynamic decision process rather than a one-time event can keep organizations optimally equipped. This study offers a robust foundation, but the changing cyber risk environment warrants ongoing research to guide the application of appropriate frameworks and tools as threats, technologies and business objectives transform.

## References

- ENISA (2023) Risk Management & Information Security Management Systems. Available at: <https://www.enisa.europa.eu/topics/risk-management/current-risk/risk-management-inventory/rm-isms> (Accessed: 2 August 2023).
- Rapid7 (2023) Information Security Risk Management (ISRM) (2023) Rapid7. Available at: <https://www.rapid7.com/fundamentals/information-security-risk-management/> (Accessed: 2 August 2023).
- Hopkin, P. (2018) *Fundamentals of Risk Management: Understanding, Evaluating and Implementing Effective Risk Management*. 5th edition. London New York, NY New Delhi: Kogan Page.
- IT Governance UK (2023). Cyber Risk Management, Available at: <https://itgovernance.co.uk/cyber-security-risk-management> (Accessed: 15 July 2023).
- PracticeTests Academy (2023). Available at: <https://www.studocu.com/en-za/document/independent-institution-of-education-monash-south-africa/financial-accounting/p3-ch10-cyber-security-tools-techniques-and-reporting/10082976> (Accessed: 2 August 2023).
- Dhillon, G. and Backhouse, J. (2001) ‘Current directions in IS security research: Towards socioorganizational perspectives’, *Information Systems Journal*, 11. Available at: <https://doi.org/10.1046/j.1365-2575.2001.00099.x>.
- Von Solms, B. and von Solms, R. (2004) ‘The 10 deadly sins of information security management’, *Computers & Security*, 23(5), pp. 371–376. Available at: <https://doi.org/10.1016/j.cose.2004.05.002>.
- Albrechtsen, E. and Hovden, J. (2010) ‘Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study’, *Computers and Security*, 29(4), pp. 432–445. Available at: <https://doi.org/10.1016/j.cose.2009.12.005>.
- Bulgurcu, B., Cavusoglu, H. and Benbasat, I. (2010) ‘Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness’, *MIS Quarterly*, 34, pp. 523–548. Available at: <https://doi.org/10.2307/25750690>.
- Alcántara, M. and Melgar, A. (2016) ‘Risk Management in Information Security: A Systematic Review’, *Journal of Advances in Information Technology*, 7(1), pp. 1–7. Available at: <https://doi.org/10.12720/jait.7.1.1-7>.

- Bergström, E., Lundgren, M. and Ericson, Å. (2019) 'Revisiting information security risk management challenges: a practice perspective', *Information & Computer Security*, 27(3), pp. 358–372. Available at: <https://doi.org/10.1108/ICS-09-2018-0106>.
- Yang, M. (2022) 'Information Security Risk Management Model for Big Data', *Advances in Multimedia*, 2022, p. e3383251. Available at: <https://doi.org/10.1155/2022/3383251>.
- Deloitte (2019), 'Smart cyber: How AI can help manage cyber risk.', Available at: <https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Risk/gx-ra-smart-cyber.pdf>
- Junior, A. and Arima, C. (2023) 'CYBER RISK MANAGEMENT AND ISO 27005:2022 APPLIED IN ORGANIZATIONS: A SYSTEMATIC LITERATURE REVIEW', *REVISTA FOCO*, 16, p. e1188. Available at: <https://doi.org/10.54751/revistafoco.v16n2-215>.
- Initiative, J.T.F.T. (2012) *Guide for Conducting Risk Assessments*. NIST Special Publication (SP) 800-30 Rev. 1. National Institute of Standards and Technology. Available at: <https://doi.org/10.6028/NIST.SP.800-30r1>.
- Alberts, C., Gordon, P., Dorofee, A., Fuller, J. (2002) *Managing Information Security Risks: The OCTAVE (SM) Approach*. 1st edition. Amsterdam Munich: Addison-Wesley Professional, ISBN-13: 978-0321118868
- Freund, J. and Jones, J. (2014) *Measuring and Managing Information Risk: A FAIR Approach*. 1st edition. Amsterdam: Butterworth-Heinemann, ISBN-13: 978-0124202313
- El Fray, I. (2012) 'A Comparative Study of Risk Assessment Methods, MEHARI & CRAMM with a New Formal Model of Risk Assessment (FoMRA) in Information Systems', in *Computer Information Systems and Industrial Management*. Berlin, Heidelberg: Springer (Lecture Notes in Computer Science), pp. 428–442. Available at: [https://doi.org/10.1007/978-3-642-33260-9\\_37](https://doi.org/10.1007/978-3-642-33260-9_37).
- Karabacak, B. and Sogukpinar, I. (2005) 'ISRAM: information security risk analysis method', *Computers & Security*, 24(2), pp. 147–159. Available at: <https://doi.org/10.1016/j.cose.2004.07.004>.
- Zargar, S.T., Joshi, J., Tipper, D. (2013) *A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks* | *IEEE Journals & Magazine* | *IEEE Xplore*. Available at: <https://ieeexplore.ieee.org/document/6489876> (Accessed: 3 August 2023).
- Heikka J., Baskerville R., Siponen M. (2006) 'A Design Theory for Secure Information Systems Design Methods' Available at: <https://aisel.aisnet.org/jais/vol7/iss11/31/> (Accessed: 3 August 2023).

- ISO (2022), *ISO/IEC 27005:2022:Information security, cybersecurity and privacy protection — Guidance on managing information security risks.*, 4<sup>th</sup> Edition, Available at: <https://www.iso.org/standard/80585.html> (Accessed: 3 August 2023).
- PECB (2023) *ISO/IEC 27005 Information Security Risk Management - EN | PECB*. Available at: <https://pecb.com/en/education-and-certification-for-individuals/iso-iec-27005> (Accessed: 3 August 2023).
- Institute, FAIR (2023) The Importance and Effectiveness of Cyber Risk Quantification. Available at: <https://www.fairinstitute.org/what-is-fair> (Accessed: 8 September 2023).
- Force, J.T. (2018) *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*. NIST Special Publication (SP) 800-37 Rev. 2. National Institute of Standards and Technology. Available at: <https://doi.org/10.6028/NIST.SP.800-37r2>.
- Cuelogic, Technologies (2019) ‘How to make sense of Cybersecurity Frameworks’, *Cuelogic An LTI Company*, 4 July. Available at: <https://www.cuelogic.com/blog/cybersecurity-frameworks> (Accessed: 5 September 2023).
- Caralli A. R., Stevens F. J., Young R. L., Wilson R. W. (2007) *Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process*. Available at: <https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=8419> (Accessed: 2 September 2023).
- CERT (Computer Emergency Response Team) (2008). *Octave® (operationally critical threat, asset, and vulnerability evaluations)*. <http://www.cert.org/octave/>
- Balbix (2022), *FAIR Model for Risk Quantification - Pros and Cons*. Available at: <https://www.balbix.com/insights/fair-model-for-risk-quantification-pros-and-cons/> (Accessed: 9 September 2023).
- Microsoft (2009), *Microsoft Security Assessment Tool*. Available at: <https://www.microsoft.com/en-ie/download/details.aspx?id=12273> (Accessed: 10 September 2023).
- CORAS (2023), *The CORAS Method* (no date). Available at: <https://coras.tools/#/> (Accessed: 11 September 2023).
- Solhaug, B., Stølen, K. (2014) ‘The CORAS Language – why it is designed the way it is’, in G. Deodatis, B. Ellingwood, and D. Frangopol (eds). CRC Press, pp. 3155–3162. Available at: <https://doi.org/10.1201/b16387-456>.
- SimpleRisk (2020), *Risk Management*. Available at: <https://www.simplerisk.com/solutions/risk-management> (Accessed: 15 September 2023).

- SAP (2023), *Cybersecurity and GRC Software*. Available at: <https://www.sap.com/products/financial-management/grc.html> (Accessed: 15 September 2023).
- Winterhawk (2023), *SAP Risk Management*. Available at: <https://winterhawk.com/sap-grc/risk-management/> (Accessed: 15 September 2023).
- JNC Consultancy (2023), '*GRC Implementation*'. Available at: <https://www.jncconsultancy.com/grc-implementation/> (Accessed: 15 September 2023).