University of Piraeus

School of Information and Communication Technologies

Department of Digital Systems

Postgraduate Program of Studies

MSc Digital Systems Security

Analysis of Frameworks/Methods for Information Security Risk Management

Supervisor Professor: Pr. Stefanos Gkritzalis

Name-Surname	E-mail	Student ID.
Theodoros-Alexandros Chandrinos	alexchandrinos@gmail.com	MTE2131

Piraeus

04/05/2023

Abstract

This thesis presents the outcomes of research and analysis of cybersecurity Risk Management (RM) frameworks/methodologies and software tools with the purpose of evaluation and comparison on specific criteria. The identification of the most prominent RM frameworks/methodologies and software tools was based on a systematic survey of related risk management approaches used in various contexts, but mainly in the IT industry. The identified collection of frameworks and methodologies includes well-known and widely used RM standards that provide high-level guidelines for risk management processes applicable in all types of organizations. Additionally, more structured methodologies are identified that follow specific phases or steps to implement RM processes. The main characteristics and features of each identified RM framework and methodology are described. Likewise, all the software tools described in this paper are well-known and widely used by all kinds of industries and organizations. Based on this analysis, we set the evaluation criteria and rate each one of these criteria for every RM framework described, with the purpose of comparing them in order to provide the community with a solid and documented result to help them choose the most fitted RM framework/methodology and software tool based on their needs and purposes.

Table of Content

ACKNOWLEDGEMENTS 1
INTRODUCTION 2
What is Information Security Risk Management 3
Stages of ISRM 4
RISK MANAGEMENT FRAMEWORKS AND METHODOLOGIS 8
ISO/IEC 27005:2018 8
NIST SP 800 Series 10
NIST SP 800-37 REV. 2 10
NIST SP 800–30 REV.1 12
NIST SP 800–39 12
NIST SP 800–82 REV. 2 14
OCTAVE Methodology 15
OCTAVE-S 16
OCTAVE ALLEGRO 16
ISACA RISK IT FRAMEWORK 17
INFORMATION RISK ASSESSMENT METHODOLOGY 2 (IRAM2) 19
ETSI TS 102 165-1, THREAT VULNERABILITY AND RISK ANALYSIS (TVRA) 20
MONARC 22
EBIOS RISK MANAGER 23
RISK MANAGEMENT TOOLS 24
Microsoft Security Assessment Tool 4.0 25
SimpleRisk 26
Modulo Risk Manager 28
Risk Management Studio 29
Practical Threat Analysis (PTA) 31
MONARC 33
VERINICE ISMS 34
vsRisk 35
COMPARISON EVALUATION FRAMEWORK 37
EVALUATIONS 38

ISO 27005:2018 38
NIST SP 800 Series 40
OCTAVE Methodology 41
ISACA RISK IT FRAMEWORK 42
INFORMATION RISK ASSESSMENT METHODOLOGY 2 (IRAM2) 43
ETSI TS 102 165-1, THREAT VULNERABILITY AND RISK ANALYSIS (TVRA) 45
MONARC 46
EBIOS RISK MANAGER 47
Comparison 48
Conclusion on Comparison 51
References 52

ACKNOWLEDGEMENTS

Firstly, I would like to thank Professor Stefanos Gkritzalis, who, as my supervising professor provided me assistance, advice, help but mostly inspiration not only during the conducting of this thesis but generally on my life and business objectives. I would also like to thank my mother and sister and the rest of my family for always being there for me in good and bad times. My friends for still being my friends even though I have been so busy during this journey and all the people who contributed and helped me in general.

INTRODUCTION

Organizations face significant cybersecurity risks and need a robust risk management framework to assess and manage those risks effectively. A risk management framework is essential because risks can never be entirely eliminated but can be managed. Without it, organizations may fall victims to data breaches, ransomware attacks, and all kinds of other security issues.

Effective risk assessment requires a systematic approach that considers all potential risks, evaluates their likelihood and impact, and develops plans to mitigate or manage them. This process involves gathering information, analysing data, and making informed decisions about which risks are most significant and require the most attention.

Risk management involves putting these plans into action and monitoring them over time to ensure that they remain effective. This requires ongoing monitoring and evaluation of potential risks, as well as adapting plans as necessary to ensure that they remain relevant and effective.

Effective risk management can help organizations to minimize the impact of potential risks, protect their assets, and maintain a competitive edge in an ever-changing business environment. It requires a commitment to ongoing evaluation and adaptation, as well as a willingness to invest resources into risk mitigation and management efforts.

As the need for secure computing environments increases, so does the number and diversity of available frameworks. Some frameworks were designed for specific organizations or regulatory compliance goals, while others have a more general security focus. However, many share common security concepts, making them potentially applicable across industries. Organizations should carefully evaluate different frameworks to select the right Information Security Risk Assessment Framework/methodology for their specific needs. When selecting a framework/methodology and a software tool for conducting the information security risk management and applying the aforementioned framework/methodology, it is crucial to ensure that they are well-suited for the intended outcomes and "fit for purpose."

Having in mind this critical aspect when it comes to the selection of those, we aim to present, analyse and evaluate the most well-known and widely used frameworks/methodologies and software tools in order to result to a well-documented

and solid comparison analysis. This comparison will help the analysts of the organizations to make the right decisions having in mind the goals and purpose of their companies.

In this thesis, we will firstly describe what an Information Security Risk Management is, then describe, analyse and present the Identified Risk Management Frameworks and Methodologies, following we will describe and analyse the Identified Risk Management Tools and finally the Comparison and Evaluation of the Frameworks, where the criteria of comparison will be stated as well as the rating scale which was used.

What is Information Security Risk Management

ISRM is part of an overall information management strategy and a key component of any company's cyber security. The goal of information security risk management is to identify and mitigate threats to the company's data, networks, and systems. It also helps in identifying the root cause of the problem and making sure that it doesn't happen again.

Information security risk management is a critical component of any organization's overall risk management strategy, especially in today's digital age where cyber threats are becoming increasingly prevalent and sophisticated.

The importance of information security risk management cannot be stressed enough. If an organization fails to do so, its data might get leaked or stolen which can lead to huge financial losses for them.

ISRM process has many benefits:

- It helps in identifying the vulnerabilities of an information system.
- It helps in determining the degree of vulnerability and possible impact on the organization.
- It helps in determining the best way to manage a given risk by evaluating its cost and likelihood of occurrence, as well as its impact on organizational objectives.
- It provides an opportunity for organizations to develop proactive strategies for managing risks and their consequences.
- It provides a systematic way for an organization to identify potential threats and vulnerabilities, as well as to manage them proactively before they can cause significant harm or damage.

Effective ISRM requires a proactive approach and collaboration between various stakeholders, including IT, legal, compliance, and business leaders. It also requires ongoing investment in technology, training, and other resources to stay ahead of

emerging threats and ensure that an organization's information assets are adequately protected.

ISRM involves a series of steps, including:

- Risk identification: identifying potential risks to an organization's information assets, such as data breaches, insider threats, malware attacks, and phishing scams.
- Risk assessment: evaluating the likelihood and impact of identified risks, using methods such as risk analysis, vulnerability assessment, and threat modeling.
- Risk treatment: developing and implementing strategies to mitigate, transfer, accept, or avoid identified risks based on an organization's risk tolerance and overall business objectives.
- Risk monitoring: continually monitoring and reviewing risks to ensure that the implemented risk treatments remain effective and relevant.

These stages of an ISRM are described in more detail bellow.

Stages of ISRM

Identification

- Identify assets: What data, systems, or other assets would be considered your organization's "crown jewels"? For example, which assets would have the most significant impact on your organization if their confidentiality, integrity or availability were compromised? It's not hard to see why the confidentiality of data like social security numbers and intellectual property is important. But what about integrity? For example, if a business falls under Sarbanes-Oxley (SOX) regulatory requirements, a minor integrity problem in financial reporting data could result in an enormous cost. Or, if an organization is an online music streaming service and the availability of music files is compromised, then they could lose subscribers.
- Identify vulnerabilities: What system-level or software vulnerabilities are putting the confidentiality, integrity, and availability of the assets at risk? What weaknesses or deficiencies in organizational processes could result in information being compromised?
- Identify threats: What are some of the potential causes of assets or information becoming compromised? For example, is your organization's data centre located in a region where environmental threats, like tornadoes and floods, are more prevalent? Are industry peers being actively targeted and hacked by a known crime syndicate, hacktivist group, or government-sponsored entity? Threat modelling is an important activity that helps add context by tying risks to known threats and the different ways those threats can cause risks to become realized via exploiting vulnerabilities.
- Identify controls: What do you already have in place to protect identified assets? A control directly addresses an identified vulnerability or threat by either completely fixing it (remediation) or lessening the likelihood and/or impact of a risk being realized (mitigation). For example, if you've identified a risk of terminated users continuing to have access to a specific application, then a control could be a process that automatically removes users from that application upon their termination. A compensating control is a "safety net" control that indirectly addresses a risk. Continuing with the same example above, a compensating control may be a quarterly

access review process. During this review, the application user list is cross-referenced with the company's user directory and termination lists to find users with unwarranted access and then reactively remove that unauthorized access when it's found.

Assessment

This is the process of combining the information you've gathered about assets, vulnerabilities, and controls to define a risk.

Treatment

Once a risk has been assessed and analysed, an organization will need to select treatment options:

- Remediation: Implementing a control that fully or nearly fully fixes the underlying risk.
- Example: You have identified a vulnerability on a server where critical assets are stored, and you apply a patch for that vulnerability.
- Mitigation: Lessening the likelihood and/or impact of the risk, but not fixing it entirely.
- Example: You have identified a vulnerability on a server where critical assets are stored, but instead of patching the vulnerability, you implement a firewall rule that only allows specific systems to communicate with the vulnerable service on the server.
- Transference: Transferring the risk to another entity so your organization can recover from incurred costs of the risk being realized.
- Example: You purchase insurance that will cover any losses that would be incurred if vulnerable systems are exploited. (Note: this should be used to supplement risk remediation and mitigation but not replace them altogether.)
- Risk acceptance: Not fixing the risk. This is appropriate in cases where the risk is clearly low and the time and effort it takes to fix the risk costs more than the costs that would be incurred if the risk were to be realized.
- Example: You have identified a vulnerability on a server but concluded that there is nothing sensitive on that server; it cannot be used as an entry point to access other critical assets, and a successful exploit of the vulnerability is very complex. As a result, you decide you do not need to spend time and resources to fix the vulnerability.
- Risk avoidance: Removing all exposure to an identified risk.
- Example: You have identified servers with operating systems (OS) that are about to reach end-of-life and will no longer receive security patches from the OS creator. These servers process and store both sensitive and non-sensitive data. To avoid the risk of sensitive data being compromised, you quickly migrate that sensitive data to newer, patchable servers. The servers continue to run and process non-sensitive data while a plan is developed to decommission them and migrate non-sensitive data to other servers.

Communication

Regardless of how a risk is treated, the decision needs to be communicated within the organization. Stakeholders need to understand the costs of treating or not treating a risk and the rationale behind that decision. Responsibility and accountability need to be clearly defined and associated with individuals and teams in the organization to ensure the right people are engaged at the right times in the process.

Rinse and Repeat

This is an ongoing process. If you chose a treatment plan that requires implementing a control, that control needs to be continuously monitored. You're likely inserting this control into a system that is changing over time. Ports being opened, code being changed, and any number of other factors could cause your control to break down in the months or years following its initial implementation.

Ownership： There are many stakeholders in the ISRM process, and each of them have different responsibilities. Defining the various roles in this process, and the responsibilities tied to each role, is a critical step to ensuring this process goes smoothly.

Process Owners: At a high level, an organization might have a finance team or audit team that owns their Enterprise Risk Management (ERM) program, while an Information Security or Information Assurance team will own ISRM program, which feeds into ERM. Members of this ISRM team need to be in the field, continually driving the process forward.

Risk Owners: Individual risks should be owned by the members of an organization who end up using their budget to pay for fixing the problem. In other words, risk owners are accountable for ensuring risks are treated accordingly. If you approve the budget, you own the risk.

In addition to risk owners, there will also be other types of stakeholders who are either impacted by, or involved in implementing, the selected treatment plan, such as system administrators/engineers, system users, etc.

Here's an example: Your information security team (process owner) is driving the ISRM process forward. A risk to the availability of your company's customer relationship management (CRM) system is identified, and together with your head of IT (the CRM system owner) and the individual in IT who manages this system on a day-to-day basis (CRM system admin), your process owners gather the information necessary to assess the risk.

Assuming your CRM software is in place to enable the sales department at your company, and the data in your CRM software becoming unavailable would ultimately impact sales, then your sales department head (i.e. chief sales officer) is likely going to be the risk owner. The risk owner is responsible for deciding on implementing the different treatment plans offered by the information security team, system administrators, system owners, etc. and accepting any remaining risk; however, your

system owner and system admin will likely be involved once again when it comes time to implement the treatment plan. System users—the salespeople who use the CRM software on a daily basis—are also stakeholders in this process, as they may be impacted by any given treatment plan.

Managing risk is an ongoing task, and its success will come down to how well risks are assessed, plans are communicated, and roles are upheld. Identifying the critical people, processes, and technology to help address the steps above will create a solid foundation for a risk management strategy and program in your organization, which can be developed further over time.

RISK MANAGEMENT FRAMEWORKS AND METHODOLOGIS

ISO/IEC 27005:2018

ISO/IEC 27005:2018 [1] 'Information technology — Security techniques — Information security risk management' is a risk management framework that provides guidance for all types of organizations to manage risks that could compromise their information security. It supports the general concepts specified in ISO/IEC 27001 for information security management and is designed to assist in the implementation of information security using a risk management approach. The framework includes a set of sub-processes that comprise the information security risk management process. These sub-processes are:

- Risk assessment: This sub-process involves identifying the risks to the organization's information security and analysing their likelihood and potential impact.
- Risk evaluation: This sub-process involves evaluating the identified risks to determine their significance and prioritize them based on their potential impact and likelihood.
- Risk treatment: This sub-process involves selecting and implementing risk treatment options to address the identified risks. The risk treatment options may include risk avoidance, risk reduction, risk sharing, or risk acceptance.
- Risk acceptance: This sub-process involves formally accepting the residual risks that remain after risk treatment has been implemented.
- Risk communication: This sub-process involves communicating information about the identified risks, their potential impact, and the risk treatment options to stakeholders.
- Risk monitoring and review: This sub-process involves monitoring and reviewing the effectiveness of the risk treatment measures and making adjustments as necessary to ensure that the organization's information security remains adequate.

Risk identification is an important step in the risk management process. It involves identifying and analysing potential risks that could impact an organization's information security. This includes identifying assets (e.g. data, systems, facilities), potential threats (e.g. natural disasters, cyber-attacks), existing controls, vulnerabilities (e.g. weaknesses in systems or processes), and potential impacts (e.g. financial loss, reputational damage). The goal of risk identification is to gain a comprehensive understanding of the organization's risk landscape and to identify potential areas of vulnerability that require further assessment and mitigation. By identifying and analysing potential risks, organizations can make informed decisions about risk mitigation strategies and allocate resources effectively.

Risk estimation according to ISO 27005:2018 could be qualitative, quantitative or hybrid. To elaborate further, qualitative risk estimation involves evaluating the likelihood and consequences of a risk using descriptive terms such as low, medium, or high. Quantitative risk estimation involves using numerical values to assess likelihood and consequences, such as assigning probabilities or monetary values. A hybrid approach combines elements of both qualitative and quantitative methods. The choice of risk estimation method depends on the organization's needs and available resources. ISO 27005:2018 recommends that the risk estimation process should consider the organization's risk tolerance level, which is the acceptable level of risk that the organization is willing to accept. This helps the organization make informed decisions on risk treatment options. Additionally, ISO 27005:2018 recommends that the risk estimation process should consider the likelihood and impact of multiple risks occurring simultaneously, also known as "combinatorial risk."

At the stage of risk evaluation, the list of risks and assigned value levels are compared against criteria for risk evaluation. Based on the results of risk evaluation, risk treatment decisions are made. Four options are proposed for risk treatment: risk modification, risk retention, risk avoidance, and risk sharing. ISO 27005:2018 recommends that risk treatment options should be evaluated based on the effectiveness of the options, their cost, feasibility, and the organization's risk tolerance. The selected risk treatment options should also take into account legal, regulatory, and contractual requirements. Regarding risk modification, ISO 27005:2018 recommends that organizations apply security controls based on ISO 27001:2013. These controls can be selected based on the risk assessment and the organization's risk treatment decisions. ISO 27001:2013 provides a set of controls organized in 14 categories, and organizations can select the controls that are relevant to their specific risks and security needs.

Risk retention involves accepting the risk and its potential consequences without taking any further action to reduce the risk. Risk avoidance involves taking steps to eliminate the risk, such as discontinuing a particular business activity or outsourcing a high-risk process. Risk sharing involves transferring the risk to another party, such as an insurance company.

The chosen risk treatment options should be documented in a risk treatment plan, which outlines the actions to be taken, the responsibilities of stakeholders, and the timeline for implementing the plan.

Risk monitoring and review is an important phase in the ISO 27005:2018 risk management process. It involves the continuous monitoring and review of the effectiveness of the risk management process, risk treatment plans, and implemented security controls. This phase is important to ensure that the risk management process is effective and that the organization is meeting its objectives. Risk monitoring and review activities typically involve regular reviews of the risk management process and its effectiveness, including the identification of new risks or changes to existing risks, the re-evaluation of existing risks, and the review of risk treatment plans and implemented security controls. The results of these activities should be documented and reported to senior management for review and decision-making. In addition, the risk monitoring and review phase may include regular audits or assessments of the risk management process and its effectiveness, as well as ongoing training and awareness activities for employees to ensure that they understand their roles and responsibilities in managing information security risks.

Overall, ISO/IEC 27005:2018 provides a comprehensive framework for information security risk management that can be adapted to suit the needs of different types of organizations. By adopting this framework, organizations can effectively manage their information security risks, reduce potential losses, and enhance their overall security posture.

NIST SP 800 Series

The NIST SP 800 Series comprises a collection of documents that offer policies, procedures, and guidelines for computer security to the US Federal Government. Compliance with NIST is obligatory for all federal agencies. These publications can serve as a roadmap for implementing security measures or as legal references for litigation related to security concerns.

NIST SP 800-37 REV. 2

NIST SP 800-37 [2] is created to cater to the needs of Federal Information Systems and comply with various regulations such as FISMA, Privacy Act of 1974, OMB policies, and Federal Information Processing Standards. This framework is not limited to government entities and can be implemented by any organization, including those in the private sector.

NIST SP 800-37 Rev. 2 is a risk management framework that is based on assets and consists of 7 steps: Prepare, Categorize, Select, Implement, Assess, Authorize, and Monitor. While it does not prescribe a particular risk assessment methodology, it does reference the NIST 800-30 guide. The framework includes mandatory tasks for each step, with some optional tasks available as well. It is expected that organizations will complete all but the optional tasks when implementing the RMF.

- **Prepare** establishes context and priorities for security and privacy risk management, identifies and assigns roles to execute the RMF, sets organisational priorities, risk tolerances etc.
- **Categorise** assesses the impact of an adversary's action for operations, individuals and assets, including information processed by systems within scope (Risk identification).
- During subsequent steps the appropriate controls are **selected**, **implemented** and **assessed**, based on their effectiveness (Risk treatment).
- The **authorisation** step requires a senior management official to determine when the privacy and security risks are acceptable (Risk treatment).
- The goal of the **monitor** step is to continue performing risk assessments and impact analyses, and to document any system changes (Risk Monitoring).

The NIST SP 800-37 Rev. 2 standard does not prescribe a particular risk assessment methodology and therefore does not provide specific guidance on assets and their taxonomies, threat and vulnerability catalogues, or risk calculation methods. However, it does reference other relevant NIST standards such as the NIST Cyber Security Framework (CSF) and the NIST Security and Privacy Controls (NIST SP 800-53).

Overall, NIST SP 800-37 Rev. 2 provides a comprehensive and flexible risk management framework that can be used by any type of organization to manage their information security risks. While it does not prescribe a specific risk assessment methodology, it provides a structure for organizations to prepare for and manage risks throughout the system life cycle. The framework is asset-based and includes seven steps that organizations can follow to manage their risks effectively. Additionally, the framework references other NIST standards, including the NIST Cybersecurity Framework and the NIST Security and Privacy Controls, which can provide additional guidance and best practices for organizations to consider and we will analyse them bellow.

NIST SP 800–30 REV.1

NIST (SP) 800-30 Rev. 1 [3] entitled ‘Guide for Conducting Risk Assessments’, is a standard published by the National Institute of Standards and Technology (NIST) on September 12, 2012. Its purpose is to provide guidance for assessing risks related to federal information systems and organizations, building on the principles and recommendations in SP 800-39. The standard aims to assist organizations in better managing IT-related risks by outlining a three-component approach: Risk Assessment, Risk Treatment, and Risk Monitoring. More specifically, the NIST SP 800-30 standard:

- describes as risk assessment the use of risk to determine the extent of a potential threat in order to identify appropriate controls for reducing or eliminating risk during the risk mitigation process, and this corresponds to risk assessment in the risk management framework.
- describes risk treatment as risk mitigation, which involves prioritising, evaluating, and implementing the appropriate risk-reducing controls as recommended by the assessment of risk.
- describes risk monitoring, which is the final functional component, as evaluation and assessment that continually updates and expands the systems and the software applications to assess the effectiveness of the security controls.

In conclusion, the NIST (SP) 800-30 Rev. 1 standard is a comprehensive guide for conducting risk assessments of federal information systems and organisations. It provides a methodology for identifying potential threats and appropriate controls for reducing or eliminating risks during the risk mitigation process. The standard includes three functional components: risk assessment, risk treatment, and risk monitoring. Risk assessment involves the use of risk to determine the extent of potential threats, while risk treatment prioritizes, evaluates, and implements risk-reducing controls. Finally, risk monitoring continually updates and expands systems and software applications to assess the effectiveness of security controls. By following the guidance in NIST SP 800-30, organisations can better manage the risks associated with IT-related missions.

NIST SP 800–39

The final version of the NIST SP 800-39 [4], entitled ‘Managing information security risk’, was published by the National Institute of Standards and Technology (NIST) in March 2011.

The purpose of NIST SP 800-39 aims to offer a flexible and organized approach for managing information security risk to an organization's operations, assets, individuals, and reputation on a continuous basis. The standard can be used in conjunction with

other NIST security standards and guidelines to ensure effective assessment, response, and monitoring of enterprise risk.

While initially intended for companies deemed part of the US critical infrastructure, many public and private sector organizations, including federal agencies, have adopted the NIST SP 800-39 framework as either an Information Security Risk Management Framework or as part of a larger Enterprise Risk Management (ERM) program. In the latter case, the framework does not replace other risk-related activities, programs, processes, or approaches that cover risk management related to other laws, directives, policies, programmatic initiatives, or strategic mission or business requirements. It is essential to implement the framework with guidance from professionals who possess expertise in both information security and risk management.

According to NIST SP 800-39, risk management should be approached as a comprehensive, organization-wide activity that encompasses risk at both strategic and tactical levels, with risk-based decision-making integrated into every aspect of the organization. The standard outlines the following components of risk management in this context:

- **Frame risk** (i.e. establish the context for risk-based decisions): To frame risk means to establish the context within which risk-based decisions will be made. This involves identifying and defining the scope of the risk management process, including the organisational objectives, stakeholders, and external factors that may impact the organisation's ability to achieve its objectives. This component maps to the **Risk Identification** phase of the risk management process.
- **Assess risk**: The "Assess risk" component in NIST SP 800-39 refers to the process of evaluating the likelihood and impact of risks to the organization's operations, assets, and individuals, taking into account the risk factors identified during the previous step of risk identification. This step involves analysing the identified risks based on their likelihood, impact, and the organization's risk tolerance level. The outcome of this step is a **Risk Assessment** report that identifies the most critical risks that require immediate attention and provides recommendations for risk treatment.
- **Respond to risk once determined**: once it has been determined is a component of the **Risk Treatment** phase. This involves selecting, implementing, and reviewing security controls to mitigate the identified risks. The response should align with the organization's risk management strategy and should prioritize risk mitigation efforts based on the potential impact to the organization.
- **Monitor risk**: Monitoring risk on an ongoing basis is an essential component of risk management. This involves using effective communication within the organization and establishing a feedback loop to continuously improve risk-related activities. This component is mapped to the Risk Monitoring step in the NIST RMF.

The risk management process is implemented across the organisation in a 3-tiered approach that covers risk at the organisational level, the mission or business process

level, and the information system level. The RM process is integrated across the three tiers with the goal of continuously enhancing the organization's risk-related activities, ensuring effective communication and collaboration between stakeholders who share a vested interest in the mission or business success of the organization.

In conclusion, NIST SP 800-39 is a comprehensive framework for managing information security risk in an organization. It provides a structured, yet flexible approach that can be used by organizations to manage risks to their operations, assets, individuals, and reputation on an ongoing basis. The framework consists of four components: framing risk, assessing risk, responding to risk, and monitoring risk. These components are integrated throughout the organization via a 3-tiered approach that addresses risk at the organizational, mission or business process, and information system levels. The framework can be used in conjunction with other NIST security standards and guidelines to ensure a specific and proper assessment, response, and monitoring of enterprise risk. Although it was designed for US critical infrastructure companies, many other organizations in the private and public sectors are using it either as an Information Security Risk Management Framework or as part of a more comprehensive Enterprise Risk Management program. To implement the framework, it is recommended to seek professional guidance from people who have expertise in both information security and risk management. Overall, the NIST SP 800-39 framework provides a holistic approach to managing risks that ensures risk-based decision-making is integrated into every aspect of the organization.

NIST SP 800–82 REV. 2

NIST SP 800-82 Rev. 2 [5], titled 'Guide to industrial control systems (ISC) security', is a technical guide aimed at providing guidance on securing Industrial Control Systems (ICS), including SCADA systems, DCS, and other control system configurations like PLCs. It was first published in May 2013 and revised in May 2015. The guide addresses the unique performance, reliability, and safety requirements of ICS while providing guidance on how to secure them. The intended audience should have a general understanding of computer security concepts and communication protocols as the guide is technical in nature.

The Risk Management Process has four components: framing, assessing, responding and monitoring. These activities are interdependent and often occur simultaneously

within an organization. Risk Management is a continuous process, meaning that each component involves ongoing activities that help organizations stay up to date with the latest risks and potential threats to their assets. This way, they can effectively manage risks and maintain the safety and security of their operations.

- The **framing** component consists of developing a framework for making decisions on the management of risk. The framing component is highly dependent on the specific context of each organization, and it aims to establish the necessary governance structure to manage risk effectively. This involves identifying key stakeholders, defining the scope and boundaries of the risk management process, and establishing the risk management policies, procedures, and guidelines that will guide the process. The framing component provides the foundation for the subsequent risk management activities and helps ensure that all stakeholders understand their roles and responsibilities in managing risk.
- **Assessing** risk is the process of identifying potential threats and vulnerabilities that could cause harm to an organization. This component of the risk management process also involves evaluating the likelihood of such events occurring and the potential impact they could have. This information is then used to prioritize risks and develop appropriate risk mitigation strategies. The DHS National Cybersecurity & Communications Integration Center (NCCIC) plays a key role in assessing cybersecurity risks and coordinating responses to incidents at a national level.
- The **response** component of the Risk Management Process involves establishing a consistent, organisation-wide approach to address identified risks. It involves taking actions to respond to the identified risks, which can include accepting, avoiding, mitigating, sharing, transferring, or implementing a combination of these options. The response options are limited by system requirements, potential adverse impacts on operations, or regulatory compliance requirements.
- **Monitoring** component is an ongoing activity that tracks the implementation of chosen risk management strategies, identifies changes in the environment that may affect the calculation of risk, and evaluates the effectiveness and efficiency of activities aimed at reducing risk. It is a crucial component that impacts all other components of the risk management process.

OCTAVE Methodology

The OCTAVE Method (Operationally Critical Threat, Asset, and Vulnerability Evaluation) (Alberts, et al., 1999) was developed in 1999 at the Software Engineering Institute. Since then, it has been updated and diverse versions have been published. It adopts an asset-based, strategic assessment of information security risk to be applied in large, hierarchic organizations.

OCTAVE-S

OCTAVE-S is a security approach based on the OCTAVE method that is self-directed, which means that individuals within an organization take responsibility for developing the organization's security strategy. It is designed for small organizations with limited resources and can be led by a small, interdisciplinary team of 3-5 people who gather and analyse information to create a protection strategy and mitigation plans specific to the organization's unique operational security risks. To effectively implement OCTAVE-S, the team must have a comprehensive understanding of the organization's business and security processes in order to carry out all activities on their own.
OCTAVE-S follows three phases.

- The objective of **Phase 1** is to create threat profiles based on assets by establishing impact evaluation criteria, identifying crucial organisational assets, and specifying security requirements. During this phase, the team selects three to five critical assets for in-depth analysis, based on their importance to the organization, and develops a threat profile for each of them.
- **Phase 2** of the process involves identifying infrastructure vulnerabilities. This is done by analysing how people use the computing infrastructure to access critical assets and by identifying who is responsible for configuring and maintaining critical components.
- **Phase 3** of the OCTAVE-S involves identifying risks to the critical assets of the organization and developing a protection strategy along with mitigation plans to address the risks. The process is supported by worksheets provided by OCTAVE-S.

In summary, OCTAVE-S is a self-directed approach to security strategy development that is tailored to small organizations with limited means and resources. It is led by a small, interdisciplinary team who gather and analyse information about the organization's business and security processes to identify critical assets and their associated threats and vulnerabilities. The approach follows three phases: asset-based threat profiling, identification of infrastructure vulnerabilities, and creation of protection strategies and mitigation plans. By following these phases, the team can develop a comprehensive security strategy that addresses the unique operational security risks of the organization.

OCTAVE ALLEGRO

The OCTAVE Allegro method [6] is a self-directed risk assessment methodology that follows the OCTAVE approach. It is designed to assess an organization’s operational risk environment broadly, with the aim of producing robust results without requiring extensive knowledge of risk assessment. Unlike previous OCTAVE approaches,

OCTAVE Allegro focuses primarily on information assets and their usage, storage, transportation, processing, and exposure to threats, vulnerabilities, and disruptions.
OCTAVE Allegro is a risk assessment methodology that can be conducted in a workshop-style manner using guidance, worksheets, and questionnaires. Unlike previous OCTAVE approaches, OCTAVE Allegro focuses on information assets and their use, storage, transport, processing, and exposure to threats, vulnerabilities, and disruptions. It is well-suited for conducting risk assessments with minimal organizational involvement, expertise, or input and can be performed by a small team consisting of members from the operational or business units and the IT department of the organization.
OCTAVE Allegro consists of eight steps that are organized into four phases.

- **In phase 1** of risk management, the organization establishes a framework for risk assessment by developing criteria for measuring risk that align with organizational drivers.
- **In phase 2**, OCTAVE Allegro profiles critical information assets by establishing clear boundaries for the assets, identifying their locations (such as where they are stored, transported, or processed), and determining their security requirements.
- **In phase 3** of the OCTAVE Allegro method, the focus is on identifying threats to the critical information assets in the context of where they are stored, transported, or processed. The team will then move on to identify and analyse the risks associated with these threats. Based on this analysis, the team will develop strategies for mitigating these risks to ensure the protection of the information assets.
- **In phase 4** of OCTAVE Allegro, the team develops an action plan to address the identified risks and vulnerabilities. This involves prioritizing risks and determining appropriate risk management strategies, such as accepting, mitigating, transferring, or avoiding risks. The team also creates a roadmap for implementation, assigns responsibilities, and establishes a timeline for completion. Additionally, ongoing monitoring and review of the risk management plan are conducted to ensure its effectiveness and to identify any necessary adjustments.

Octave Allegro is a flexible method that can be tailored for most organizations, it is driven by operational risk and security practices and it provides practical guidance, worksheets, and examples.

ISACA RISK IT FRAMEWORK

The Information Systems Audit and Control Association (ISACA) [7] created the Risk IT Framework in 2009 (1st edition) to address the need for a bridge between general risk management principles and detailed IT risk management frameworks, which were primarily focused on security issues.

The Risk IT Framework operates at the convergence of business and IT and enables organizations to manage and potentially benefit from risks while striving for their goals. It expands the globally recognized IT governance framework, COBIT, by offering a complete view of risks connected to the use of IT and a detailed approach to risk management, from leadership's tone and culture to operational concerns.

The Risk IT Framework is universally applicable and can be used across various industries and types of organizations. It allows enterprises to comprehend and oversee their exposure to harm, loss or danger arising from the use of information and communications technology, digital or electronic communications, and electronic data. It is essential to implement the framework under the professional guidance of individuals with expertise in information security, risk management, and governance.

The Risk IT Framework is designed to provide enterprises with a process model for governing and managing IT risk through a set of guiding principles and supporting practices. By focusing on areas of IT-related business risk, it enables enterprises to achieve their objectives, take advantage of opportunities, and reduce risk exposure. It addresses various types of IT risks, such as late project delivery, compliance, misalignment, obsolete IT architecture, and IT service delivery problems. The framework outlines key activities for each process, assigns responsibilities, facilitates information flows between processes, and provides guidance for performance management. To ensure effective implementation, the framework should be guided by professionals with expertise in information security, governance, and risk management.

The Risk IT Framework consists of three domains, which are Risk Governance, Risk Evaluation, and Risk Response. Each domain includes three processes that need to be executed for effective IT risk management.:

- Risk Governance
  - establish and maintain a common risk view.
  - integrate with enterprise risk management.
  - make risk-aware business decisions.
- Risk Evaluation (maps to Risk Identification & Assessment)
  - collect data.
  - analyse risk.
  - maintain risk profile.
- Risk Response (maps to Risk Treatment)
  - articulate risk.
  - manage risk.
  - react to events.

The Risk Management Workflow is a flexible process that can be adapted to the needs of each enterprise, and it consists of several major phases that do not necessarily need to be executed sequentially. The process starts with setting the context, including communication, after determining the types and categories of risks, such as strategic, operational, IT risk, cybersecurity, and information security. The next phases include **Risk Identification** and **Risk Assessment**, **Risk Analysis** and **Business Impact Evaluation**, **Risk Response**, and **Risk Reporting and Communication**. Each enterprise should develop a workflow that supports the most efficient and effective means to accomplish necessary tasks.

To summarize, the Risk IT Framework provides a methodical approach for enterprises to comprehensively manage various IT risks, regardless of their control frameworks. This framework enables organizations to identify and assess current and potential risks and establish suitable operational capabilities to ensure that business processes remain operational in adverse situations.

INFORMATION RISK ASSESSMENT METHODOLOGY 2 (IRAM2)

IRAM2 stands for "Information Risk Analysis Methodology 2" and is a comprehensive methodology for identifying, assessing, and managing information risk. It was developed by the Information Security Forum (ISF), a leading global authority on cybersecurity and information risk management. IRAM2 is designed to be flexible and scalable, making it suitable for organizations of all sizes and in all industries. It can be used as a standalone methodology or integrated with other risk management frameworks, such as ISO 27001 and NIST SP 800-53.

The methodology provides a framework for assessing risks to an organization's information assets and determining appropriate controls to mitigate those risks. It takes a holistic approach to risk management, focusing on the entire information lifecycle and the various threats and vulnerabilities that can affect information at each stage. IRAM2 is based on a four-step process:

- **Scoping** and **Planning**: This involves identifying the scope of the risk assessment, defining the objectives and methodology, and obtaining stakeholder buy-in.
- **Asset Identification** and **Valuation**: This step involves identifying and valuing the information assets that are critical to the organization's operations and defining the associated risks.

- **Threat Assessment** and **Vulnerability Assessment**: This step involves assessing the likelihood and impact of potential threats to the identified assets and identifying the vulnerabilities that could be exploited by those threats.
- **Risk Evaluation** and **Risk Treatment**: This step involves evaluating the risks to the identified assets and determining the appropriate controls to mitigate those risks.

IRAM2 is implemented by an automated toolset also developed by the ISF. The toolset is accessible exclusively to ISF members, with supplementary support documentation and consultancy being offered by ISF to assist with its use.

Overall, IRAM2 is a robust and effective methodology for managing information risk and is widely used by organizations around the world.

ETSI TS 102 165-1, THREAT VULNERABILITY AND RISK ANALYSIS (TVRA)

ETSI TS 102 165-1 provides a methodology and pro-forma for conducting a threat, vulnerability, and risk analysis (TVRA). TVRA [8] is used to identify the risks to an information system by considering the likelihood of an attack and the impact that the attack could have on the system.

The TVRA methodology offers a systematic approach for documenting the reasoning behind the implementation of security measures in a system. It enables the visualisation of the connection between objectives, requirements, system design, and vulnerabilities by employing a structured approach. The methodology assesses and quantifies the assets, threats, and vulnerabilities associated with a system. The primary focus is on the system's assets to ensure that they can continue to operate effectively when faced with a malicious attack. The result of the TVRA process is a measure of the risk to the assets and a set of specific security requirements to reduce that risk.

The TVRA process consists of the following steps:

- **Step 1:** The first step in the TVRA process is to identify the target of evaluation (TOE), which involves creating a high-level description of the main assets of the TOE and the TOE environment. This step also includes specifying the goal, purpose, and scope of the TVRA. By identifying the TOE and defining its objectives, the TVRA process can be focused on the specific system or environment being evaluated, ensuring that the analysis is relevant and effective.
- **Step 2:** In the TVRA process, the second step is the identification of the objectives. This step results in a high-level statement of the security aims and issues that need to be resolved. By identifying the objectives, the security aims of the organization are established, and the issues that need to be addressed are defined. This helps to ensure that the TVRA is focused on the most important security issues and that the objectives are clearly defined, measurable and achievable. The objectives should be aligned with

the organization's overall goals and should take into account any legal, regulatory, or contractual requirements that may apply.

- **Step 3:** In this step, functional security requirements are identified based on the objectives identified in step 2. The functional security requirements specify the features, capabilities, and functionalities that are necessary to achieve the security objectives. These requirements are derived from the objectives and should be specific, measurable, achievable, relevant, and time-bound. The functional security requirements can include but are not limited to access control, authentication, encryption, data backup, and disaster recovery. The identification of functional security requirements is essential to ensure that the security objectives are achieved through the implementation of specific security controls.
- **Step 4:** In step 4, a comprehensive inventory of the assets is created. This is achieved by refining the high-level asset descriptions from step 1, and by identifying additional assets resulting from steps 2 and 3. The assets may include hardware, software, data, and personnel. Each asset is described in detail, including its purpose, function, and criticality to the system. This step ensures that all assets that are essential to the system are identified and considered in the TVRA process.
- **Step 5:** The focus now is on identifying and classifying vulnerabilities in the system. This includes determining the specific weaknesses and flaws that could be exploited to compromise the security of the system. Once vulnerabilities are identified, potential threats that could exploit them are identified and classified. Additionally, the unwanted incidents that may occur if the threats exploit vulnerabilities are determined. This step is crucial as it enables the organization to understand the potential risks that the system is facing.
- **Step 6:** Quantifying the likelihood of an occurrence and impact of the threats involves assessing the probability of a threat occurring and the potential impact it could have on the system or assets. This step helps in determining the level of risk associated with each threat and prioritizing them for further analysis and response.
- **Step 7:** After quantifying the likelihood and impact of threats, the next step is to establish the risks associated with them. This involves assessing the probability of the threats occurring and the potential impact they could have on the system assets. By combining these factors, risks can be prioritized and further analysed to determine the appropriate risk response strategies.
- **Step 8:** In this step, a conceptual framework of countermeasures is identified. This involves developing a list of alternative security services and capabilities that can be implemented to reduce the risks identified in the previous steps. The list should be based on the identified vulnerabilities, threats, and risks, as well as the functional security requirements derived from the objectives. The focus should be on selecting the most effective and efficient countermeasures to address the risks. The result of this step is a list of potential countermeasures that can be used to mitigate the identified risks.
- **Step 9:** In this step, a cost-benefit analysis is performed on the list of countermeasures identified in step 8. The analysis takes into account the cost of implementing each countermeasure as well as its potential benefits in terms of reducing risk. The scope and purpose of the TVRA are considered when conducting the cost-benefit analysis of security requirements. The goal is to identify the most effective and efficient security services and capabilities among the alternatives identified in step 8. This step helps organizations make informed decisions about which countermeasures to implement and prioritize based on their budget, resources, and risk management objectives.
- **Step 10:** After identifying the best-fit security services and capabilities from step 9, the next step is to specify the detailed requirements for those security services and

> capabilities. This involves defining the specific actions or measures that need to be taken in order to implement the chosen countermeasures. These requirements may include technical specifications for hardware or software, procedures for implementing and maintaining security measures, and training requirements for personnel who will be responsible for implementing and operating the security measures. The goal is to ensure that the chosen countermeasures are effectively implemented and can be maintained over time to provide ongoing protection against identified risks.

The application of countermeasures adds assets to the system and may create new vulnerabilities, indicating that the TVRA will need to be undertaken again, and the method should be repeated until all the risks have been reduced to an acceptable level.

MONARC

MONARC (Méthode Optimisée d'analyse des risques CASES – 'Method for an Optimised Analysis of Risks by CASES' [9] is both a tool and a method designed for conducting accurate and consistent risk assessments. It was developed in 2013 by the Cyberworld Awareness Security Enhancement Services (CASES) department of the Cybersecurity Agency for the Luxembourg Economy and Municipalities in Luxembourg.

MONARC's purpose is to facilitate risk assessments for both small and large organizations. MONARC employs risk analysis techniques that are commonly used in business contexts. As businesses face similar threats and vulnerabilities, MONARC enables risk management that is precise and repeatable. By generalizing risk scenarios for common assets such as servers, printers, smartphones, and Wi-Fi antennas, MONARC allows risk management to be applied by context and business.

MONARC provides a straightforward solution for risk management and information security governance, following established industry standards. It offers pre-built and customizable risk analysis models that adhere to the ISO/IEC 27005:2011 international standard (CASES, 2013). It also includes risk models that comply with various standards and laws, such as the GDPR for personal data protection, ISO/IEC 27001 certification, and the PCI-DSS standard.

The MONARC method consists of four phases, namely Context Establishment, Risk Modelling, Risk Assessment and Treatment, and Implementation and Monitoring. These phases follow the ISO/IEC 27005:2011 international standard guidelines for information security risk management. At the end of each phase, a report is generated detailing the decisions made and the results obtained. This approach simplifies risk

management by offering a risk management solution compliant with industry standards, including ISO/IEC 27001 certification, PCI-DSS standard, and European regulations for the protection of personal data (GDPR). MONARC allows for analysis from existing and customizable models to be made, facilitating precise and repeatable risk management.

- During the **Context Establishment** phase of MONARC, the information related to the organization is collected to define the scope and limitations of the risk analysis. This phase also involves defining the criteria for evaluation, acceptance, and impact. MONARC utilizes a qualitative evaluation method while for vulnerabilities, threats, and impacts, it uses quantitative criteria.
- In the **Risk Modelling** phase, the risk manager identifies potential threats and vulnerabilities and defines their potential impacts. The MONARC tool uses a pre-determined set of objects and associated risk scenarios that are linked to primary assets to build the risk tree. The selection of assets and scenarios is determined by external experts based on the maturity level of the entity undergoing the risk analysis. By using pre-determined objects and scenarios, MONARC simplifies the risk modelling process and ensures consistency across different risk analyses.
- In the **Risk Assessment** and **Treatment** phase, the level of risk is evaluated, and a plan is developed to reduce the risk to an acceptable level. The assessment involves quantifying the threats, vulnerabilities, and impacts to calculate the level of risk. The risk treatment plan is based on the four types of treatments provided in the ISO/IEC 27005:2011 standard, which are modification, rejection, acceptance, and sharing.

MONARC is a constantly evolving tool that is regularly updated and improved to provide better risk management solutions. Therefore, the Implementation and Monitoring phase involves ongoing security monitoring and recurring control of security measures to improve security management in a sustainable manner.

EBIOS RISK MANAGER

The EBIOS method [10] was developed in 1995 to analyse, evaluate, and mitigate risks related to information systems. In 2018, a new version of the method called EBIOS Risk Manager was introduced, and it is currently maintained by the French National Cybersecurity Agency (ANSSI) with support from Club EBIOS.

EBIOS Risk Manager is a versatile risk management method that can be applied to organizations of all sizes, operating in any industry sector and at any stage of their information system's development. The method uses an iterative approach to risk management, starting with an assessment of the highest-level objectives of the object under study, and then gradually examining the relevant business and technical functions. The EBIOS Risk Manager methodology involves five workshops, where

possible risk scenarios are studied, and a synthesis is obtained between "conformity" and "scenarios" to maximize their added value.

EBIOS Risk Manager offers a versatile toolbox that can be customized to meet the specific needs of a project. The method is compatible with existing risk management standards, such as ISO 31000:2018, and cybersecurity standards in the ISO/IEC 27000 series, with ISO27005 being of particular relevance.

The EBIOS Risk Manager methodology connects decision-makers and operational teams by adopting a scenario-based approach, which includes business strategic scenarios and operational scenarios that involve stakeholders within the ecosystem such as clients, partners, providers, and supply chain. By leveraging this approach, the decision process at the highest level of the organization can be clarified and informed by the operational reality provided by the operational scenarios.

EBIOS Risk Manager benefits from a comprehensive ecosystem that supports its use. This ecosystem includes an active community of experts from both the public and private sectors, known as Club EBIOS. The method is also supported by a community of editors who develop tools that are compliant with EBIOS Risk Manager, some of which are available as freemium. Additionally, EBIOS Risk Manager has a large network of trainers and nine training organizations that support its implementation and use.

RISK MANAGEMENT TOOLS

For organizations seeking to manage potential risks and their negative impacts, risk management software offers numerous benefits. By using such software, your business can gain an accurate understanding of the risks it faces and make informed decisions about which controls to implement. Risk management software can also integrate corporate governance, risk management, and compliance processes to lower costs and maximize efficiency. Additionally, it can help to strengthen your operations and internal controls by providing knowledge of the risk landscape and current mitigation efforts. By demonstrating a sophisticated approach to IT governance, risk management software can help to earn customer trust, improve brand reputation, and increase shareholder value. Finally, it can also assist in driving compliance and avoiding violations, fines, litigation costs, and business disruptions.

Microsoft Security Assessment Tool 4.0

The Microsoft Security Assessment Tool 4.0 [11] is an updated version of its predecessors, the Microsoft Security Assessment Tool (MSAT) released in 2004 and the Microsoft Security Assessment Tool 2.0 released in 2006. Given the evolution of security issues since 2004, the MSAT 4.0 includes additional questions and answers to provide a comprehensive toolset that helps you stay informed about the changing security threat landscape that could affect your organization.

The tool assesses an organization's security posture by taking a holistic approach that covers people, process, and technology. It provides prescriptive guidance, recommended mitigation efforts, and links to further information for additional industry guidance, assisting organizations in staying aware of specific tools and methods to improve their IT environment's security posture.

There are two assessments that define the Microsoft Security Assessment Tool:

- **Business Risk Profile Assessment**
- **Defense in Depth Assessment**

The survey questions and corresponding answers in the Microsoft Security Assessment Tool are based on widely accepted best practices in security, covering both general and specific topics. These best practices are established by standards such as ISO 17799 and NIST-800.x, as well as recommendations and guidance from Microsoft's Trustworthy Computing Group and other trusted sources in the security industry.

The MSAT is tailored to suit mid-sized organizations that have between 50 to 500 computers. It presents a set of 172 questions, grouped into different categories, and after analysing your responses, it provides you with an evaluation of your situation and recommendations on how to improve it. The tool starts by asking you questions about your business model, which it uses to create a Business Risk Profile (BRP) that assesses your security risk in comparison to others within your industry. The questionnaire typically takes about two hours to complete, and you have the option to pause and resume it at any time. The categories and sample questions are as follows:

Basic Information: How many clients and servers are in your organization?

Infrastructure Security: Do your employees work remotely? Do external contractors access your network?

Applications Security: Does your company develop applications? Does it store sensitive data processed by your applications?

Operations Security: Does your corporate network connect to external networks? Does your organization receive data feeds from external parties?

People Security: Does your company outsource computer maintenance? Do you let employees download sensitive company data to their workstations?

Environment: How many employees are in your organization? Is there high turnover in your IT department?

Following the completion of the questionnaire, the MSAT produces an evaluation that measures the effectiveness of your security processes, called the Defense-in-Depth Index (DiDI). It evaluates the security measures you have implemented in each category, such as the use of firewalls at each location, the deployment of patches and updates to your PCs, and whether your users have administrative rights on their workstations. Depending on your responses, the MSAT generates three reports to provide you with prescriptive guidance on how to improve your security posture.

The MSAT offers three reports in response to your answers. The Summary Report presents a bar graph that depicts the results. The Business Risk Profile (BRP) score indicates higher risk with a high score, while a high Defense-in-Depth Index (DiDI) score represents greater security. However, the MSAT emphasizes that it's crucial to examine individual areas, even if a low BRP and high DiDI might seem preferable. For each area, the Complete Report informs you whether you meet best practices, require improvement, or are severely lacking. Additionally, you can anonymously upload your results to the secure MSAT Web server and compare your data with that of your peers by industry and company size. The application will retrieve the most recent data available simultaneously with your data upload.

SimpleRisk

SimpleRisk Core [12] is a software solution that encompasses fundamental Governance, Risk Management, and Compliance capabilities that organizations require to commence their program. Below is a compilation of some of the significant features that are integrated into SimpleRisk Core:

One of the main features included in SimpleRisk Core is the capability to create customized **frameworks and controls** that align with your organization's specific risk management needs. As your risk management program evolves, these frameworks and controls can be utilized to associate controls with risks during Risk Management or to

validate control effectiveness for Compliance purposes. Additionally, SimpleRisk Core offers the ability to upload documentation for all of your organization's policies, guidelines, standards, and procedures. Users can track exception approvals for policies and controls, link them to controls, and assign owners and approvers while also keeping track of review dates and status.

With SimpleRisk Core, you can define an unlimited number of **tests** across all of the frameworks and controls that you have set up in Governance. These tests can be used to initiate audits at the framework, control, or test level. You can filter and track active audits, along with all associated documentation and evidence. Additionally, you can view past audits, and restrict access to testing progress and results to only those individuals who require it.

With SimpleRisk Core, you can take advantage of **pre-configured risk assessments** for various frameworks, such as CIS Critical Security Controls, HIPAA, NIST 800-171, or PCI DSS 3.2. These assessments consist of a series of Yes/No questions, and your answers are used to generate pending risks. You can easily add these risks to your risk registry by clicking a button, allowing you to quickly identify potential threats to your organization's security.

You can submit new **risks** and keep a registry to monitor all risks associated with your organization. The software enables you to **plan risk mitigations** by setting mitigation dates, defining the level of effort, assigning ownership, associating with the controls defined in Governance, and tracking changes in residual risk through the mitigation percentage. To involve management in the risk management process, the software outlines next steps for your risks in the review process. You can group risks together into higher-level projects for batch management and reporting purposes. SimpleRisk also assists you in tracking review dates and status for your risks, ensuring regular reviews are taking place.

SimpleRisk Core offers a basic automated discovery feature for identifying **assets** within your organization, and you also have the option to manually add assets with the ability to assign a value and link them to teams and locations. Additionally, assets can be grouped logically and linked to associated risks.

SimpleRisk offers an extensive range of **reports** that can aid you in maximizing the benefits of your risk management program. These reports comprise of graphical dashboards, reports for recognizing risks that exceed your risk tolerance level, reports that provide recommendations on how to prioritize remediation efforts to attain

maximum return on investment, reports that showcase the linkages between your risks, controls or assets, and a highly adaptable report that enables you to create customized reports based on the fields managed by SimpleRisk.

The SimpleRisk Core is a flexible platform that can be **customized** to fit the unique risk management needs of your organization. You have the ability to modify dropdown options, edit risk formulas, and manage the risk catalog to ensure it aligns with your specific requirements. You can also create and manage user accounts, assign them to roles, and configure permissions with granularity. Every change made within the system is tracked and recorded in an audit trail that can be reviewed by your system administrators.

Modulo Risk Manager

Modulo Risk Manager [13] is a single, fully integrated platform for organizations to automate and unify their IT governance, risk and compliance (GRC) processes. It automates the process of identifying, analysing, evaluating and treating risks across the enterprise - reducing complexity and costs and offering visibility into the risk management process by identifying risk, measuring the impact to the business and tracking what the organization is doing about it.

The product is a set of modules that includes risk management; compliance management; policy management; continuous monitoring supporting ongoing monitoring of risks and controls across the portfolio of client products, including vulnerability assessment, security information and event management, intrusion detection system and intrusion prevention systems products; vendor risk management; audit management; incident management; asset management and knowledge management. IT risk and vulnerability management integration is included and supports integration with popular vulnerability scanners.

Based on the ISO 31000 standard, the Risk Manager Module provides tools to inventory, analyse, evaluate and manage/mitigate risks. It delivers quantitative and qualitative information on identified risks and helps to prioritize actions. Risk is calculated using three dimensions: probability, relevance and severity. There is a complete incident management tool for addressing risks and non-compliant assets, allowing one to monitor progress through a comprehensive incident and workflow-management system. This function has been updated in this revision and provides better

automated remediation options. One can easily automate the asset management process by providing asset inventory (both technology and non-technology-oriented assets, such as people, processes and facilities) that are imported from a number of third-party sources. The audit function is easy to use and, as mentioned above, has a ton of prepopulated content. The assessment process is done via email, but there is also a mobile application that allows users to not only answer questions but also upload evidence from a mobile device. The output of these modules provides a clear, comprehensive and prioritized view of risks and vulnerabilities, while integrating IT assets, resources, environment and processes into a single platform.

The reporting and visual dashboarding capabilities are very strong. It has role-based dashboarding, easy-to-use report editors and, most importantly, a correlated view of all risk aspects in the enterprise.

Risk Management Studio

RM Studio [14] is a comprehensive risk management software that streamlines the risk assessment process. It is customizable and dynamic, designed by ISMS professionals to simplify risk management. With its modular structure, RM Studio enables users to incorporate global standards and deploy various risk management modules, such as the risk assessment and business continuity modules. The software guides users through the intricate risk assessment, risk treatment, and risk management process, providing increased efficiency.

RM Studio offers an all-in-one solution that assists in managing and addressing risk, controls, and risk treatment objectives in an intuitive, simple, and easily managed way. The software provides a complete view of the risk assessment process, enabling users to promptly access the underlying, existing, and future security risk status. The primary advantages of utilizing RM Studio for risk assessments include:

Integrated asset categories and threat library: RM Studio simplifies the risk assessment process by providing a comprehensive asset category library and an embedded threat library. Users can easily categorize assets and connect them with relevant threats, removing the need for guesswork. The threat library is connected to the asset categories, automatically associating the appropriate threats. Users can also create custom asset categories to fit their organizational needs and add or remove threats as necessary. RM Studio allows for a quick and easy view of the relationship between

assets and threats, enabling users to identify the associated threats with a single asset or vice versa with a single click.

Embedded standards option: RM Studio offers the ability to embed and deploy various international accredited standards such as ISO standards, Payment Card Industry Data Security Standards, and the World Lottery Association Security Control Standard. These standards can be easily accessed and utilized within the software. Additionally, users can input their own specific standards or requirements, allowing for a customizable approach to meet the unique needs of each organization. This feature ensures that RM Studio can adapt and remain relevant in an ever-changing market.

Easily repeatable processes and embedded evaluation templates: RM Studio's assessment templates are pre-configured according to industry best practices and can be easily deployed with a single click, streamlining the risk assessment process. Users also have the flexibility to customize evaluation criteria based on their specific requirements, enabling them to respond dynamically to changing needs.

Benchmark risk calculations: RM Studio uses risk calculations developed by ISMS experts, which are scalable and easily customizable. The software simplifies the risk assessment process by utilizing built-in asset evaluation criteria and threat evaluation criteria to automatically calculate the risk value. Users can also implement their own evaluation criteria for assets and threats, which can be based on internal processes, international standards, or other organization-specific needs. This flexibility allows for a more comprehensive and tailored risk assessment process.

Integrated implementation guide: When RM Studio is integrated with international standards, it includes an implementation guide for the respective standards. Users can leverage this guide to help mitigate risks and establish controls, as well as create policies for their organization. Additionally, users have the option to create their own implementation guides for standards that are already in use or newly defined by the organization.

Linked gap analysis and risk treatment plan: RM Studio streamlines the risk assessment process by seamlessly integrating the subsequent steps of gap analysis and risk treatment planning. With the Gap Analysis feature, users can quickly and easily perform compliance checks, while being guided through the implementation of controls that align with their risk appetite. RM Studio simplifies the tracking of implemented controls and responsible parties, making it easy for users to ensure that all required actions have been carried out. When used in conjunction with embedded standards, the

Gap Analysis feature also provides an extensive implementation guide based on the specific standards.

In addition, RM Studio's Risk Treatment feature further simplifies the overall risk assessment process by automatically consolidating the risk assessment and gap analysis into a centralized repository, where current and future security risks are calculated and compared to the base security risk calculated during the risk assessment. Users are then led through the process of determining the appropriate risk treatment decision, which can involve avoiding, reducing, accepting, or transferring risk.

Integrated reporting and exporting options: RM Studio offers 11 preformatted reports that are readily available for users to generate with a simple click of a button. These reports include a detailed Risk Assessment Report, Statement of Applicability, Gap Analysis Results, and an Executive Summary, among others. In addition to the preformatted reports, RM Studio also allows users to export all data to Excel or PDF with a click of a button for easy sharing and integration into other organizational documents.

Practical Threat Analysis (PTA)

The Practical Threat Analysis (PTA) [15] tool is based on the PTA calculative threat analysis and threat modelling methodology and enables effective management of operational and security risks in complex systems. The tool utilizes a dynamic threat model that can adapt to changes in the system's assets and vulnerabilities. Using PTA, analysts can maintain a growing database of threats, create documentation for security reviews, and generate reports that prioritize the importance of various threats and corresponding countermeasures. PTA calculates the priorities of threats and countermeasures based on the system's asset values, potential damage levels, and the probability of threats. It also considers the degree of mitigation provided by countermeasures. The tool generates an updated risk mitigation plan that reflects changes in threat realities and identifies the most cost-effective countermeasures against the identified threats.

PTA threat modelling steps are presented below:

Identifying Assets: The financial values of system assets and the potential losses resulting from damages can be mapped in order to calculate the priorities for threats, risks, and countermeasures. These asset values serve as the foundation for determining

the importance of different threats and the corresponding priorities for countermeasures.

Identifying Vulnerabilities: To identify potential vulnerabilities in a system, it is necessary to have a good understanding of its functionality, architecture, business and operational procedures, and the types of users who interact with it. This task requires continuous iteration and is closely tied to the step of identifying threats.

Defining Countermeasures: Defining the countermeasures relevant to system vulnerabilities. The effectiveness of countermeasures to address system vulnerabilities is defined, taking into consideration the estimated cost of implementation.

Building Threat Scenarios and Mitigation Plans: The process of composing potential threat scenarios involves several steps, including entering a brief description of the scenario and identifying the assets that may be threatened, along with the level of damage that may result. System vulnerabilities that could be exploited by the threat are identified, which automatically generates a list of recommended countermeasures. The probability of the threat occurring is then established, and the overall risk level is calculated based on the potential damage and likelihood of the threat. Finally, a mitigation plan is determined by selecting the most effective combination of countermeasures. Starting the threat analysis process with predefined entities of assets, vulnerabilities, and countermeasures typical to the system being analysed can be an effective way to jumpstart the process.

Reviewing the threat analysis results can help improve the threat model and refine the model entities parameters. The basic analysis outcomes are described below:

- List of threats, their risk and potential damage to assets when threats materialize.
- List of assets and the financial risk that threatens them.
- List of countermeasures, their overall mitigation effect and cost-effectiveness relative to their contribution to system risk reduction.

The maximal financial risk to the system, the final risk to the system (after all mitigation plans were implemented) and the current level of system risk according to the status of countermeasure’s implementation.

MONARC

MONARC [9] is a risk assessment tool and method that helps organizations perform optimized, precise, and repeatable risk assessments. Depending on their size and security needs, organizations must respond in the most appropriate way, adopting good practices, taking necessary measures, and adjusting them proportionally. MONARC enables precise and repeatable risk management by capitalizing on risk analyses already performed in similar business contexts. Similar vulnerabilities often appear in many businesses as they face the same threats and generate similar risks. Since most companies have servers, printers, smartphones Therefore, it is possible to generalize risk scenarios for these assets based on the organization's context and business. The phases of MONARC are described below:

Context Establishment: The initial stage of risk analysis involves assessing the company or organization's context, challenges, and priorities. This helps identify the key activities and critical processes that require the most attention during the risk analysis. A kickoff meeting is typically held with management and key individuals to gain insight into the organization's operations and identify potential threats and vulnerabilities that could impact the business. The objective is to determine what sustains the company's operations and what could potentially threaten it, while also identifying any internal or external threats as well as any organizational, technical, or human vulnerabilities that need to be addressed.

Context Modelling: In this phase, the focus is on modelling objects and trees which involves formalizing and detailing the assets that were previously identified in the context establishment phase. A diagram is created to display the interdependencies of these assets, and the impacts are defined at the primary asset level (such as processes or information), based on the information gathered in the previous phase. The impact of the primary asset is then inherited by the secondary assets that are attached to it (in an object tree). The impact level of the secondary assets can be manually modified as needed.

Evaluation and treatment of risks: In the assessment phase, the objective is to quantify the threats, vulnerabilities and impacts to determine the level of risk. This requires accurate information regarding the likelihood of the threats, the extent to which vulnerabilities can be exploited and the potential impact. Validated metrics by experts are essential to ensure the quality of the assessment. If the assessment reveals a risk

level that exceeds the acceptable threshold defined in the risk acceptance grid, risk treatment measures should be implemented to mitigate the risk and bring it down to an acceptable level.

Implementation and monitoring: After the initial risk treatment measures have been implemented, it is crucial to enter the ongoing management phase. This phase involves continuous security monitoring and regular assessments of the effectiveness of the security measures in place, with the goal of achieving sustainable improvement. By continuously improving the level of detail of objects used and expanding the scope of the risk analysis, security can be optimized over time.

VERINICE ISMS

Verinice [16] is an open-source tool that helps with managing information security. The tool can be used for a variety of purposes such as establishing, maintaining, and improving an Information Security Management System (ISMS) based on various standards like ISO 27001, BSI IT Baseline Protection, IDW PS 330, and others. It can also help with compliance with standards, risk analysis based on ISO 27005, auditing, document management, report generation, and more. Additionally, Verinice supports a wide range of standards including ISO 27001, ISO 27002, ISO 27005, ISO 27018, ISO 27019, ISO 27004, BSI 100-1 bis -4, PCI DSS, COBIT, BDSG, EU DSGVO, SSAE 16, BCBS 239, ISAE 3402, MaRisk-E, SREP, VDA ISA, IDW PS 330, and IDW PH 9.330.1. The tool can be run on Windows, Linux, and macOS, and all relevant standards are either integrated into the tool or can be easily imported.

Verinice provides a comprehensive risk analysis solution for information assets by allowing users to add threats and vulnerabilities from different sources such as vulnerability scanners or penetration tests. The tool supports the identification of risks according to different processes, including ISO 27005, BSI Standard 100-3/200-3, and others. Users can also build their own risk scenarios as part of risk assessment workshops or use the pre-existing **risks** listed in the BSI IT Baseline Protection catalogue. Verinice.PRO includes a generic risk scenario catalogue that is categorized into **threats** and **vulnerabilities** to enable a simple and realistic risk assessment. With drag-and-drop functionality, Verinice maintains risk assessments effectively.

Verinice allows you to maintain your information assets and processes, and it offers an **asset register** that can be exported with just one click. You can link your assets with

processes, process owners, and other assets, and Verinice can automatically inherit business impact values in the asset tree. Additionally, Verinice offers filtering and processing functions like the mass editor, which can simplify your work. Furthermore, Verinice supports various import and export formats such as CSV, XML, and XLS, making it easier to transfer data from existing sources and enabling further processing with other tools.

Questionnaires such as the Information Security Assessment (ISA) of the German Association of the Automotive Industry (VDA) offer a guided self assessment based on the ISO 27002. The ISA gives organizations across all industries the opportunity to assess their own state of information security or to learn about those of their contractors.

Verinice provides powerful **reporting** capabilities, allowing users to generate reports for auditors, management, process owners, and for reference documents during the certification process. Reports can be used to document the state of information security within an organization and support decision-making and planning with tables and charts. Verinice allows reports to be generated in various formats, including PDF, HTML, DOC, XLS, ODT, and ODS. Users of verinice.PRO also have access to the vDesigner report designer, which enables the customization of report templates, including the ability to incorporate branding and corporate design. Additionally, users can create completely customized reports.

vsRisk

vsRisk is an information security risk assessment tool developed by Vigilant Software. vsRisk is designed to simplify the risk assessment process for organizations of all sizes, and it has a number of features that make it an effective tool for managing information security risks.

One of the key benefits of vsRisk is that it is designed to be easy to use. The software comes with a **pre-built** risk assessment template based on ISO 27001, which is one of the most widely recognized international standards for information security. This means that users don't need to be experts in risk assessment or ISO 27001 to get started with the tool. The software guides users through the risk assessment process step-by-step, using simple language and clear instructions.

vsRisk also includes a risk assessment **wizard** that helps users identify potential **threats** and **vulnerabilities** to their information **assets**. The wizard prompts users to answer a series of **questions** about their organization and its information assets, such as data storage locations, hardware, software, and network infrastructure. Based on the user's answers, vsRisk automatically generates a risk assessment report that highlights potential risks and identifies areas where additional security measures may be needed.

Another benefit of vsRisk is that it is fully customizable. Users can modify the pre-built risk assessment template to suit their organization's specific needs and requirements. They can also add their own information assets, risks, and controls to the tool, or import data from other sources such as vulnerability scanners or penetration testing tools. This makes vsRisk a flexible tool that can adapt to the unique security challenges faced by different organizations.

In addition to its risk assessment capabilities, vsRisk also includes several other features that make it a comprehensive tool for managing information security risks. These include:

- **Compliance tracking**: vsRisk tracks compliance with relevant regulations and standards, such as ISO 27001, GDPR, and HIPAA.
- **Action tracking**: vsRisk allows users to assign actions to team members and track progress towards completion.
- **Reporting**: vsRisk generates detailed risk assessment reports that can be customized to include specific data and metrics. The reports can be exported in a variety of formats, including PDF, Excel, and Word.
- **Collaboration**: vsRisk allows multiple users to work on a risk assessment project simultaneously, making it a useful tool for teams and departments.

vsRisk is a cloud-based tool, which means that it is accessible from anywhere with an internet connection. This makes it ideal for organizations with multiple locations or remote workers. Additionally, the tool is updated regularly to ensure that it remains current with the latest threats and vulnerabilities.

COMPARISON EVALUATION FRAMEWORK

A Comparison Evaluation Framework (CEF) is a set of guidelines and procedures that are used to evaluate and compare the performance, quality, and effectiveness of different entities. The framework provides a structured approach to the comparison process, ensuring that all relevant factors are taken into account and that the evaluation is conducted objectively and consistently.

A CEF typically involves the following steps:

- **Identify the entities to be compared**: The first step is to identify the entities that will be evaluated and compared. This may include products, services, processes, or organizations.
- **Determine the criteria for comparison**: The next step is to determine the criteria that will be used to evaluate and compare the entities. These criteria should be relevant to the goals of the evaluation and should be measurable and objective.
- **Collect data**: Data is collected on each entity based on the criteria established in step two. This may involve surveys, interviews, observations, or other methods of data collection.
- **Analyse the data**: The data collected is analyzed using statistical methods and other techniques to identify differences and similarities between the entities being compared.
- **Generate a final rating**: Based on the analysis, a final rating is generated for each entity being compared. This rating is typically presented in a report or other format that is easily understood by stakeholders.
- **Support decision-making**: The final rating generated by the CEF is used to support decision-making processes of stakeholders, such as selecting a product, service, or vendor.

In our case, we have created the following CEF for risk management frameworks and methodologies:

1. **Scope and Objectives**: This category evaluates the scope and objectives of the risk management methodology. It includes criteria such as the methodology's applicability to different industries, the specific risks it addresses, and the overall effectiveness of the methodology in achieving its objectives.
2. **Risk Assessment Process**: This category assesses the methodology's risk assessment process. It includes criteria such as the identification and categorization of risks, the assessment of risk likelihood and impact, and the development of risk treatment plans.
3. **Risk Treatment Process**: This category evaluates the methodology's risk treatment process. It includes criteria such as the selection and implementation of risk treatment options, the monitoring of risk treatment effectiveness, and the evaluation of residual risk.
4. **Integration with Business Processes**: This category evaluates the methodology's integration with business processes. It includes criteria such as the methodology's alignment with organizational goals and objectives, its integration with existing business processes, and its impact on business operations.

5. **Governance and Compliance**: This category assesses the methodology's governance and compliance aspects. It includes criteria such as the methodology's compliance with relevant laws and regulations, its adherence to industry standards, and its overall governance structure and processes.
6. **Reporting and Communication**: This category evaluates the methodology's reporting and communication capabilities. It includes criteria such as the methodology's ability to generate meaningful reports, its communication channels with stakeholders, and its ability to facilitate decision-making.
7. **Scalability and Flexibility**: This category assesses the methodology's scalability and flexibility. It includes criteria such as the methodology's ability to adapt to changing business needs and risks, its ability to scale for larger or more complex organizations, and its overall flexibility in implementation.
8. **Tools and Technology**: This category evaluates the methodology's tools and technology capabilities. It includes criteria such as the availability of software and tools to support the methodology, the ease of use of those tools, and the level of automation provided.
9. **Training and Education**: This category assesses the methodology's training and education capabilities. It includes criteria such as the availability of training materials and resources, the level of expertise required to implement the methodology, and the overall accessibility of the methodology for different stakeholders.

We are going to evaluate each of the risk assessment framework and methodologies that we have already analysed and the rate every category for each one of them from a scale from 1 to 5 (1 being the lowest rating and 5 being the best rating).

EVALUATIONS

ISO 27005:2018

You may find the Evaluation of the ISO 27005:2018 below:

Scope and Objectives: ISO 27005:2018 is applicable to all types of organizations, regardless of their size, nature, and complexity. Its scope is to provide guidelines for risk management in information security and to support the overall management system of the organization. The objectives of the methodology are to establish a systematic approach to risk management, to enable the identification of risks and their potential impact on the organization, and to ensure that appropriate measures are implemented to manage those risks.

Risk Assessment Process: ISO 27005:2018 provides a structured risk assessment process that includes the identification of assets and their values, the identification of threats and vulnerabilities, the analysis of the likelihood and impact of risks, and the

evaluation of risk levels. The methodology also includes guidelines for selecting risk assessment methods and tools.

Risk Treatment Process: ISO 27005:2018 provides a framework for selecting and implementing risk treatment options, which includes risk avoidance, risk reduction, risk sharing, and risk acceptance. The methodology emphasizes the importance of monitoring the effectiveness of risk treatment and the evaluation of residual risks.

Integration with Business Processes: ISO 27005:2018 is designed to be integrated with the overall management system of the organization, including business processes, policies, and procedures. The methodology emphasizes the need for risk management to be aligned with organizational goals and objectives.

Governance and Compliance: ISO 27005:2018 provides guidance on the governance and compliance aspects of risk management. It emphasizes the need for risk management to be aligned with legal and regulatory requirements, industry standards, and best practices. The methodology also includes guidelines for the establishment of risk management policies and procedures.

Reporting and Communication: ISO 27005:2018 emphasizes the importance of reporting and communication in risk management. The methodology includes guidelines for the preparation of risk management reports, as well as the communication of risk management activities and outcomes to relevant stakeholders.

Scalability and Flexibility: ISO 27005:2018 is designed to be scalable and flexible, to accommodate organizations of different sizes and complexity levels. The methodology includes guidelines for adapting risk management to changing business needs and risks, as well as the implementation of risk management in different contexts.

Tools and Technology: ISO 27005:2018 provides guidance on the use of tools and technology in risk management, including the selection of appropriate software and tools to support the risk assessment and treatment processes.

Training and Education: ISO 27005:2018 emphasizes the importance of training and education in risk management, including the provision of training materials and resources, the level of expertise required to implement the methodology, and the accessibility of the methodology for different stakeholders.

NIST SP 800 Series

You may find the Evaluation of the NIST SP 800 Series below:

Scope and Objectives: NIST SP 800 series has a broad scope and is applicable to a wide range of industries. It addresses various risks related to information security and aims to provide guidance for managing those risks effectively.

Risk Assessment Process: NIST SP 800 series provides a structured approach to risk assessment that includes the identification, categorization, assessment, and prioritization of risks. It also provides guidance on risk mitigation and the development of risk treatment plans.

Risk Treatment Process: The methodology provides guidance on the selection and implementation of risk treatment options, as well as the monitoring and evaluation of risk treatment effectiveness. It also addresses residual risks and provides guidance on their management.

Integration with Business Processes: NIST SP 800 series is designed to align with organizational goals and objectives and can be integrated with existing business processes. It provides guidance on the integration of risk management with other management processes and the overall impact of risk management on business operations.

Governance and Compliance: NIST SP 800 series is compliant with relevant laws and regulations, adheres to industry standards, and has a well-defined governance structure and processes. It provides guidance on the establishment of risk management roles and responsibilities and the development of risk management policies and procedures.

Reporting and Communication: The methodology provides guidance on generating meaningful reports and communicating risk information to stakeholders. It also addresses the importance of effective communication channels and stakeholder involvement in the risk management process.

Scalability and Flexibility: NIST SP 800 series is designed to be scalable and flexible, enabling it to adapt to changing business needs and risks. It provides guidance on the application of risk management to larger or more complex organizations and the customization of the methodology to suit specific organizational requirements.

Tools and Technology: The methodology provides guidance on the use of various tools and technologies to support the risk management process. It also addresses the importance of the ease of use of those tools and the level of automation provided.

Training and Education: NIST SP 800 series provides guidance on the level of expertise required to implement the methodology and the availability of training materials and resources. It also emphasizes the importance of educating stakeholders on risk management concepts and practices.

OCTAVE Methodology

You may find the Evaluation of the Octave Methodology below:

Scope and Objectives: OCTAVE is designed to be applicable to various industries, with a focus on assessing risks to critical assets and information systems. The methodology aims to identify potential threats and vulnerabilities and to develop risk mitigation strategies.

Risk Assessment Process: OCTAVE's risk assessment process involves identifying and categorizing risks, analyzing their likelihood and impact, and identifying vulnerabilities and threats. The methodology uses a variety of techniques, such as workshops and surveys, to gather information about the organization's assets and potential risks.

Risk Treatment Process: OCTAVE's risk treatment process involves selecting and implementing appropriate risk mitigation strategies based on the risk assessment. The methodology emphasizes the need for ongoing monitoring and evaluation to ensure the effectiveness of the selected risk treatment options.

Integration with Business Processes: OCTAVE is designed to be integrated with an organization's existing business processes, with a focus on aligning risk management activities with the organization's objectives and goals.

Governance and Compliance: OCTAVE emphasizes the importance of compliance with relevant laws and regulations and adherence to industry standards. The methodology includes guidance on governance structure and processes to ensure effective risk management practices.

Reporting and Communication: OCTAVE provides guidance on reporting and communication practices, including the use of risk profiles and other reporting tools to communicate risk information to stakeholders.

Scalability and Flexibility: OCTAVE is designed to be scalable for larger or more complex organizations, with the flexibility to adapt to changing business needs and

risks. The methodology emphasizes the need for ongoing evaluation and adjustment to ensure its continued effectiveness.

Tools and Technology: OCTAVE does not rely on specific software or tools, but it provides guidance on the use of various techniques and methods to support the risk management process.

Training and Education: OCTAVE provides guidance on training and education for stakeholders involved in the risk management process, including the level of expertise required to implement the methodology effectively. The methodology emphasizes the need for ongoing training and education to support effective risk management practices.

ISACA RISK IT FRAMEWORK

You may find the Evaluation of the ISACA risk IT framework below:

Scope and Objectives: The ISACA Risk IT Framework aims to provide guidance on managing IT risk to organizations of all sizes and in various industries. Its objectives include enhancing the organization's understanding of IT risk, improving decision-making related to IT risk, and increasing the effectiveness of IT risk management.

Risk Assessment Process: The ISACA Risk IT Framework includes a risk assessment process that involves identifying and categorizing IT risks, assessing the likelihood and impact of those risks, and determining the organization's risk appetite. It also includes guidance on developing risk treatment plans based on the identified risks.

Risk Treatment Process: The framework provides guidance on selecting and implementing risk treatment options, monitoring the effectiveness of those treatments, and evaluating the residual risk. It emphasizes the importance of continuous monitoring and improvement of the risk management process.

Integration with Business Processes: The ISACA Risk IT Framework is designed to align with organizational goals and objectives and integrate with existing business processes. It emphasizes the need for IT risk management to be integrated with the overall organizational risk management process.

Governance and Compliance: The framework includes guidance on governance and compliance aspects of IT risk management. It highlights the importance of complying with relevant laws and regulations and adhering to industry standards. It also provides guidance on establishing an IT risk governance structure and processes.

Reporting and Communication: The framework provides guidance on generating meaningful reports and communicating with stakeholders. It emphasizes the importance of effective communication in facilitating decision-making related to IT risk management.

Scalability and Flexibility: The ISACA Risk IT Framework is designed to be scalable and flexible to adapt to changing business needs and risks. It provides guidance on how to customize the risk management process based on the organization's size, complexity, and risk profile.

Tools and Technology: The framework does not provide specific software or tools, but it provides guidance on selecting and implementing tools to support the risk management process. It emphasizes the need for tools that are easy to use and provide automation where possible.

Training and Education: The ISACA Risk IT Framework provides guidance on the level of expertise required to implement the methodology and the availability of training materials and resources. It emphasizes the need for continuous training and education to keep up with changing IT risk management practices.

INFORMATION RISK ASSESSMENT METHODOLOGY 2 (IRAM2)

You may find the Evaluation of IRAM2 below:

Scope and Objectives: IRAM2 is designed to provide a comprehensive framework for risk management in IT environments. It is applicable to various industries and can address specific risks such as cyber threats, IT failures, and data breaches. The objective of IRAM2 is to help organizations identify and assess IT-related risks, develop effective risk treatment plans, and monitor and report on risk management activities.

Risk Assessment Process: IRAM2's risk assessment process includes the identification and categorization of IT-related risks, the assessment of risk likelihood and impact, and the prioritization of risks based on their potential impact on the organization. IRAM2 also provides guidance on how to identify and evaluate risk sources and how to document the risk assessment process.

Risk Treatment Process: The risk treatment process in IRAM2 includes the selection and implementation of risk treatment options, the monitoring of risk treatment effectiveness, and the evaluation of residual risk. IRAM2 also provides guidance on how to develop a risk treatment plan and how to document risk treatment activities.

Integration with Business Processes: IRAM2 emphasizes the importance of integrating risk management with the organization's business processes. It provides guidance on how to align risk management with organizational goals and objectives, how to integrate risk management with existing business processes, and how to ensure that risk management activities do not disrupt business operations.

Governance and Compliance: IRAM2 has a strong focus on governance and compliance. It provides guidance on how to comply with relevant laws and regulations, how to adhere to industry standards, and how to establish an effective governance structure for risk management activities. IRAM2 also emphasizes the importance of senior management involvement in risk management.

Reporting and Communication: IRAM2 provides guidance on how to generate meaningful reports, how to communicate risk management activities to stakeholders, and how to facilitate decision-making. It emphasizes the importance of clear and concise communication to ensure that stakeholders understand the organization's risk management activities and their impact on the business.

Scalability and Flexibility: IRAM2 is designed to be scalable and flexible, allowing it to adapt to changing business needs and risks. It provides guidance on how to scale risk management activities for larger or more complex organizations and how to ensure that risk management activities are flexible enough to accommodate changes in the organization's IT environment.

Tools and Technology: IRAM2 does not provide specific tools or technology for risk management, but it does provide guidance on how to select and use tools and technology to support risk management activities. It emphasizes the importance of using technology to automate risk management tasks and to improve the efficiency and effectiveness of risk management activities.

Training and Education: IRAM2 provides guidance on how to develop training materials and resources for risk management, how to ensure that stakeholders have the expertise required to implement the methodology, and how to ensure that the methodology is accessible to all stakeholders. It emphasizes the importance of continuous education and training to ensure that stakeholders are up-to-date on the latest risk management practices and techniques.

ETSI TS 102 165-1, THREAT VULNERABILITY AND RISK ANALYSIS (TVRA)

You may find the Evaluation of TVRA below:

Scope and Objectives: TVRA focuses on evaluating the security of specific technology solutions, so its scope and objectives are more limited than those of the CEF. However, the TVRA framework is applicable to a wide range of industries and technologies, so it can be customized to address different risks.

Risk Assessment Process: TVRA's risk assessment process involves identifying potential threats and vulnerabilities associated with a technology solution, assessing their likelihood and impact, and prioritizing them for treatment. The framework provides guidance on how to conduct these assessments in a structured and repeatable manner.

Risk Treatment Process: TVRA's risk treatment process involves selecting and implementing appropriate controls to mitigate identified risks and verifying their effectiveness. The framework provides guidance on how to evaluate different treatment options and implement them in a cost-effective manner.

Integration with Business Processes: TVRA's integration with business processes is limited, as it primarily focuses on evaluating the security of technology solutions in isolation. However, the framework can be integrated with broader risk management processes to ensure that security risks are properly considered in the context of the organization's overall risk profile.

Governance and Compliance: TVRA provides guidance on how to ensure that technology solutions are compliant with relevant laws, regulations, and industry standards. However, the framework does not provide guidance on broader governance issues, such as how to establish an effective governance structure for risk management.

Reporting and Communication: TVRA provides guidance on how to communicate the results of security assessments to stakeholders in a clear and concise manner. However, the framework does not provide guidance on how to facilitate decision-making based on these results.

Scalability and Flexibility: TVRA is designed to be scalable and flexible, so it can be adapted to the needs of different organizations and technologies. The framework can be used to evaluate the security of both simple and complex technology solutions.

Tools and Technology: TVRA does not provide specific tools or technologies for conducting security assessments, but it does provide guidance on how to select and use appropriate tools and technologies.

Training and Education: TVRA provides guidance on the level of expertise required to conduct security assessments using the framework, and it includes recommendations for training and education to develop this expertise. However, the framework does not provide specific training materials or resources.

MONARC

You may find the Evaluation of MONARC method below:

Scope and Objectives: The MONARC methodology aims to provide a comprehensive risk assessment framework for information security management. It is applicable to a wide range of industries and focuses on identifying, evaluating, and managing information security risks.

Risk Assessment Process: MONARC provides a structured approach to risk assessment that includes the identification of assets, threats, vulnerabilities, and impacts. The methodology includes a risk matrix to evaluate the likelihood and impact of identified risks.

Risk Treatment Process: The MONARC methodology provides guidance on selecting and implementing risk treatment options, as well as monitoring and reviewing the effectiveness of the chosen controls. It also includes guidance on the residual risk evaluation process.

Integration with Business Processes: MONARC aligns with organizational goals and objectives and integrates with existing business processes. The methodology emphasizes the importance of involving stakeholders and communicating risk management activities throughout the organization.

Governance and Compliance: MONARC is designed to comply with relevant laws and regulations and adhere to industry standards. The methodology includes a governance structure and process, which outlines roles and responsibilities for risk management activities.

Reporting and Communication: The MONARC methodology includes a reporting and communication process, which includes generating reports on risk management activities and communicating risk management results to stakeholders. The methodology emphasizes the importance of effective communication in facilitating decision-making.

Scalability and Flexibility: MONARC is scalable and flexible, allowing it to adapt to changing business needs and risks. The methodology can be customized to fit the specific requirements of different organizations.

Tools and Technology: MONARC provides a range of tools and templates to support the risk assessment process, including a risk assessment spreadsheet, threat analysis template, and vulnerability assessment template. The methodology also includes guidance on the use of risk management software.

Training and Education: MONARC provides training materials and resources to support the implementation of the methodology, including training courses, workshops, and e-learning modules. The methodology is accessible to stakeholders with varying levels of expertise in risk management.

EBIOS RISK MANAGER

You may find the Evaluation of EBIOS risk manager framework below:

Scope and Objectives: EBIOS Risk Manager is designed to provide a comprehensive and standardized approach to risk management in information systems. The framework's scope and objectives include identifying and assessing risks to information systems and developing risk treatment plans to mitigate those risks.

Risk Assessment Process: EBIOS Risk Manager includes a well-defined risk assessment process that involves identifying assets, threats, vulnerabilities, and impacts, and assessing the likelihood and consequences of potential risk events. The framework also provides guidance on the selection of risk treatment options.

Risk Treatment Process: EBIOS Risk Manager includes a structured risk treatment process that involves selecting and implementing risk treatment options based on the results of the risk assessment process. The framework also includes guidance on monitoring and evaluating the effectiveness of risk treatments.

Integration with Business Processes: EBIOS Risk Manager is designed to be integrated with an organization's existing business processes. The framework includes guidance on aligning risk management objectives with organizational goals and objectives, and on integrating risk management activities with other business processes.

Governance and Compliance: EBIOS Risk Manager includes governance and compliance aspects, such as compliance with relevant laws and regulations, adherence

to industry standards, and the establishment of risk management policies and procedures.

Reporting and Communication: EBIOS Risk Manager includes capabilities for generating meaningful reports, communicating with stakeholders, and facilitating decision-making. The framework provides guidance on communicating risks to relevant stakeholders and on reporting risk management activities to management and other interested parties.

Scalability and Flexibility: EBIOS Risk Manager is designed to be scalable and flexible, with guidance on adapting the framework to different business needs and risks. The framework can be used by organizations of various sizes and complexity and can be applied to a wide range of information systems.

Tools and Technology: EBIOS Risk Manager provides guidance on the use of tools and technology to support the risk management process. The framework includes a software tool to support risk assessments and risk treatment plans.

Training and Education: EBIOS Risk Manager includes training and education capabilities, such as the availability of training materials and resources, and the level of expertise required to implement the methodology. The framework also includes guidance on the roles and responsibilities of different stakeholders in the risk management process.

Comparison

Comparing all the frameworks and methodologies together, we can see that each framework has its strengths and weaknesses in different categories. Here's a summary of the comparison:

Scope and Objectives: All frameworks have a clear scope and objectives, with ISO 27005, NIST, and OCTAVE having the most comprehensive scope, while TVRA and EBIOS have a more limited scope.

Risk Assessment Process: ISO 27005, NIST, and OCTAVE have a well-established and widely recognized risk assessment process, while ISACA, IRAM2, TVRA, and EBIOS have slightly different approaches to risk assessment. MONARC has a unique approach that includes modelling and simulation.

Risk Treatment Process: All frameworks have a clear and well-defined risk treatment process, with some frameworks such as ISO 27005, NIST, and OCTAVE having more detailed guidance on selecting and implementing risk treatment options.

Integration with Business Processes: All frameworks emphasize the importance of integrating risk management with business processes, with ISACA and NIST having the most comprehensive guidance on integration.

Governance and Compliance: All frameworks have strong governance and compliance aspects, with NIST and ISACA having the most comprehensive guidance on compliance.

Reporting and Communication: All frameworks have reporting and communication capabilities, with some frameworks such as NIST and ISACA having more comprehensive guidance on communicating risk to stakeholders.

Scalability and Flexibility: All frameworks have varying degrees of scalability and flexibility, with NIST and ISO 27005 being particularly adaptable to different organizations and contexts.

Tools and Technology: All frameworks have some level of support for tools and technology, with NIST having the most comprehensive guidance on selecting and using tools.

Training and Education: All frameworks have some level of training and education support, with ISACA having the most comprehensive guidance on training and certification programs.

Categories/Frameworks	ISO 27005	NIST	OCTAVE	ISACA	IRAM2	TVRA	MONARC	EBIOS
Scope and Objectives	5	5	5	4	4	3	4	2
Risk Assessment Process	5	5	5	4	4	3	5	3
Risk Treatment Process	5	5	5	4	4	4	5	3
Integration with Business Processes	4	5	4	5	4	4	4	3
Governance and Compliance	4	5	4	5	4	4	4	4
Reporting and Communication	4	5	4	5	4	4	4	4
Scalability and Flexibility	5	5	4	4	5	4	4	3
Tools and Technology	4	5	4	4	4	4	4	3
Training and Education	4	4	4	5	4	4	4	3

Conclusion on Comparison

Each framework has its own strengths and weaknesses, as well as its own unique features and approaches to risk management. For example, the ISO 27005:2018 standard provides a comprehensive and systematic approach to risk management, while NIST's framework offers a practical and flexible approach that can be customized to suit different organizations' needs. IRAM2 is known for its scalability and flexibility, while ISACA's framework emphasizes governance and compliance aspects.

When selecting a risk management framework, it's important to evaluate it based on the specific needs and goals of the organization. Factors to consider might include the industry, the size and complexity of the organization, the types of risks it faces, and its existing risk management program. For example, an organization in the healthcare industry may benefit from a framework with a strong focus on regulatory compliance, while a startup may prioritize scalability and ease of implementation.

Ultimately, the most appropriate framework will depend on the organization's unique context and requirements. It's important to evaluate each framework's strengths and weaknesses in relation to the organization's needs and goals, and to select the one that provides the best fit for its risk management program.

References

1. ISO/IEC 27005:2018. ISO. (2022, October 25). Retrieved April 26, 2023, from https://www.iso.org/standard/75281.html
2. Computer Security Division, I. T. L. (n.d.). NIST Risk Management Framework: CSRC: CSRC. NIST Risk Management Framework | CSRC. Retrieved April 26, 2023, from https://www.nist.gov/cyberframework/risk-management-framework
3. Initiative, J. T. F. T. (2012, September 17). Guide for Conducting Risk Assessments. CSRC. Retrieved April 26, 2023, from https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final
4. NIST SP 800-39. (n.d.). Retrieved April 26, 2023, from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf
5. Stouffer, K., Lightman, S., Pillitteri, V., Abrams, M., & Hahn, A. (2015, June 3). Guide to industrial control systems (ICS) security. CSRC. Retrieved April 26, 2023, from https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final
6. Introducing Octave Allegro: Improving the Information Security Risk Assessment Process. Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process. (2007, May 1). Retrieved April 26, 2023, from https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=8419
7. Isaca Portal. (n.d.). Retrieved April 26, 2023, from https://www.isaca.org/bookstore/bookstore-risk-digital/ritf2
8. TS 102 165-1 - v5.2.3 - Cyber; methods and protocols; part 1 ... - etsi. (n.d.). Retrieved April 26, 2023, from https://www.etsi.org/deliver/etsi_ts/102100_102199/10216501/05.02.03_60/ts_10216501v050203p.pdf
9. Cybersecurity, L. H. of. (n.d.). What is Monarc? MONARC. Retrieved April 26, 2023, from https://www.monarc.lu/
10. Ebios risk manager – the method | agence nationale de la ... - anssi. (n.d.). Retrieved April 26, 2023, from https://www.ssi.gouv.fr/en/guide/ebios-risk-manager-the-method/
11. Microsoft Security Assessment Tool. Microsoft. (n.d.). Retrieved April 26, 2023, from https://www.microsoft.com/en-us/download/details.aspx?id=12273
12. Alford, A., Tatum, G., Bicker, M., Waringa, N., Batten, G., & McRee, R. (n.d.). Simplerisk GRC Software. SimpleRisk GRC Software. Retrieved April 26, 2023, from https://www.simplerisk.com/
13. Módulo. (n.d.). Retrieved April 26, 2023, from https://www.modulo.com/
14. Integrated Risk Management Framework. Risk Management Studio. (2022, January 12). Retrieved April 26, 2023, from https://www.riskmanagementstudio.com/
15. PTA: Practical threat analysis - HOLISTICINFOSEC. (n.d.). Retrieved April 26, 2023, from https://holisticinfosec.io/toolsmith/pdf/september2008.pdf
16. The Open Source Isms Tool: verinice. verinice. (2023, April 6). Retrieved April 29, 2023, from https://verinice.com/en/