# Information Security Risk Management Context establishment at APSS

Katungye Johnson
*Masters in Computer Science*
*University of Trento*


*Azienda Provinciale per i Servizi Sanitari*
*Provincia Autonoma di Trento*

**Supervisors:**
Franco Giampaolo
Alessandro Marchetto

**Abstract**

The COVID-19 pandemic has had a significant impact on how organizations operate, with a major shift towards remote work and an increased reliance on digital technologies.This shift has heightened the importance of cybersecurity, as the need to protect information assets from various cyber threats has become more critical than ever. The Azienda Provinciale per i Servizi Sanitari (APSS) in Trento, Italy, has faced similar challenges and has had to adapt its cybersecurity strategies accordingly. In this paper, I will provide an overview of the cybersecurity risk assessment practices at APSS, highlighting how the organization manages its IT resources and mitigates risks in its operational environment.

# Contents

# 1 Introduction, Motivation and objectives

The medical sector has become increasingly a target for cyber-criminals that leverage the opportunity to disrupt services, claim a ransom, sell the data online, or even use the data to perform other attacks. The use of cutting-edge technology like artificial intelligence (AI) and big data analytics to enhance patient outcomes and change medical treatment is becoming more and more popular. Artificial Intelligence (AI) holds great potential to improve clinical decision-making, optimize administrative procedures, and customize patient care through its capacity to evaluate large volumes of data and produce practical insights. [23]. The advancement in technology has also enabled attackers to perform more sophisticated attacks more easily hence the motivation to review cyber security in the medical sector with a case study of APSS The rapid migration of services that were traditionally paper-based to digital form can be attributed to COVID-19 as many business operations were migrated online to enable citizens to access these services during the lockdown. Ransomware has been a huge cyber threat and has gotten many organizations and individuals into trouble such as financial loss. The attacking pattern of encrypting important data and files causes the daily operation of the organization to be halted. There are various ransomware attacks such as NotPetya, Jigsaw, CryptoLocker, Spider, Wannacry, etc. each with a different attack pattern. Wannacry ransomware started infecting computers in May 2017 and was spread globally at a very fast rate. [39]. WannaCry, exploits a Microsoft Windows vulnerability to encrypt files and this disrupted healthcare services globally, including the UK's National Health Service (NHS), leading to significant operational and financial impacts [17]. Another significant threat is the SamSam ransomware, which involves manual infiltration by attackers, causing extensive disruptions and financial losses in healthcare facilities [22]. Similarly, Ryuk ransomware targets large enterprises, including hospitals, and has led to severe disruptions in emergency services and overall healthcare operations [32]. These attacks not only disrupt critical healthcare services but also compromise sensitive patient data, leading to legal and reputational consequences for the affected organizations [9]. The Convention for the Protection of Individuals regarding automatic processing of Personal Data first introduced in 1981 by the Council of Europe is the only international data protection instruction that is binding to its signatories. The conservation requires the signatories to establish national-level data protection legislation with adequate sanctions for breaking the law. The convention also provides the data subjects access and correction rights, which are more well-known, especially with the European Union General Data Protection Regulation (GDPR) [42]. Through this report I will explore the application of the ISO IEC 27005:2018 to establish the context for a successful risk assessment at APSS, focusing on how the organization's infrastructure architecture, policies, assets and impact core business functions. APSS is an organization that operates mainly in the medical field, which makes it very susceptible to attacks. I aim to document the context of APSS while clearly showing the scope to be considered in the risk assessment and the methodology will be documented to guide the information risk assessment. The Provincial Health Authority of Trento is an instrumental body of the Autonomous Province of Trento with entrepreneurial autonomy and legal personality under public law. It is responsible for the coordinated management of health and social-health activities for the entire provincial territory, in accordance with the provisions of the Provincial Health Plan, the Provincial Health and Social-Health Programme, and the guidelines and provisions of the Provincial Council. [2] Establishing the context is the first step when conducting cybersecurity risk assessment according to the ISO/IEC 27001 [18] and this is fundamental to ensuring that the risk assessment process is aligned with the organization's objectives, environment, and the specific security requirements necessary to protect its information assets.

# 2 Literature Review

With the development of technology throughout the last decades, Information Security risk management (ISRM) has increasingly become more critical in day-to-day operations as it is crucial in determining what to protect and how to invest in security. Several frameworks have been documented by well-known key players in the cybersecurity industry and some by government entities. To stick a balance requires a blend of several frameworks while observing the legal requirements, and organization policies and putting both internal and external factors into consideration to establish the context. ISO/IEC 27005 is an international standard designed to provide guidelines for information security risk management within the broader framework of ISO/IEC 27001 [18]. The ISO/IEC 27005 [18] framework has a role in helping organizations identify, assess, and manage information security risks systematically. According to [**?**], the standard offers a structured approach that integrates risk management into the organization's overall management system. This integration is vital as it ensures that risk management practices are not isolated but rather embedded within the organization's operational procedures and strategic objectives. The framework of ISO/IEC 27005 is built upon fundamental principles of risk management, which include risk identification, risk analysis, risk evaluation, risk treatment, risk acceptance, and risk communication. Literature by [35] underscores the importance of a comprehensive risk assessment process as outlined in the standard. Their research highlights that the effectiveness of ISO/IEC 27005 [18] relies heavily on the accurate identification and analysis of potential threats and vulnerabilities that could impact an organization's information assets. They argue that a thorough understanding of these elements allows for more effective risk evaluation and treatment strategies, ultimately leading to better protection of information assets. Another significant aspect covered in the literature is the flexibility and adaptability of ISO/IEC 27005 [18] to different organizational contexts. Studies by [8] illustrate how the standard can be tailored to various industry sectors, including healthcare, finance, and manufacturing. Their findings suggest that ISO/IEC 27005 provides a robust framework that can be customized to meet the specific needs and regulatory requirements of different sectors. This adaptability is crucial for organizations operating in dynamic environments where risks continually evolve, requiring a flexible and responsive risk management approach. Furthermore, the literature indicates that successful implementation of ISO/IEC 27005 [18] can lead to numerous benefits beyond improved security posture. Consequently, the standard not only helps in managing information security risks but also supports broader organizational goals, making it a critical tool in today's interconnected and risk-prone business environment.

## 2.1 Information Security Risk Management

Information security risk management (ISRM) is a critical process within organizations that involves identifying, assessing, and mitigating risks to information assets. This process is essential for maintaining the confidentiality, integrity, and availability of information in an increasingly digital and interconnected world. The literature extensively explores various frameworks and standards designed to guide organizations in implementing effective ISRM practices. ISO/IEC 27005, a prominent standard in this domain, provides comprehensive guidelines for risk management within the context of an information security management system (ISMS) as specified by ISO/IEC 27001. The core principles of ISRM, as highlighted in ISO/IEC 27005, involve a systematic approach to risk identification, risk assessment, and risk treatment. According to the ISO/IEC 27005 framework [19], context establishment, risk assessment, and risk treatment as the main steps however communication and consultation are very important while monitoring and review facilitate the continuous improvement. The risk identification process is foundational, as it enables organizations to pinpoint potential threats and vulnerabilities. This process is typically followed by a detailed risk assessment, which evaluates the likelihood and impact of identified risks. The literature emphasizes that an accurate risk assessment is crucial for prioritizing risks and determining appropriate risk treatment strategies, which can include risk avoidance, mitigation, transfer, or acceptance [37]. Moreover, the adaptability and flexibility of ISO/IEC 27005 make it applicable to various organizational contexts. Research by Raggard [31] suggests that the standard's guidelines can be tailored to meet the specific needs and regulatory requirements of different industries, such as healthcare, finance, and manufacturing. This adaptability is essential for organizations operating in diverse environments where the nature of information security risks can vary significantly. For instance, healthcare organizations might prioritize patient data protection, while financial institutions might focus on safeguarding transaction integrity and preventing fraud. The ability to customize the Information Security Risk Management approach ensures that organizations can effectively address their unique risk landscapes. The successful implementation of Information Security Risk Management, guided by standards like ISO/IEC 27005, offers numerous benefits beyond enhanced security. Organizations that adopt robust Information Security Risk Management practices often experience improved regulatory compliance, as they can demonstrate adherence to relevant laws and regulations [28]. Additionally, effective risk management fosters stakeholder confidence by showing a commitment to protecting sensitive information. This confidence can translate into a competitive advantage, as clients and partners are more likely to trust organizations with strong security practices. Furthermore, integrating Information Security Risk Management with broader business objectives helps align IT strategies with organizational goals, promoting operational efficiency and resilience [36].

To maintain effective security risk management, it is necessary to identify and implement appropriate security controls [27]. Information security risk management is required to protect the information and ensure confidentiality, integrity, and availability, Security Risk Management and control of information security at APSS's critical assets is an important aspect in providing protection, maintaining business process continuity, and increasing security maturity level. The Cyber Maturity level aims to assess the suitability of the work process of implementing information security management systems in the APSS. The process of information security risk management is regulated by ISO 27001, which is divided into four stages: Plan, Do, Check, and Act [33]

## 2.2 Cyber Security Risk assessment

A cybersecurity risk assessment is a systematic process aimed at identifying vulnerabilities and threats within an organization's IT environment, assessing the likelihood of a security event, and determining the potential impact of such occurrences. [24] Risk analysis is a process of identifying and assessing factors that may harm the business to identify appropriate controls to mitigate these inherent risks, and maintain the impact within acceptable limits (residual risk). Controls and mitigation actions are designed to reduce the likelihood of a risk or impact that has already occurred. The causes of the risks can be the specific internal/external situations, conditions, or events that cause the risk. The causes are unique and very specific to the process, product, service, or activity of the organization. The causes can be weak or inadequate controls, accidental or intentional failures [6] Cyber security is aimed at the protection of hardware, software, and associated infrastructure, networks and the data on them, and the services they provide [40]

## 2.3 Core business Function and business processes of APSS

The Provincial Company for Health Services of Trento is an instrumental body of the Autonomous Province of Trento with entrepreneurial autonomy and legal personality under public law. It is responsible for the coordinated management of health and social-health activities for the entire provincial territory, in accordance with the provisions of the Provincial Health Plan, the Provincial Health and Social-Health Program, and the guidelines and provisions of the Provincial Council [1] By taking the functional approach, this report will be focused on the processes and functions of APSS since the hardware is currently managed by a third-party entity that has separate controls and measures in place to address cyber risk. The function-focused approach is the opposite of the asset-focused approach. Instead of focusing on critical assets, an organization focuses on the critical processes and functions an organization performs. This approach is best for organizations where infrastructure continuity is more important than the assets themselves. [29] Information in the medical domain is PII(personally identifiable Information) and can easily be used to directly or indirectly identify a person making this information highly confidential despite its great importance to different stakeholders, which may include the doctors to find the right diagnosis, the researchers to discover new treatment methods, to students that a in the process of becoming medical practitioners but also to the government that needs to allocate resources to the medical sector and provide funding to medical activities. Technology has become the central nervous system of a business, supporting the flow of information that drives each business process from product development to sales. [14]

# 3 Context Establishment

A systematic approach to information security risk management is necessary to identify organizational needs regarding information security requirements and to create an effective information security management system [19]. This report will mainly focus on the Context establishment while applying the ISO 27005 [18]. ISO 27005, a part of the ISO 27000 series of standards, provides a framework for managing information security risks. Context establishment is the initial phase of the ISO 27005:2018 process. It involves defining the external and internal parameters to be taken into account when managing information security risks, setting the scope and boundaries of the risk management process, and defining the risk assessment methodology [5]. The context of an organization is not static and can change over time due to

various factors such as changes in the external or external environment, changes in the organization's strategy and objectives, and changes in the information security risks. Therefore, it's important to monitor and review the context periodically to ensure that it remains relevant and up-to-date. The findings from the monitoring and review process should be adequately communicated through well-established channels to the designated individuals tasked with imaging risk. [5]

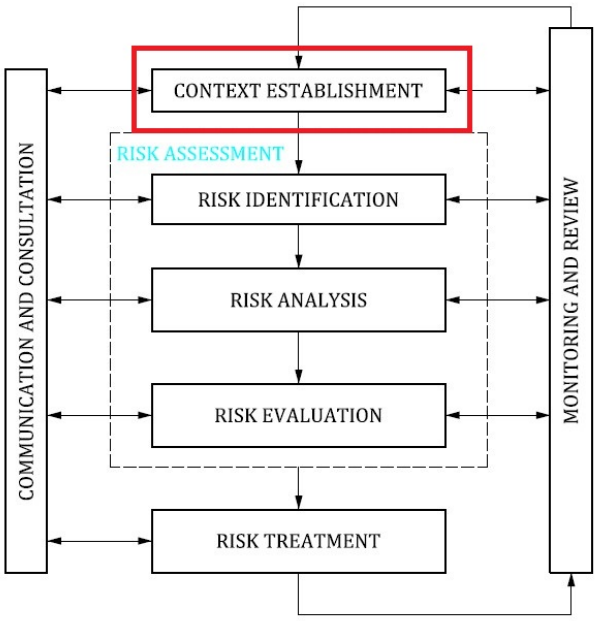


Figure 1: The risk management process

The first step will involve understanding the daily operations of the organization as already established APSS is involved in the medical industry. This implies that not only does it have to comply with the GDPR but also with the NIS2. The EU cybersecurity rules introduced in 2016 were updated by the NIS2 Directive that came into force in 2023. It modernized the existing legal framework to keep up with increased digitization and an evolving cybersecurity threat landscape. By expanding the scope of the cybersecurity rules to new sectors and entities, it further improves the resilience and incident response capacities of public and private entities, competent authorities, and the EU as a whole. [10] Legal obligations such as NIS2 The NIS2 Directive sets out a number of requirements for organizations to improve their cybersecurity, which include

- Risk assessment and management: Organizations must identify and evaluate the cybersecurity risks they face and implement appropriate security measures to prevent or mitigate them.
- Incident reporting: Organizations must notify their national cybersecurity authority of any significant cybersecurity incidents that affect their networks or information systems within 24 hours.
- Incident response: Organizations must have plans and procedures to respond to and recover from cybersecurity incidents as quickly and effectively as possible.

- Communication and cooperation: Organizations must share information and best practices with the national cybersecurity authority to enhance their cybersecurity capabilities and awareness.
- Security awareness and training: Organizations must ensure that their staff is trained and educated on how to protect themselves and their organization from cyber threats and how to report any suspicious activity.
- Supply chain security: Organizations must assess and manage the cybersecurity risks posed by their suppliers and ensure that the products and services they use are secure and reliable.
- Resilience: Organizations must take steps to increase the resilience of their networks and information systems to withstand and recover from cyberattacks. This includes having backup systems, recovery plans, and security controls that are resistant to cyberattacks

## 3.1 Stakeholder Internal and External Identification

### 3.1.1 Internal Stakeholders

Internal stakeholders, including employees, IT staff, and management, are integral to the ISRM process. Employees at all levels must be aware of and adhere to information security policies and procedures. [34] emphasize that employees' compliance with security practices is vital for reducing human-related security risks. Training and awareness programs are often highlighted in the literature as essential tools for fostering a security-conscious culture within the organization.

IT staff and security professionals are particularly crucial in the technical implementation of ISRM. According to [38], these individuals are responsible for identifying vulnerabilities, deploying security measures, and monitoring systems for potential threats. Their expertise is necessary for conducting thorough risk assessments and implementing effective risk treatment strategies. Furthermore, top management plays a pivotal role in providing the necessary resources and support for ISRM initiatives. The commitment of leadership to prioritizing information security can significantly influence the success of ISRM efforts [41].

### 3.1.2 External Stakeholders

External stakeholders, including customers, partners, suppliers, and regulatory bodies, also play a critical role in ISRM. Customers and partners often demand assurance that their data is protected, which can drive organizations to adopt stringent security measures. Literature by [11] suggests that maintaining strong security practices can enhance customer trust and business relationships. Suppliers and third-party vendors, who may have access to sensitive information or critical systems, must also be considered in the ISRM process. Effective third-party risk management involves assessing the security posture of these external entities and ensuring they comply with the organization's security requirements [13].

Regulatory bodies impose legal and compliance requirements that organizations must meet to avoid penalties and reputational damage. Compliance with standards such as the General Data Protection Regulation (GDPR) or industry-specific regulations (e.g., HIPAA for healthcare) is a critical aspect of ISRM. Research by [21] highlights the importance of aligning ISRM practices with regulatory expectations to ensure legal compliance and protect the organization's

interests. Engaging with regulators and understanding the evolving legal landscape is essential for maintaining a robust ISRM framework.

### 3.1.3 Collaborative Approach

The literature underscores the need for a collaborative approach involving both internal and external stakeholders to enhance the effectiveness of ISRM. [41] argue that fostering communication and cooperation among stakeholders can lead to better risk identification and more comprehensive risk management strategies. For instance, regular interactions between IT staff and business units can help align security measures with organizational goals, while collaboration with external partners can strengthen overall security posture through shared knowledge and resources.

In conclusion, internal and external stakeholders are crucial to the success of information security risk management. Internal stakeholders, including employees, IT staff, and management, provide the necessary support and expertise for implementing ISRM practices. External stakeholders, such as customers, partners, suppliers, and regulatory bodies, influence the organization's security requirements and compliance efforts. A collaborative approach that integrates the contributions of all stakeholders is essential for developing a resilient and effective ISRM framework, ultimately safeguarding the organization's information assets.

## 3.2 Scope and Boundaries

All information about the organization relevant to the information security risk management context establishment will include Assets derived from Critical business processes and functions that have been mapped to the services they are associated with. With an environment made of both on Prem, IaaS, and SaaS, APSS will have to apply a wide range of measures to accommodate the hybrid nature of the infrastructure setup.

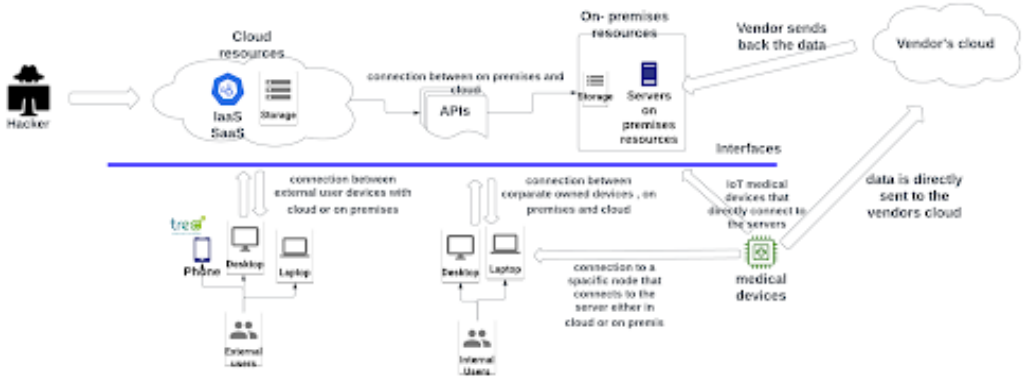


Figure 2: Abstract infrastructure at APSS.

Risk varies over time and for different environments in which organizations operate and to examine all vulnerabilities a daunting task must be undertaken requiring a lot of resources however organizations have to prioritize among the constantly growing number of vulnerabilities to derive a list of priorities to be considered. This can be considered a good representation of a cyber risk context. For risk management to be effective, the objectives registered must include the top value creation/preservation objectives and specify owners and sponsors at the highest organizational level There are two ways to perform this as indicated below

- Active scanning: By using specialized scanning tools to send packets to map out existing hardware devices and applications in a network for example Nmap
- Passive scanning: This uses scanning software to gather information from a network or target system without actively interacting with its endpoints

Both methods result in an inventory with details of crucial information such as asset name, description, location, owner, asset tag [29]

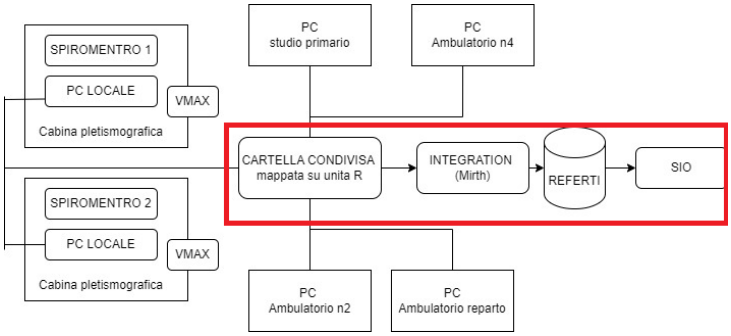


Figure 3: Scenario

The area marked in the red square is comprised of servers that process and store data, there is an endpoint to the Tec+ app. The area out of the red square are considered clients and are mainly involved in collecting data and providing the interface to review and update the data.

# 4 Methodology

To establish an ideal approach I have chosen guidelines that will help evaluate the acceptable risk through a systematic consistent approach that is well-aligned with the organization's objectives By taking the business processes and mapping them to the Information Technology services I will assume that services that are connected to multiple business processes are more important than those connected to few services. The services are mapped to possible threats and vulnerabilities with a likelihood and impact score attached. It's from the product of Impact and likelihood scores that the risk is derived to indicate the risk level which is then compared against the risk acceptance to determine the action. This report will mainly stop at identifying the risk score of the selected assets in this case the IT services derived from the business process.

## 4.1 Information assets Inventory

By understanding the data lifecycle and its associated states is essential for comprehensive risk management in information security. Data typically progresses through several stages: creation or collection, storage, processing or use, transmission or transfer, archival or retention, and finally, deletion or disposal. At each stage, data faces distinct security risks, such as unauthorized access, data breaches during transmission, or incomplete erasure upon disposal. Effective risk management involves conducting thorough risk assessments at each lifecycle stage to identify vulnerabilities and threats.

## 4.2 Impact, Likelihood, and Risk

A risk is a function of the impact and probability of an event that may impede the achievement of business objectives and processes and may lead to some losses. [6] Information security risk is associated with the potential threats that will cause vulnerabilities of an information asset or group of information assets to be exploited and thereby cause harm to an organization [25] while the World Economic Forum points out that Cyber risk is a combination of the probability of an event in the field of network information systems and the effects of this event on assets and reputation of an organization, [43]. I would like to point out that probability has often been inferred to as the likelihood while effect as impact as stated by NIST. Risk is a measure of the extent to which an entity is threatened by a potential circumstance or event, and is typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. Information security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (i.e., mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation. Information security is generally defined as the process of maintaining the confidentiality, integrity and availability of information, also in terms of maintaining the authenticity, accountability, non-repudiation and reliability of information. In carrying out the processes related to information security, its involves three main elements, namely those (people) who do the job, procedures and policies as well as a reference process technology as a tool in the implementation of information security systems. Management of information security system covers at least four important aspects, namely privacy / confidentiality, integrity, authentication, and availability [25]

Risk assessment is the process of identifying, estimating, and prioritizing information security risks. Assessing risk requires the careful analysis of threat and vulnerability information to determine the extent to which circumstances or events could adversely impact an organization and the likelihood that such circumstances or events will occur [26]. confidentiality is concerned with ensuring that information is neither disclosed nor made available to those who are not authorized to have access to it. Integrity is concerned with securing the accuracy and trustworthiness of information however it's stored or transmitted. integrity involves ensuring that only authorized people can create, change, or delete information and is very closely linked with confidentiality since people who have whether authorized or not access to information will also cause integrity issues. Availability is concerned with ensuring that systems and the information stored on them are available for use when required and by whatever means have been agreed upon. [42] The Common Vulnerability Scoring System (CVSS) is an open framework for communicating the characteristics and severity of software vulnerabilities. CVSS consists of three metric groups: Base, Temporal, and Environmental. The Base group represents the intrinsic qualities of a vulnerability that are constant over time and across user environments, the Temporal group reflects the characteristics of a vulnerability that change over time, and the Environmental group represents the characteristics of a vulnerability that are unique to a user's environment. The Base metrics produce a score ranging from 0 to 10, which can then be modified by scoring the Temporal and Environmental metrics. A CVSS score is also represented as a vector string, a compressed textual representation of the values used to derive the score. [12]

The risk ($R$) is calculated as the product of impact ($I$) and likelihood ($L$):

$$R = I \times L \tag{1}$$

The Base metric group represents the intrinsic characteristics of a vulnerability that are

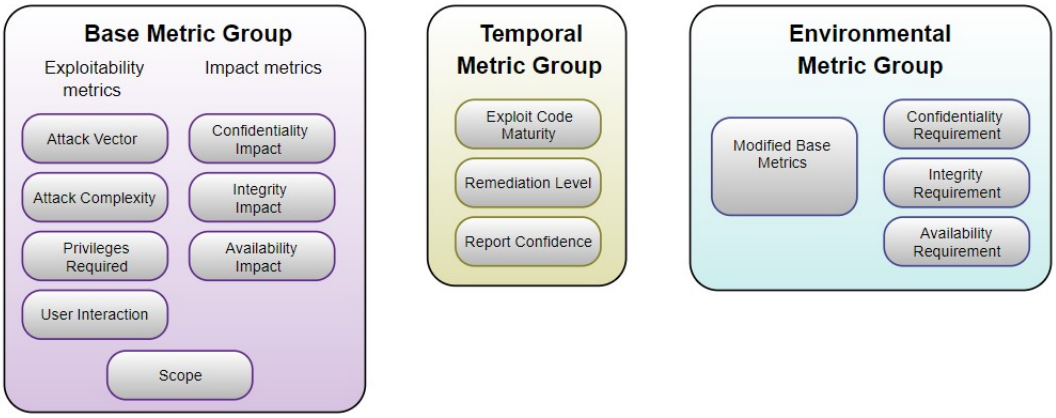


Figure 4: Common Vulnerability Scoring System v3.1

constant over time and across user environments. It is composed of two sets of metrics: the Exploitability metrics and the Impact metrics. The Acceptability metrics reflect the ease and technical means by which the vulnerability can be exploited. That is, they represent characteristics of the thing that is vulnerable, which we refer to formally as the vulnerable component. The Impact metrics reflect the direct consequence of a successful exploit, and represent the consequence to the thing that suffers the impact, which we refer to formally as the impacted component. While the vulnerable component is typically a software application, module, driver, etc. (or possibly a hardware device), the impacted component could be a software application, a hardware device, or a network resource. This potential for measuring the impact of a vulnerability other than the vulnerable component was a key feature introduced with CVSS v3.0. This property is captured by the Scope metric, discussed later. The Temporal metric group reflects the characteristics of a vulnerability that may change over time but not across user environments. For example, the presence of a simple-to-use exploit kit would increase the CVSS score, while the creation of an official patch would decrease it. The Environmental metric group represents the characteristics of a vulnerability that are relevant and unique to a particular user's environment. Considerations include the presence of security controls which may mitigate some or all consequences of a successful attack, and the relative importance of a vulnerable system within a technology infrastructure. [12]

## 4.3 Risk Appetite and Tolerance

Risk appetite and risk tolerance are fundamental concepts in information security risk management (ISRM) that play a crucial role in shaping an organization's approach to handling risks. Within the framework of ISO/IEC 27005, these concepts help define the levels of risk that an organization is willing to accept and the thresholds at which risks become unacceptable. Understanding and articulating risk appetite and tolerance are essential for effective decision-making and for aligning risk management practices with organizational objectives.

## 4.4 Risk Appetite in APSS

Risk appetite refers to the amount and type of risk an organization is willing to pursue or retain in order to achieve its strategic objectives. According to the ISO/IEC 27005 standard, establishing a clear risk appetite is vital as it guides the organization in making informed decisions

about risk management. The literature emphasizes that risk appetite should be aligned with the organization's overall strategy, culture, and external environment [7]. It acts as a benchmark for evaluating whether potential risks are acceptable in the context of the organization's goals and resources.

The process of determining risk appetite involves input from various internal stakeholders, including senior management, IT staff, and risk management professionals. A study by [16] highlights that risk appetite must be communicated effectively across the organization to ensure that all employees understand the levels of risk that are permissible. This clarity helps in aligning the actions and decisions of different departments with the organization's risk management objectives. Additionally, risk appetite should be periodically reviewed and adjusted to reflect changes in the organization's internal and external environments.

## 4.5 Risk Tolerance in APSS

Risk tolerance, on the other hand, refers to the specific maximum risk that an organization is willing to accept for particular risk categories or activities. It is more granular than risk appetite and provides detailed thresholds for acceptable risk levels. ISO/IEC 27005 suggests that organizations should establish risk tolerance levels to facilitate the consistent application of risk management practices. These levels help in identifying when risk treatment actions are necessary and when risks can be accepted without further mitigation [18].

Literature by [3] indicates that risk tolerance thresholds should be based on quantitative and qualitative assessments of potential impacts and the likelihood of risks materializing. This involves using risk assessment tools and techniques to evaluate risks against the defined tolerance levels. By setting clear risk tolerance thresholds, organizations can ensure a uniform approach to managing risks and avoid subjective or inconsistent decision-making. Moreover, risk tolerance should be flexible enough to adapt to emerging threats and changing business conditions.

## 4.6 Integrating Risk Appetite and Tolerance

The integration of risk appetite and tolerance within ISO/IEC 27005 is essential for a coherent and effective ISRM strategy. By defining both concepts clearly, organizations can create a robust framework for identifying, assessing, and treating risks. Research by [20] suggests that a well-defined risk appetite and tolerance framework enables organizations to prioritize risk management efforts and allocate resources more effectively. It also supports better communication and understanding of risk-related decisions among stakeholders.

Furthermore, ISO/IEC 27005 emphasizes the importance of aligning risk appetite and tolerance with the organization's risk treatment options. For instance, risks that exceed the tolerance levels might require mitigation actions such as implementing additional security controls, transferring the risk through insurance, or avoiding the risk altogether. Conversely, risks within the acceptable tolerance levels might be accepted with continuous monitoring. This alignment ensures that risk management practices are not only effective but also efficient, avoiding unnecessary expenditures on low-priority risks.

## 4.7 Legal, regulatory and contractual

Implementing robust security controls such as encryption for data in transit and at rest, stringent access controls, and regular monitoring for anomalies ensures data confidentiality, integrity, and

availability are upheld. Moreover, adherence to regulatory requirements and industry standards throughout the data life cycle enhances compliance and reduces legal risks associated with data management. By integrating these practices into their information security frameworks, organizations can proactively mitigate risks and safeguard sensitive data throughout its lifecycle. [4] The term data life cycle refers both to the transformations applied to data and to the states that data goes through as a result of these transformations. While there is not, unfortunately, general agreement on the exact details of what is involved at each transformation and state, or how to refer to them, there is a wide consensus on the basic outlines. The states of the cycle can be summarized as follows:

Raw data → cleaned data → prepared data → data + results → archived data

The arrows here indicate precedence; that is, raw data comes first and cleaned data is extracted from it, and so on. The activities are usually described as follows:

Data Acquisition/capture → data storage → data cleaning/wrangling/enrichment → data analysis → data archival/preservation [4]

data can be obtained from various sources and several operations can be performed on the data at different stages where it is in transit, storage, or in use.

# 5 Acknowledgement

There is no 100% effective way to prevent all cybersecurity breaches but cybersecurity must form part of the risk management process and cyber resilience must be ensured. Cyber resilience is a holistic view of cyber risk, which looks at culture, people, and processes, as well as technology [30] Cybersecurity is an essential part of maintaining the safety, privacy, and trust of patients. More money and effort must be invested into 5ensuring the security of healthcare technologies and patient information. Security must be designed into the product from conception and not be an afterthought. Cybersecurity must become part of the patient every organization that has digitalized business processes.

# 6 conclusion

While healthcare technologies play key roles in our population's health they are vulnerable to security threats due to interconnected, easily accessible access points, outdated systems, and a lack of emphasis upon cybersecurity. Focus has tended to be placed upon patient care, however healthcare technologies hold vast amounts of valuable, sensitive data. In many cases financial gain is the motivation for attacks, as medical identity is more valuable than other identity credentials. Other attacks may be motivated by political gain, even cyber warfare. However if critical health systems are attacked, human lives are at risk.An attack could result in loss of functioning of critical equipment within hospitals such as intensive care units [15]

# References


[1] apss.tn.it. Servizi e prestazioni. Azienda Provinciale per I Servizi Sanitari, June 22 2020. Accessed: 2024-06-20.

[2] Apss.Tn.It. Azienda. `https://www.apss.tn.it/Azienda`, November 17 2023. Retrieved from `https://www.apss.tn.it/Azienda`.

[3] T. Aven. On the meaning of a black swan in a risk context. *Safety Science*, 57:44–51, 2013.

[4] Antonio Badia. *SQL for Data Science: Data Cleaning, Wrangling and Analytics with Relational Databases*. Springer, 2020.

[5] Gijs Brandenburg and Gijs Brandenburg. ISO27005 series part 2: Context Establishment, 6 2023.

[6] V. Briceag and T. Bragaru. Cyber security risk assessment. *Economica*, 1(115):123–139, 2021.

[7] P. Bromiley, M. McShane, A. Nair, and E. Rustambekov. Enterprise risk management: Review, critique, and research directions. *Long Range Planning*, 48(4):265–276, 2015.

[8] A. Brown and Z. Nasir. *Adapting ISO/IEC 27005 to Industry-Specific Contexts*. Publisher Name, 2019.

[9] Lynn Coventry and Dawn Branley. Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. *Maturitas*, 113:48–52, 2018.

[10] Digital-Strategy.ec.europa.eu. Directive on measures for a high common level of cybersecurity across the union (nis2 directive) — shaping europe's digital future. `https://digital-strategy.ec.europa.eu/en/policies/nis2-directive`, n.d. Retrieved June 20, 2024.

[11] M. M. Eloff and J. H. P. Eloff. Information security architecture. *Computer Fraud & Security*, 2005(11):10–16, 2005.

[12] FIRST — Forum of Incident Response and Security Teams. CVSS v3.1 Specification Document. FIRST — Forum of Incident Response and Security Teams, 2019. Retrieved from `https://www.first.org/cvss/v3.1/specification-document`.

[13] L. A. Gordon, M. P. Loeb, W. Lucyshyn, and R. Richardson. Csi/fbi computer crime and security survey. Technical report, Computer Security Institute, 2006.

[14] M. Harkins. *Managing Risk and Information Security: Protect to Enable*. Apress, Berkeley, CA, 2013.

[15] Debiao He, Sherali Zeadally, Neeraj Kumar, and Jae-Hyun Lee. Anonymous authentication for wireless body area networks with provable security. *IEEE Systems Journal*, 11(4):2590–2601, 2017.

[16] D. Hillson and R. Murray-Webster. *Understanding and Managing Risk Attitude*. Gower Publishing, Ltd., 2007.

[17] Mohammad I Hussain, A Abubakar, and F Haque. The impact of wannacry ransomware on hospital services: A brief report. *Cureus*, 10(2):e2091, 2018.

[18] International Organization for Standardization. *ISO/IEC 27005:2018. Information Technology — Security Techniques — Information Security Risk Management*, 2018.

[19] International Organization for Standardization. Iso/iec 27005:2018, 2023.

[20] R. S. Kaplan and A. Mikes. Managing risks: A new framework. *Harvard Business Review*, 2012.

[21] M. Ko, J. Lee, and J. Lee. A study on the impact of regulations on information security management systems. *Journal of Information Systems*, 23(2):77–94, 2009.

[22] James B Kramer, Alan Watson, and Richard Nathan. The rising threat of ransomware in healthcare settings. *Journal of Healthcare Protection Management*, 35(1):65–72, 2019.

[23] Anit Mukherji. The evolution of information systems: their impact on organizations and structures. *Management Decision*, 40(5):497–507, 2002.

[24] Janani Nagarajan. How To Perform a Cybersecurity Risk Assessment - CrowdStrike — crowdstrike.com. https://www.crowdstrike.com/cybersecurity-101/advisory-services/cybersecurity-risk-assessment/. [Accessed 24-06-2024].

[25] Merry Nancylia, Eddy K Mudjtabar, Sarwono Sutikno, and Yusep Rosmansyah. The measurement design of information security management system. In *2014 8th International Conference on Telecommunication Systems Services and Applications (TSSA)*, pages 1–5, 2014.

[26] National Institute of Standards and Technology. Guide for conducting risk assessments nist special publication 800-30 revision 1. JOINT TASK FORCE TRANSFORMATION INITIATIVE, 2012. Retrieved from https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf.

[27] Jay Payette, Esther Anegbe, Erika Caceres, and Steven Muegge. Secure by design: Cybersecurity extensions to project management maturity models for critical infrastructure projects. *Technology Innovation Management Review*, 5:26–34, 06/2015 2015.

[28] Thomas R. Peltier. *Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management*. Auerbach, 2002.

[29] Proact Group. Conducting a cyber risk assessment: a comprehensive guide. https://www.proact.eu/blog/cyber-risk-assessment/, n.d. Retrieved June 20, 2024.

[30] PwC. Pwc insurance 2020 and beyond, 2015. https://www.pwc.com/gx/en/insurance/publications/assets/pwc-insurance-2020-and-beyond.pdf.

[31] Bel G. Raggad. *Information Security Management: Concepts and Practice*. CRC Press, an imprint of Taylor and Francis, first edition, 2010.

[32] R Richardson and M North. Ransomware: Evolution, mitigation and prevention. *International Management Review*, 13(1):10–21, 2017.

[33] Dana Indra Sensuse, Andy Syahrizal, Faizan Aditya, and Muhammad Nazri. Information security risk management planning of digital certificate management case study: Balai sertifikasi elektronik. In *2020 Fifth International Conference on Informatics and Computing (ICIC)*, pages 1–7, 2020.

[34] M. Siponen, M. A. Mahmood, and S. Pahnila. Employees' adherence to information security policies: An exploratory field study. *Information & Management*, 51(2):217–224, 2014.

[35] J. Smith and D. Brooks. *The Comprehensive Guide to ISO/IEC 27005*. Publisher Name, 2018.

[36] T. Sommestad, J. Hallberg, K. Lundholm, and J. Bengtsson. A review of the theory of planned behaviour in the context of information security policy compliance. *Computers & Security*, 34(1):46–55, 2014.

[37] Gary Stoneburner, Alice Goguen, and Alexis Feringa. Risk management guide for information technology systems, January 2002. `https://doi.org/10.6028/nist.sp.800-30`.

[38] D. W. Straub and R. J. Welke. Coping with systems risk: Security planning models for management decision making. *MIS Quarterly*, 22(4):441–469, 1998.

[39] Chee Chung Tan and Vinesha Selvarajah. Wannacry ransomware attack: The enemy lies under your blanket. *AIP Conference Proceedings*, 2802(1):150007, 01 2024.

[40] Hasan Mahbub Tusher, Ziaul Haque Munim, Theo E. Notteboom, Tae-Eun Kim, and Salman Nazir. Cyber security risk assessment in autonomous shipping. *Maritime economics logistics*, 24(2):208–227, 2022.

[41] R. Von Solms and B. Von Solms. The 10 deadly sins of information security management. *Computers & Security*, 23(5):371–376, 2004.

[42] Helen Wong. *Cyber security : law and guidance*. Bloomsbury Professional, Haywards Heath, 2018.

[43] World Economic Forum. Global risks 2012, seventh edition, January 5 2012. Retrieved from https://www.weforum.org/publications/global-risks-2012-seventh-edition/.