Computer and Information Science; Vol. 16, No. 4; 2023
ISSN 1913-8989 E-ISSN 1913-8997
Published by Canadian Center of Science and Education

The Evolution of Information Security Strategies: A Comprehensive Investigation of INFOSEC Risk Assessment in the Contemporary Information Era

Abdullah Al Hayajneh[1], Hasnain Nizam Thakur[1], Kutub Thakur[1]

[1] Professional Security Studies Department, New Jersey City University, Jersey City, NJ, USA

Correspondence: Abdullah Al Hayajneh, Professional Security Studies Department, New Jersey City University, Jersey City, NJ, USA.

Received: September 14, 2023 Accepted: October 21, 2023 Online Published: November 20, 2023

doi:10.5539/cis.v16n4p1 URL: https://doi.org/10.5539/cis.v16n4p1

Abstract

In the contemporary era marked by the extensive utilization of data, information systems have been extensively embraced by global organizations and also hold a pivotal position in national defense and various other domains. The growing interconnectedness between individuals and diverse information systems has resulted in an intensified emphasis on the evaluation of potential risks. The mitigation of these dangers extends beyond simple technological solutions and includes established standards, legal structures, and policies, adopting a complete approach based on safety engineering concepts. This study aims to develop a robust framework for the harmonization of Information Technology Security Standards. It will explore prevalent techniques for conducting risk assessments and differentiate between quantitative and qualitative approaches to evaluation. Moreover, this study illustrates the combination of quantitative and qualitative evaluation methodologies, providing a comprehensive framework for the analysis and design of risk assessment. In addition, this study advances our understanding of INFOSEC risk assessment and contributes to the advancement of more efficient information security strategies by sharing global perspectives, addressing challenges in classification, clarifying the incorporation of Information Security Management Systems (ISMS), and highlighting the significance of Artificial Intelligence in the domain of Information Security (INFOSEC).

Keywords: information Security Systems (INFOSEC), Information Security, Risk Assessment, Quantitative and Qualitative approaches, Artificial Intelligence

1. Introduction

1.1 Information Risk

The necessity for information security arises from the inherent risks associated with the utilization of technology in the management of information. From a comprehensive perspective, information is susceptible to unauthorized disclosure, which has the potential to compromise its confidentiality; it is vulnerable to unauthorized alterations, posing risks to its integrity; and it is also susceptible to destruction or loss, which could undermine its availability. The financial impact on the proprietor resulting from the loss of a valuable information asset, whether explicitly apparent or not, is a consistent outcome. Such financial repercussions can manifest both directly, influencing the inherent worth of the information asset itself, and indirectly, giving rise to diverse consequences encompassing service disruptions, reputational harm, erosion of competitive advantage, legal accountabilities, and other contributing factors (Blakley et al., 2001). The application of risk assessment principles to the realm of information security has been evident since the 1960s. Initially, the focus of risk assessment was primarily directed toward matters of confidentiality. However, during the transition period spanning from the late 1980s to the mid-1990s, the safeguarding of computers and network security emerged as prominent concerns within the ambit of risk assessment (Blakley et al., 2001), (Behnia et al., 2012). Notably, experts introduced additional dimensions such as integrity and availability, thereby enhancing the comprehensiveness of information security considerations. The swift and profound evolution of the internet and mobile communication technologies has engendered a ubiquitous challenge for global denizens of the digital realm – that of effectively preserving the confidentiality of personal information. A pivotal milestone in the domain of international information security standards occurred in 2013 with the revision of the "Information Technology – Security Techniques – Code of Practice for Information

Security Management," a publication endorsed by ISO/IEC (Behnia et al., 2012).

In the pursuit of enhancing the precision and effectiveness of risk assessment, the development of supplementary methodologies has been undertaken to facilitate the evaluation of security risks. A notable illustration of such advancements is exemplified by COBRA (Consultative, Objective and Bi-functional Risk Analysis), devised by British C & A Systems Security Ltd. in the year 1991 (Schmidt, 2023). Within this framework, the enterprise leverages collected questionnaire data to appraise the security status of an organization within the context of the risk assessment report. Another noteworthy tool, CRAMM (CCTA Risk Analysis and Management Method), stands as an expansive and adaptable mechanism tailored for the strategic substantiation of prioritized countermeasures at a managerial echelon. Notably, the optimal deployment of CRAMM necessitates the engagement of proficient and seasoned practitioners to ensure efficacious outcomes (Schmidt, 2023), (Fredriksen et al., 2002). Furthermore, the arena of risk assessment has witnessed the emergence of CORA (Cost-of-Risk Analysis), introduced by International Security Technology, Inc. (ICT). CORA employs meticulously gathered data pertaining to the spectrum of threats, functions, assets, and vulnerabilities inherent in said functions and assets. Subsequently, these factors are harmonized with the corresponding threat profiles, thereby facilitating the quantitative estimation of potential consequences ensuing from identified risks (Behnia et al., 2012), (Schmidt, 2023), (Fredriksen et al., 2002).

Modern risk assessment goes beyond what was previously limited to a technological study report. Its scope has expanded to include a detailed analysis of many different aspects, such as technology infrastructure, technical examination of systems and physical hardware, human resource management, and a nuanced characterization of the benefits and drawbacks of current methods. The modern paradigm of information security risk assessment demands a holistic approach that goes beyond narrow focal points. However, it is important to recognize that results from similar situations may show variances that might be ascribed to the various criteria created by various national committees.

This paper focuses on the following key areas:

a) A meticulous examination of current global research efforts related to risk assessment alongside a succinct introduction to prevalent evaluative methodologies.

b) An investigation into the classification and valuation of essential risk components such as assets, threats, and vulnerabilities, along with a comprehensive explanation of the challenges inherent to risk assessment and the resulting evolving requirements.

c) A clear explanation of the standards governing Information Security Management Systems (ISMS), along with an exploration of how these standards are put into practice and the presentation of a comprehensive framework detailing the stages of evaluation.

1.2 Risk Assessment of Information System

The field of information security encompasses the protection of the confidentiality, integrity, and availability of information. Furthermore, it covers additional properties such as authenticity, accountability, non-repudiation, and reliability (ISO/IEC JTC1 SC 27, 2013). Within the framework of risk assessment talks, there is a tendency for financial concerns, assets, and threats to assume a position of priority. Examining a scenario from the perspective of risk assessment: let us contemplate a circumstance in which I experience a financial loss of one hundred dollars as a consequence of my own carelessness, leading to a lack of finances for the purpose of having dinner. Within this particular framework, the term '100 dollars' serves as a representation of an asset, while 'negligence' denotes a state of vulnerability. Additionally, 'stealing' is characterized as a potential danger, 'loss of money' is conceptualized as a manifestation of risk, and the subsequent inability to afford supper is regarded as the resultant effect. Significantly, vulnerability and threat are identified as causal elements, whereas risk and effect are regarded as end results. The process of conducting a security risk assessment entails the examination of factors such as Confidentiality, Integrity, and Availability (CIA), in addition to other safety considerations, during the various stages of information processing, transmission, and storage within a system. The objective of this analytical procedure is to assess the level of security by incorporating the elements of vulnerability, threat, risk, and the subsequent consequences (ISO/IEC JTC1 SC 27, 2013). The primary objective of information security management is to mitigate risk to a degree that is financially feasible and in accordance with established norms through the implementation of comprehensive and cohesive risk control methodologies.

1.3 Meaning of Risk Assessment

Risk assessment serves as the fundamental basis for ensuring the security of information systems. The ability of an executor to effectively assess, manage, and mitigate risks is contingent upon their accurate and comprehensive understanding of the various hazards involved (Stoneburner et al., 2002). Moreover, it is impractical to strive for absolute safety or eradicate all risks inside a system without taking into account associated costs. Information security necessitates being directed by social demands and prioritizing numerous crucial aspects. This entails doing a thorough risk assessment followed by implementing appropriate control measures. Organizations use risk assessment to determine the extent of the potential threat and the risk associated with an IT system throughout its Software Development Life Cycle SDLC. Risk is a function of the likelihood of a given threat-source's exercising a particular potential vulnerability and the resulting impact of that adverse event on the organization (Stoneburner et al., 2002). To determine the likelihood of a future adverse event, threats to an IT system must be analyzed in conjunction with the potential vulnerabilities and the controls in place for the IT system. Impact refers to the magnitude of harm that could be caused by a threat's exercise of vulnerability. The level of impact is governed by the potential mission impacts and, in turn, produces a relative value for the IT assets and resources affected (e.g., the criticality and sensitivity of the IT system components and data) (Stoneburner et al., 2002).

The risk assessment technique consists of nine fundamental components, including: The first step involves system characterization, followed by the identification of threats in the second step. The third step entails identifying vulnerabilities, while the fourth step involves doing a control analysis. The fifth step focuses on determining the likelihood of occurrence, and the sixth step involves conducting an impact analysis. The seventh step entails determining the overall risk, followed by the eighth step, which involves making control recommendations. Finally, the ninth step involves documenting the results obtained from the previous steps. Steps 2, 3, 4, and 6 have the potential to be executed concurrently subsequent to the completion of Step 1. Figure 1 illustrates the sequential progression of these processes, together with the corresponding inputs and outputs associated with each step (Stoneburner et al., 2002)

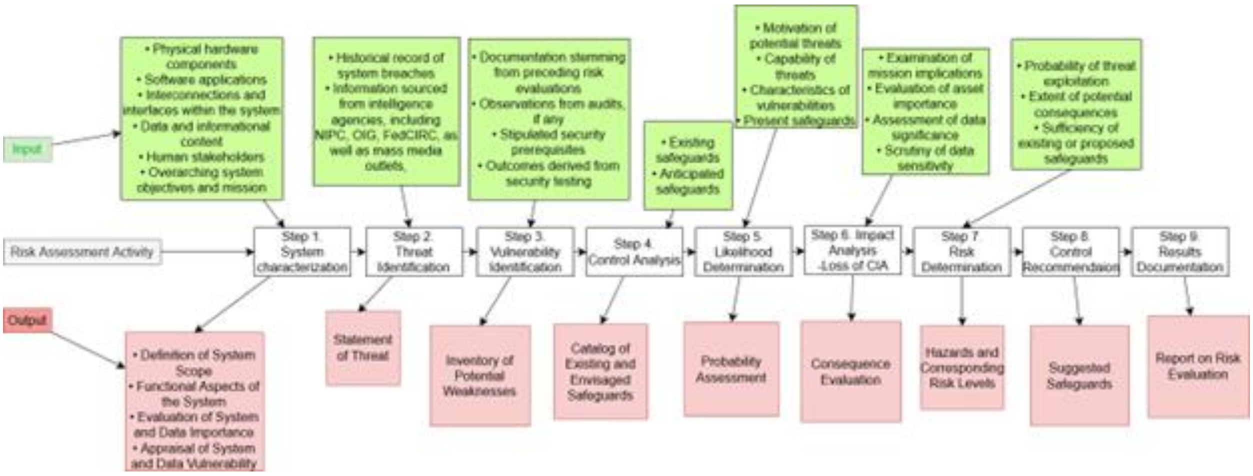
Input
• Physical hardware components
• Software applications
• Interconnections and interfaces within the system
• Data and informational content
• Human stakeholders
• Overarching system objectives and mission
• Historical record of system breaches
• Information sourced from intelligence agencies, including NIPC, OIG, FedCIRC, as well as mass media outlets.
• Documentation stemming from preceding risk evaluations
• Observations from audits, if any
• Stipulated security prerequisites
• Outcomes derived from security testing
• Existing safeguards
• Anticipated safeguards
• Motivation of potential threats
• Capability of threats
• Characteristics of vulnerabilities
• Present safeguards
• Examination of mission implications
• Evaluation of asset importance
• Assessment of data significance
• Scrutiny of data sensitivity
• Probability of threat exploitation
• Extent of potential consequences
• Sufficiency of existing or proposed safeguards
Risk Assessment Activity
Step 1. System characterization
Step 2. Threat Identification
Step 3. Vulnerability Identification
Step 4. Control Analysis
Step 5. Likelihood Determination
Step 6. Impact Analysis -Loss of CIA
Step 7. Risk Determination
Step 8. Control Recommendaion
Step 9. Results Documentation
Output
• Definition of System Scope
• Functional Aspects of the System
• Evaluation of System and Data Importance
• Appraisal of System and Data Vulnerability
Statement of Threat
Inventory of Potential Weaknesses
Catalog of Existing and Envisaged Safeguards
Probability Assessment
Consequence Evaluation
Hazards and Corresponding Risk Levels
Suggested Safeguards
Report on Risk Evaluation

Figure 1. Flowchart Illustrating Risk Assessment Methodology

1.4 Foundation for Harmonization of Information Technology Security Standards

Many countries have made significant efforts to develop standards for information technology (IT) security. In the past ten years, the concepts and standards that govern the assessment of security goods have reached a level of maturity in the European Community (EC), United States (US), and Canada (Task, 1993). The widespread prevalence of products in the global market highlights the necessity for a standard that achieves broad acceptance and relevance among vendors in international contexts. Manufacturers face the challenge of the infeasibility of constructing and subjecting items to review systems in several countries, each with their own unique requirements. The main goal of this project is to develop a strategy that promotes the coordination of standards, thus facilitating harmonization (Task, 1993). The United States Department of Defense (DoD) introduced the initial safety assessment standard in the field of information technology, commonly referred to as "TC SEC" or the "Orange Book" (Latham, 1986), in 1983. The primary objective of the development of this standard was to assess the security of operating systems. This program represents a significant endeavor within the field of Information Technology Security. Other examples of evaluation criteria for information technology security are the Information Technology Security Evaluation Criteria (ITSEC) (Gehrke et al., 1992), the Canadian Trusted Computer Product Evaluation Criteria (CTCPEC) (Bacic, 1990), and the Federal Criteria for Information

Technology Security (Rannenberg, 1993). The complete Trusted Computer System Evaluation Criteria (CTCPEC) was developed in April 1992 as a merged framework that combines the Trusted Computer System Evaluation Criteria (TCSEC) and the European Information Technology Security Evaluation Criteria (ITSEC). Its purpose is to provide a complete structure for evaluating information technology (IT) products (Rannenberg, 1993). In addition, the International Organization for Standardization (ISO) introduced ISO/IEC 13335 in 1996, followed by the development of an information system management system centered on risk management in the year 2000 (Gehrke et al., 1992), (Bacic, 1990), (Rannenberg, 1993). The diagram below (Figure 02) depicts the comprehensive framework for the management of information security (Wawrzyniak, 2006).

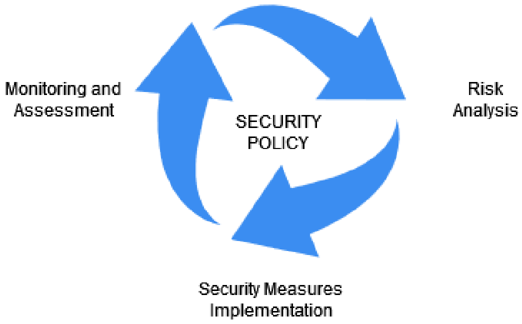

Figure 2. The overall structure for the process of managing information security (Wawrzyniak, 2006)

2. Common Methods of Risk Assessment

The main objective of doing risk assessment is to identify potential threats and consequences faced by information systems, and thereafter develop solutions to address the gap between the system's security level and organizational needs. Nevertheless, it is crucial to recognize that various assessment procedures can result in disparate evaluation results. Hence, the careful incorporation of comprehensive system-specific information is imperative when determining suitable approaches. In a general sense, risk assessment methodologies can be classified into three main categories: those that rely on quantitative analysis, those that are based on qualitative analysis, and those that integrate both quantitative and qualitative elements (Szczepankiewicz et al., 2006). To be more specific, Quantitative and qualitative methods are two primary categories of methodologies that are employed for the examination of risks to which assets within companies are exposed. Table I presents the primary pros and cons associated with IT risk assessment approaches. There exist various categories of IT risk analysis approaches, as outlined by the literature (Szczepankiewicz et al., 2006)

- Quantitative procedures involve the assessment of the amount of risk by employing numerical measurements. In this particular framework, the quantification of asset worth is based on measurable quantities, the measurement of threat frequency is expressed in terms of occurrence instances, and vulnerability is assessed by taking into account the probability of experiencing loss (Rot, 2008). The result of these approaches manifests in the form of measurable indicators. There are other quantitative approaches that can be identified, including Annual Loss Expected, Courtney's method, Fisher's method, and the ISRAM model (Rot, 2008).
- Qualitative methods, in contrast to quantitative approaches, do not depend on numerical data but instead provide outcomes in the form of descriptive narratives and corresponding recommendations. In the context of these methodologies, the process of risk assessment is intricately linked with:
    - The qualitative assessment of asset value, along with the development of qualitative scales indicating the occurrence frequency of threat incidents and the vulnerability linked to a specific threat, or alternatively: - The formulation of threat scenarios by predicting the essential elements that contribute to risk (Szczepankiewicz et al., 2006), (Rot, 2008).

Failure Mode and Effects Analysis/Failure Mode, Effects, and Criticality Analysis (FMEA/FMECA), the Risk Management Framework utilized by the Microsoft Corporate Security Group, the National Institute of Standards and Technology Special Publication 800-30 (NIST SP 800-30), and the Computerized Risk Analysis and Management Methodology (CRAMM) encompass various instances of quantitative methodologies (Rot, 2008).

The selection of risk metrics is contingent upon the magnitude of a particular hazard (Szyjewski, 2004). The metrics encompass a range of evaluations, starting from basic assessments that classify risk into high, medium, or low categories to more accurate measures that calculate the probability of a specific occurrence taking place.

When assessing the inherent risk associated with information security in an Information System, it is customary to do a qualitative analysis. This technique commonly relies on the fundamental principles of information security, specifically confidentiality, integrity, and availability. Each bestowed element can undergo a comprehensive examination of risk on an individual basis. In order to enhance the efficiency of the analysis process, a pre-established scale of information value (low, medium, high) has been implemented. The evaluation of risk magnitude can be demarcated by the utilization of a categorical scale containing designations such as very low, low, medium, high, and very high. A thorough assessment of risk and an understanding of its probability of occurrence are essential for gaining a comprehensive understanding of its impact on the overall operating efficiency of the Information System (Rot, 2008), (Szyjewski, 2004).

Table 1. The Advantages and Disadvantages of Quantitative and Qualitative Approaches in IT Risk Analysis (Rot, 2008)

Risk Analysis	Quantitative methods	Qualitative methods
Selected benefits	● The utilization of quantitative methods enables the determination of the repercussions resulting from incidents, hence facilitating the assessment of costs and benefits when selecting protective measures. ● They provide a more precise representation of the level of risk.	● This feature facilitates the prioritization of risks in a systematic manner. ● This approach enables the identification of high-risk locations quickly and cost-effectively. ● The process of analysis is characterized by its relative ease and affordability.
Selected drawbacks	● The effectiveness of quantitative measures is contingent upon the extent and precision with which the measuring scale is defined. ● The findings of the analysis may lack precision and potentially lead to confusion. ● It is necessary to enhance conventional methodologies by incorporating qualitative descriptions, such as comments and interpretations. ● The utilization of these methodologies in analysis typically incurs more costs, necessitates a higher level of expertise, and requires the use of specialized equipment.	● The method lacks the capability to ascertain probability and outcomes through numerical metrics. ● The process of evaluating costs and benefits becomes more challenging when making decisions on the selection of protective measures. ● The obtained outcomes possess a broad scope and are characterized by their general nature, as well as an approximate quality.

2.1 Methods of Quantitative Assessment

When employing quantitative approaches, analysts are faced with the challenge of accurately evaluating the essential quantities necessary for calculation. The quantification of risk can be expressed through various scales or directly within the financial domain as the projected magnitude of losses associated with a specific type of risk over a defined time period (Szczepankiewicz et al., 2006).

Quantitative risk analysis comprises a wide range of methods and procedures used for evaluation purposes, which include (Volkan Evrin, 2021), ("Risk Assessment and Analysis Methods," ISACA, n.d.):

- Heuristic methods refer to procedures employed to estimate contingency, which are based on either experience or expertise.
- The three-point estimate method involves the utilization of optimistic, likely, and pessimistic values in order to achieve an ideal estimation.
- Decision tree analysis is a visual tool used to illustrate the potential consequences of different choices or alternatives. It provides a diagrammatic picture of the implications associated with each alternative.
- The utilization of monetary evaluation to establish contingency reserves in a project or business process budget is commonly referred to as Expected Monetary Value (EMV).
- The Monte Carlo analysis method involves the utilization of estimated values for different outcomes in order to calculate business costs and project completion deadlines.
- Sensitivity analysis involves the identification of the most influential risks associated with a project.

Fault Tree Analysis (FTA) and Failure Modes and Effects Analysis (FMEA) are two methodologies utilized in engineering and risk management to systematically identify and analyze the various factors that contribute to system failure. These methodologies employ structured diagrams to visually represent the elements responsible for the occurrence of failures within a given system ("Risk Assessment and Analysis Methods," ISACA, n.d.).

Quantitative risk assessment encompasses essential variables, such as Single Loss Expectancy (SLE), which denotes the anticipated loss resulting from a singular occurrence. The Annual Rate of Occurrence (ARO) denotes the frequency at which the incident is anticipated to transpire during a one-year time frame. The integration of System Loss Expectancy (SLE) and Annual Rate of Occurrence (ARO) results in the derivation of the Annual Loss Expectancy (ALE), which serves as a basis for determining the economic feasibility of countermeasure investments. The Asset Loss Expectancy (ALE) can be calculated by multiplying the Single Loss Expectancy (SLE) by the Annual Rate of Occurrence (ARO). The aforementioned value functions as the resultant of risk assessment in quantitative analysis (Volkan Evrin, 2021).

The availability of trustworthy data is crucial for the accurate and effective execution of the IT risk assessment process, but it is uncommon for the team responsible for this activity to have access to such data. Furthermore, accurately measuring the extent of losses pertaining to individual and organizational assets might pose challenges. One of the primary focal points revolves around the potential vulnerability of sensitive data. The establishment of value requires a clear and precise demarcation of information, which is crucial for the effective implementation of various business activities. Moreover, it is of utmost importance to understand the value of information in maintaining the operational integrity of different segments within an organization, which in turn has implications for the overall enterprise. The underlying correlation employed in IT risk assessment is delineated as follows (Szczepankiewicz et al., 2006), (Galach, 2004).

$$\mathbf{R = P \times W \text{ and } P = F \times V}$$

In this context, the variables are denoted as follows: R represents the risk value, P represents the probability or expected number of incidents that may occur, resulting in the loss of assets value within a specified time period. W refers to the value of loss, which represents the anticipated decrease in the value of assets resulting from a single incident. F, on the other hand, denotes the frequency at which threats are expected to occur. The susceptibility of an information system, or its individual elements, to a danger, refers to the likelihood that a certain vulnerability would be exploited by that threat. The justification for this rests in the understanding that the evaluation of IT risk is typically expressed through the anticipated value of a loss, a metric derived from the description of three essential variables (Szczepankiewicz et al., 2006). The quantification of resources, which includes crucial factors such as knowledge necessary for efficient organizational operation, is attributed with value. The quantification of possible threats targeting resources, such as processed information, is determined by calculating the frequency of their occurrences within a specified timeframe. The usual practice is to establish a one-year duration for the purpose of determining frequency. The quantification of the susceptibility of an information technology (IT) system or its individual components to threats is achieved by an evaluation of the probability of experiencing losses as a result of prospective occurrences (Rot, 2008). The ALE model (Annual Loss Expected) is widely recognized as the prevailing and commonly utilized quantitative approach for risk assessment. The underlying idea of this model is based on the concept of expected loss, which is determined by multiplying the probability of bad occurrences impacting information technology (IT) systems with the monetary losses associated with these events. The subsequent models offer comprehensive information regarding this method (Rot, 2008), (Wawrzyniak, 2007), (Szczepankiewicz et al., 2006).

ALE = (Probability of event) x (value of loss)

$$ALE = \sum_{i=1}^{n} I(O_i)F_i$$

Here, let $\{O_1, O_2, ..., O_n\}$ represent the collection of negative effects coming from an event. The value of $I(O_i)$ denotes the loss indicated by the event. The variable F_i represents the frequency of the event i.

The calculation of annual predicted losses in companies is based on the summation of anticipated yearly losses, which serves as a fundamental basis. A variety of alternative approaches for the assessment and evaluation of IT risk arise from the aforementioned methodology. These adjustments are tailored to address specific needs and conditions that are inherent to a given organizational context. One strategy that deserves consideration is Courtney's method, which was formulated by Robert Courtney. Similar to the ALE (Annualized Loss Expectancy) methodology, this method assesses potential losses by calculating the product of the value of losses associated with a hazard and an indicator that measures the likelihood of its happening. Courtney asserts that the crux of risk assessment relies on the utilization of the following formula (Rot, 2008), (Ryba et al., 2009).

$$\mathbf{R = P \times C}$$

R represents the risk value. The variable P represents the probability of the occurrence of a specific number of times throughout a year, pertaining to an event that results in a loss for the organization. The term "C-loss" refers to the financial loss experienced by an organization as a direct consequence of a singular incident that leads to such loss.

$$\boldsymbol{ALE = \frac{10^{f+i-3}}{3}}$$

The variable "f" represents an index that quantifies the assessed frequency of the event that leads to a loss. The index is used to determine the extent of loss resulting from the occurrence of an event (Rot, 2008).

Courtney's method presents a comprehensive framework consisting of six primary vulnerability types. These categories comprise accidental data disclosure, unintended data modification, inadvertent data deletion, intentional data disclosure, deliberate data change, and deliberate data removal. The approach in question has been officially acknowledged by national bodies in the United States as a recognized method for performing risk assessments (Ryba et al., 2009).

Fisher's method, which builds upon Courtney's approach, functions as a complete framework for the development of security solutions in the field of Information Systems. The presence of a well-established information security policy within the company is essential for the efficient application of this concept. This methodology comprises various stages within the process of managing risk in Information Systems (Ryba et al., 2009), (Rot, 2008).

- Phase 1 of the research process entails the systematic collection of data. This phase involves identifying and categorizing the various resources inside Information Systems. Once these resources have been identified, relevant information about them is gathered. This information will then be subjected to additional analysis in later phases (Rot, 2008).
- Phase 2 of the study involves the process of identifying threats. This entails the mapping of the six threat categories indicated in Courtney's technique onto eleven Fisher control points. These points comprise several acts including the gathering, transmission, transformation of form, transit, reception, processing, migration, removal, and utilization of data (Rot, 2008).
- Phase 3 of the project involves conducting a risk assessment. This assessment aims to evaluate the level of risk using Courtney's method formula, which is represented by the equation R = P × C. In this equation, P represents the probability of an event causing loss occurring a specific number of times per year, while C represents the loss incurred by the organization as a result of a single occurrence of the event causing loss (Rot, 2008).
- Phase 4 of the project entails the design of control mechanisms, wherein the task at hand involves the careful selection of appropriate control mechanisms for each risk that has been identified. The strategies under consideration encompass preventive, detective, and remedial aspects (Rot, 2008).
- Phase 5 - Economic Viability The evaluation of mechanisms entails doing a comprehensive business assessment of the identified mechanisms. This assessment involves the utilization of the Return on Investment (ROI) indicator, which was previously described, and is expressed through a specific formula (Rot, 2008).

ROI = Operational profit in a given period ÷ value of invested capital

This approach considers the operational gain as the representation of the degree of risk for certain control mechanisms, while the measure of invested capital is viewed as the evaluated cost of these mechanisms (Ryba et al., 2009). The ISRAM model (Information Security Risk Analysis Method) is presented as the subsequent approach in the paper. The foundation of this model is based on the ALE (Annual Loss Expected) approach, which predominantly utilizes survey research as its primary methodology. The assessment of risk in information technology is achieved by employing the following formula (Wawrzyniak, 2007), (Karabacak et al., 2005).

$$RISK = \left(\frac{\sum_m T_1(\sum_i w_i p_i)}{m}\right)\left(\frac{\sum_m T_2(\sum_j w_j p_j)}{n}\right)$$

Here, the variable "i" denotes the number of survey questions pertaining to the assessment of the probability of incident occurrences. The variable "j" represents the quantity of survey questions that pertain to assessing the effects. The variables "m" and "n" represent the number of participants involved in the survey. The weights assigned to questions "i" and "j" are denoted as wi and wj, respectively. The variables pi and pj are used to denote the values that correspond to the selected responses for "i" and "j" respectively. T1 represents the tabulated probability associated with the occurrence of specific events. The term "T2" refers to a table that encompasses the unfavorable consequences that result from the occurrence of events. The Courtney's approach, which is commonly employed in risk assessment, has been reconstructed through the utilization of the Exposure Analysis Matrix. The foundation of this approach is the underlying notion that the magnitude of risks is contingent upon the number of individuals capable of causing harm, hence necessitating a risk analysis that involves the categorization of specific occupational cohorts inside the organization. Parker's approach incorporates Courtney's method but expands upon it by incorporating qualitative analysis of risk. Additionally, Parker's method formalizes the assessment of the impact of human factors on risk, setting it apart from other methods (Szyjewski, 2004).

2.2 Methods of Qualitative Assessment

The main purpose of qualitative risk analysis is to identify risks that require thorough consideration, and to develop appropriate controls and actions based on the implications and impact of the risks on objectives (Behnia et al., 2012). In the realm of qualitative risk analysis, there exist two well acknowledged and easily implementable approaches for risk appraisal (Kuzminykh et al., 2021). The Keep It Super Simple (KISS) approach is well-suited for projects that have a narrow focus or restricted magnitude. Its purpose is to minimize needless complexities and facilitate uncomplicated review by teams with limited experience in risk assessment. This particular methodology involves assessing risks using a fundamental scale, commonly classified as very high, high, medium, low, and very low ("Risk Assessment and Analysis Methods," ISACA, n.d.), (Kuzminykh et al., 2021). The utilization of this approach is more appropriate for complex and substantial challenges, as well as for teams who possess expertise in risk assessment. The methodology employed in this study involves the assessment of both the probability of risk occurrence and the subsequent consequences or impacts. Probability is a measure that measures the likelihood of a risk being realized, whereas impact pertains to the potential consequences that can affect several aspects, including time, cost, scope, and quality. The assessment of probability and impact is conducted using a predetermined scale, such as a range of 1 to 10 or 1 to 5. The risk score is then derived by multiplying these two evaluations (Behnia et al., 2012), ("Risk Assessment and Analysis Methods," ISACA, n.d.). Qualitative risk analysis is a widely applicable approach that may be utilized to effectively identify risk areas associated with regular business operations across different industries. This methodology evaluates the extent to which employees' concerns over their job are consistent with the identified risk domains. The utilization of the quantitative technique is employed in tandem to investigate relevant risk scenarios, hence providing detailed insights for making well-informed decisions ("Risk Assessment and Analysis Methods," ISACA, n.d.). Quantitative risk analysis provides enhanced objectivity and exact facts in the context of crucial decision-making or complex activities, as opposed to its qualitative equivalent. However, it is crucial to recognize that quantitative analysis is still susceptible to estimation or inference, leading prudent risk managers to take into account supplementary considerations during the decision-making procedure (Kuzminykh et al., 2021). Although qualitative risk analysis is commonly favored for its simplicity in execution, there may be situations that need the utilization of a quantitative approach. Following the completion of qualitative research, the subsequent step involves doing quantitative analysis. However, in cases where qualitative analysis provides sufficient insights, it may not be necessary to perform a quantitative analysis for every individual risk ("Risk Assessment and Analysis Methods," ISACA, n.d.), (Kuzminykh et al., 2021), (Peixoto et al., 2022).

There are several qualitative procedures that can be utilized for risk analysis. This discourse will focus on three specific methods: FMEA/FMECA methodologies, NIST 800-30, and CRAMM methodologies. The origins of FMEA (Failure Mode and Effects Analysis) and FMECA (Failure Mode and Effects Criticality Analysis) may be traced back to the 1950s, during which they were developed for the purpose of evaluating the reliability of weaponry. These methods are still utilized, particularly in sectors such as aviation, space exploration, and electronics (Bialas, 2006). The FMEA/FMECA process essentially entails a thorough examination of the potential consequences of each fault on the overall functionality of the system, as well as the classification of probable flaws based on their severity levels. The FMECA methodology enhances the analysis by evaluating the severity of defects and their possible impact on the system's functionality. Although these methods have proven to be effective, they require a significant amount of manual effort and skill from practitioners. Additionally, specialized tools that integrate parts of knowledge engineering and fuzzy logic are necessary for their implementation (Bialas, 2006). The NIST SP 800-30 methodology outlines a comprehensive framework for conducting IT risk assessment, which encompasses nine fundamental phases (Stoneburner et al., 2002), (Ryba et al., 2009).

a) **Selection of Evaluated Systems:** The task at hand involves the identification of the systems that are subject to assessment.

b) **Scope Definition and Information Collection:** The process of delineating the parameters of evaluation and collecting the requisite data.

c) **Threat Identification:** Identifying potential risks associated with the assessed systems.

d) **Susceptibility Identification:** The task at hand involves the identification of vulnerabilities inside the systems that have been analyzed.

e) **Analysis of Control and Protection Mechanisms:** This study aims to assess the existing or proposed systems of control and protection.

f) **Determination of Susceptibility Probabilities:** The probabilities of susceptibility incidence can be specified by identifying threat sources and assigning likelihood levels categorized as low, medium, or high.

g) **Analysis of Incident Impact:** This study aims to conduct an analysis and assessment of the effects of incidents on the system, data, and organization. These incidents will be grouped into three levels: high, medium, and low.

h) **Risk Level Determination:** The Risk Level Matrix is utilized to determine risk levels by multiplying the probabilities of incident occurrence, which are assigned weights of 1.0 for high, 0.5 for medium, and 0.1 for low, with the corresponding impact strengths of incidents, which are assigned weights of 100 for high, 50 for medium, and 10 for low. The matrix presented below serves to determine the comprehensive level of risk associated with each identified danger, which is classified into three categories: high (with a product range of (50,100]), medium (with a product range of (10,50]), or low (with a product range of [1,10]).

i) **Elaboration of Control and Protection Recommendations:** The objective of this study is to propose control methods and alternative alternatives that can effectively mitigate risks to an acceptable level.

The CRAMM technique, known as the CCTA's Risk Analysis and Management technique, has been officially recognized by the CCTA (UK Government Central Computer and Telecommunications Agency) as a standard for risk analysis and management. This methodology is structured around a three-stage procedure (Ryba et al., 2009).

a) **Resource Identification and Evaluation:** The process of identifying and evaluating resources.

b) **Threat and Susceptibility Evaluation:** Evaluating potential risks and weaknesses.

c) **Control and Protection Mechanism Selection and Recommendation:** The process of selecting and recommending control and protection systems.

The objective of IT risk analysis is to assess the probability of occurrences that may disturb the optimal operation of resources. The process entails the classification of identified resources into distinct asset groups, followed by the creation of inventories of significant threats associated with each asset group. This ultimately leads to the assessment of the risk level for each group, utilizing a five-level scale.

The aforementioned approach incorporates specialized software as an essential component that facilitates the aforementioned processes (Rot, 2008).

2.3 Combination of Quantitative and Qualitative Evaluation

The key advantages of quantitative risk assessment stem from its utilization of empirical and measurable data. This approach enables the provision of accurate outcomes pertaining to risk appraisal and the determination of the optimal investment necessary for effective risk treatment, hence ensuring the profitability of the company ("Risk Assessment and Analysis Methods," ISACA, n.d.). One instance of a quantitative methodology employed for doing cost-benefit analysis is the Annual Loss Expected (ALE) calculation. This approach assists companies in assessing the projected financial loss linked to a particular asset or investment, as a result of associated risks, within a span of one year ("Risk Assessment and Analysis Methods," ISACA, n.d.).

The determination of Annualized Loss Expectancy (ALE) for an investment in a virtualized system encompasses the subsequent procedures ("Risk Assessment and Analysis Methods," ISACA, n.d.):

The monetary worth of the virtualization system's hardware is estimated to be $1 million, as determined by the Single Loss Expectancy (SLE) for hardware ("Risk Assessment and Analysis Methods," ISACA, n.d.).

The estimated monetary worth of virtualized system management software is $250,000, as determined by the

Single Loss Expectancy (SLE) for software ("Risk Assessment and Analysis Methods," ISACA, n.d.).

According to the vendor data, there is an occurrence of system catastrophic failure, caused by either software or hardware issues, once per 10 years, resulting in an Annual Rate of Occurrence (ARO) of 0.1 ("Risk Assessment and Analysis Methods," ISACA, n.d.).

The annualized loss expectancy (ALE) for the homework assignment is calculated by multiplying the asset value of $1 million by the annualized rate of occurrence (ARO) of 0.1, resulting in an ALE of $100,000 ("Risk Assessment and Analysis Methods," ISACA, n.d.).

The annual license expense (ALE) for software (SW) can be calculated by multiplying the initial cost of $250,000 by the annual maintenance fee rate of 0.1, resulting in an ALE of $25,000 ("Risk Assessment and Analysis Methods," ISACA, n.d.).

In the given context, the organization is confronted with a recurring risk of incurring a financial loss up to $100,000 per annum due to hardware failure, and a loss of $25,000 per annum due to software failure in the event of virtualization system malfunction. Any control mechanism that is applied, such as backup systems, disaster recovery plans, or fault tolerance systems, which incurs costs lower than the specified amounts, would result in a profitable outcome ("Risk Assessment and Analysis Methods," ISACA, n.d.).

Some risk evaluations require the consideration of complex parameters. Further illustrations can be obtained by employing the subsequent "sequential deconstruction of quantitative risk analysis" ("Risk Assessment and Analysis Methods," ISACA, n.d.).

- Perform a comprehensive evaluation of potential hazards and weaknesses to ascertain relevant factors of risk. Determine the Exposure Factor (EF), which is the percentage of asset loss attributed to the identified threat. The Single Loss Expectancy (SLE) can be calculated by taking into account the risk variables and the values of the assets that are at risk. The SLE is obtained by multiplying the value of the asset by the Exposure Factor (EF). When considering adjustments, it is important to consider historical records of incidents and the prevalent institutional culture as influential elements.
- Estimate the Annual Rate of Occurrence (ARO) associated with each risk determinant. Determine the necessary steps to mitigate each risk factor. Utilize a numerical scale spanning from 1 to 10 in order to quantitatively assess the level of severity, where a rating of 10 represents the highest degree of severity. This scale functions as a corrective factor for evaluating risk, taking into account the company's specific risk profile.
- Determine the Annualized Loss Expectancy (ALE) associated with each risk factor. It is imperative to acknowledge that, despite the implementation of countermeasures, the Annual Rate of Occurrence (ARO) that contributes to the Annual Loss Expectancy (ALE) may not be completely eliminated in every case. The computation of the adjusted Annual Loss Expectancy (ALE) involves multiplying the ALE, as indicated in the table, by the adjustment factor and then by the size correction factor.
- Perform a thorough assessment of the expenses and advantages by conducting a comparative analysis of the Annual Loss Expectancy (ALE) before and after the installation of countermeasures. The Internal Rate of Return (IRR) can be employed as a foundational metric for computing the Return on Investment (ROI) within the context of a cost/benefit analysis methodology.
- In conclusion, it is imperative to concisely summarize the results in order to facilitate the assessment of performance by management.

The utilization of combined approaches has the potential to optimize process efficiency and facilitate the achievement of required security levels. When it comes to the risk assessment process, the decision between quantitative and qualitative methodologies may often be made with reasonable ease. The execution of qualitative risk assessment is expeditious since it does not heavily rely on mathematical calculations or measurements, hence facilitating its straightforward implementation. Organizations derive advantages from the presence of seasoned personnel who possess knowledge of assets and processes. However, it is crucial to acknowledge the inherent biases that may arise when evaluating the likelihood and consequences of certain events (Rot, 2008). In general, a balanced integration of qualitative and quantitative research methods, along by thorough preparation of assessment procedures and suitable modeling techniques, may be the most advantageous approach for a successful risk assessment procedure (Rot, 2008), ("Risk Assessment and Analysis Methods," ISACA, n.d.).

3. Analysis and Design of Risk Assessment

The Information Security Management System (ISMS) is a comprehensive framework consisting of a set of well-defined policies designed to effectively manage information security and address IT-related risks (Cranor et al., 2005). The aforementioned methodology has increasingly garnered attention as a highly efficient strategy for tackling intricate issues within the field of information security, thus garnering broader recognition and approval on an international level. The effectiveness and functioning of this system are inherently dependent on the careful implementation of the risk assessment phase, which is a crucial step in its formation and smooth operation. It is crucial to highlight that the domain of ISMS functions within a context marked by dynamic aspects, and these constituents inject a certain degree of unpredictability into the equation (Abbas et al., 2011).

One notable element concerns the dynamic nature of security requirements inside an organization. The aforementioned requirements are subject to change as a result of the inherent obsolescence of current security methods and the need to address developing vulnerabilities. The rapid advancements in technology have given rise to a set of vulnerabilities that businesses must actively confront, marking the onset of a new era of problems (Abbas et al., 2011).

The second dynamic component underscores the potential for the implementation of an Information Security Management System (ISMS) to result in unanticipated external effects that impact other interconnected systems. The prediction of these externalities is inherently unpredictable and difficult to ascertain in advance. The complex interaction among different systems might give rise to cascading consequences that may only manifest themselves once the Information Security Management System (ISMS) has been implemented and is actively engaging with its surrounding environment (Abbas et al., 2011).

The evaluative procedures for security issues included within Information Security Management Systems (ISMS) are important to the concept of the third dimension. The aforementioned mechanisms are intrinsically interconnected with the technical environment of their respective era. As technological advancements progress, novel risks and susceptibilities arise, hence rendering the assessment standards employed in Information Security Management Systems (ISMS) outdated. This highlights the importance of employing a flexible strategy that can adjust to the changing landscape of threats, guaranteeing the resilience and efficacy of the Information Security Management System (ISMS) in the presence of continuously increasing difficulties (Abbas et al., 2011).

In light of the aforementioned context, the incorporation of a perpetual security assessment mechanism within the Information Security Management System (ISMS) emerges as not merely a choice, but a vital necessity. The mechanism, deeply embedded in the organizational structure, functions as a dynamic feedback loop that consistently assesses the effectiveness and pertinence of the Information Security Management System (ISMS). The implementation of this measure guarantees the maintenance of a resilient and flexible system, which is capable of effectively addressing emerging threats and vulnerabilities. As a result, it significantly contributes to the attainment of the overall objectives related to information security (Cranor et al., 2005). In an environment marked by swift technological progress and ever-changing risk elements, the implementation of a proactive and flexible security evaluation framework is crucial for maintaining the integrity and efficacy of an Information Security Management System (ISMS) (Cranor et al., 2005), (Abbas et al., 2011).

3.1 Information Security Standards

Within the field of information security, a multitude of standards have been developed. The integration of security standards within corporations and enterprises not only boosts the efficacy of security measures but also optimizes their development process. In order to achieve a collective agreement regarding the extent of safeguarding offered by these standards, it is imperative to incorporate security measures in a systematic fashion. The following is a comprehensive review of the primary standards (Asosheh et al., 2013):

The ISO/IEC 27000-series comprises a collection of information security standards that are collaboratively issued by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). At now, this series encompasses a total of eleven well-established standards, while more standards are still in the developmental process. The primary criteria in this series are:

- ISO 13335, also known as ISO/IEC 13335, is a standard named "Information technology — Security techniques — Management of information and communications technology security." This standard is divided into two portions. The ISO 27005 standard has superseded specific portions of the old ISO 13335 standard.
- ISO 17799, often referred to as BS7799, offers a complete examination of security considerations. The subject matter involves a set of control criteria that are especially complex.

- ISO 27001 is a standard that delineates the necessary elements for establishing, executing, overseeing, evaluating, sustaining, and improving an Information Security Management System. The standard is based on a methodology that emphasizes the importance of process-oriented practices.
- ISO 27002 provides a set of control objectives and best practice procedures that can be selected and implemented to mitigate risks and achieve information security objectives. This standard includes 11 clauses that consist of a total of 39 primary security categories and 133 individual controls.
- ISO 27003 provides practical recommendations for the deployment of Information Security Management Systems (ISMS) in accordance with ISO/IEC 27001.
- ISO 27004 offers guidance on the development and implementation of metrics for assessing the efficiency of Information Security Management Systems (ISMS), control goals, and controls specified in ISO/IEC 27001.
- ISO 27005 provides guidelines for the effective management of risks associated with information security.
- ISO 27006 provides a comprehensive framework that outlines the necessary criteria and offers guidance for entities involved in the auditing process.
- ISO 27007 provides guidance on the implementation of audits for Information Security Management Systems (ISMS) and outlines the necessary skills and qualifications for ISMS auditors.
- ISO 27008 provides recommendations pertaining to the evaluation and execution of controls in order to assess their implementation and operational effectiveness.
- There are further standards that are part of the ISO27k series. The ISO27k series encompasses standards 27000–27019 and 27030–27044, which jointly provide a range of security management characteristics that are in line with the requirements of ISO 27001.

The BS7799 Security Standard was initially developed by the British Standards Institution (BSI). The 1995 version, together with its succeeding iterations in 1999 and 2000, are widely acknowledged and referred to as BS Version 1, BS Version 2, and BS Version 3, respectively (Broderick, 2006).

The Payment Card Industry Data Security Standard (PCIDSS) is an internationally recognized information security standard developed by the Payment Card Industry Security Standards Council. Its purpose is to assist enterprises involved in card payment processing in their efforts to prevent credit card fraud. This applies to all organizations that are responsible for managing cardholder information associated with card brands that display the corresponding logos (Susanto12 et al., 2011).

The Information Technology Infrastructure Library (ITIL) emerged in the 1980s as a direct response to the insufficient quality of IT service. ITIL comprises a comprehensive framework of principles and practices that pertain to the management of Information Technology Services (ITSM), including aspects connected to security. The primary objective of ITIL is the management of IT services, with an emphasis on the viewpoint of service providers (Tofan, 2011).

COBIT, which stands for Control Objectives for Information and Related Technology, presents a structured approach for addressing and managing the risks associated with information technology inside business operations. COBIT, developed by the IT Governance Institute (ITGI) under the auspices of the Information Systems Audit and Control Association (ISACA), serves as a framework for governing and managing IT to ensure its alignment with business objectives (Broderick, 2006).

Finally, the origins of the Government Access to Secure Systems Program (GASSP) can be traced back to the year 1992, with its establishment being supported by the support of the United States government, the Information Security Institute, and several other institutions. Following a series of developmental stages, the framework was designated as the 'Generally Accepted System Security Principles' (GAISP) and later transformed into the 'Generally Accepted Information Security Principles' (GAISP) to align with the expanding range of its objectives. The establishment of GASSP received support from a wide range of stakeholders, and the resulting document encompasses a comprehensive structure. The GAISP iteration is a crucial reference material that provides developers with direction based on concepts supported by respected organizations such as the OECD and ISF. It can be likened to a comprehensive cookbook, with detailed instructions and recommendations (Siponen & Willison, 2009), (Asosheh et al., 2013).

4. The Significance of Artificial Intelligence in Information Security (INFOSEC)

The preservation of information and system security is a significant challenge in the digital communication landscape. The inherent significance of information highlights the crucial need to guarantee data security in communication systems. The utilisation of inherent properties of artificial neural networks, such as their adaptive learning capabilities, can facilitate the possibility for security advancements (Karapilafis, 2015). Moreover, artificial intelligence (AI) functions across multiple modalities, including learning, comprehension, and decision-making. The evolution of AI is apparent in the development of autonomous intelligence, as demonstrated by the breakthroughs made in the field of self-driving vehicles. Prominent business companies such as Google, IBM, Juniper Networks, and Balbix have utilised artificial intelligence (AI) in the field of information security. Google utilises artificial intelligence (AI) to enhance the performance of Gmail, while IBM applies AI to identify potential attacks. Additionally, Balbix's Breach Control Platform harnesses AI to proactively anticipate and mitigate potential hazards. By efficiently integrating artificial intelligence (AI) with security measures, a more robust cybersecurity posture is established, leading to the successful mitigation of many threats, including ransomware. The combination of AI capabilities with security requirements is a significant shift, marking the beginning of a new age in digital defence ("Artificial Intelligence and its Application," Onyango).

4.1 Methodological Approaches for Integrating Artificial Intelligence into INFOSEC

Artificial Intelligence (AI) is a distinct field of study within the discipline of computer science that focuses on the development of computer systems possessing sophisticated cognitive ability to perform a wide range of activities. The area of information security management can be categorised into three distinct classifications: Artificial Narrow Intelligence (ANI), Artificial General Intelligence (AGI), and Artificial Super Intelligence (ASI) ("Artificial Intelligence and its Application," Onyango).

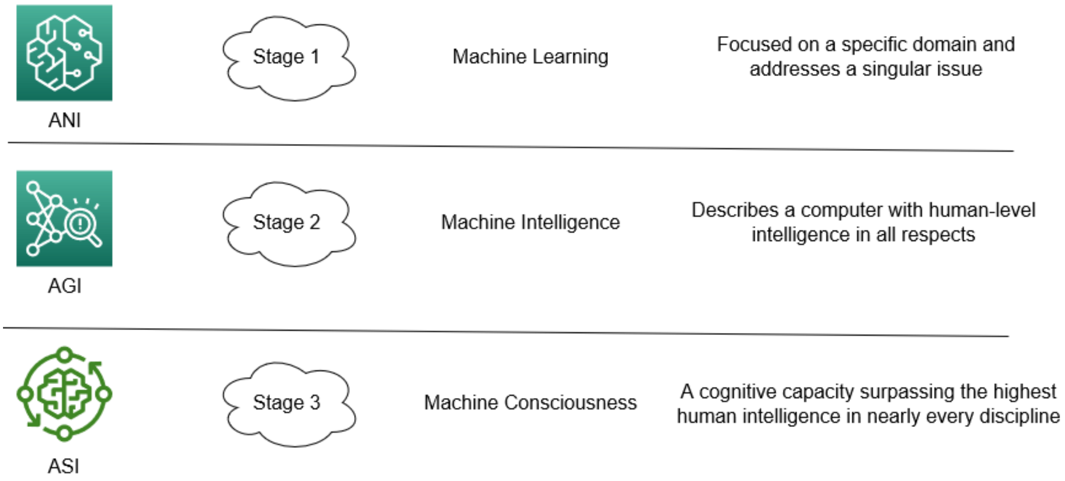
ANI
Stage 1
Machine Learning
Focused on a specific domain and addresses a singular issue
AGI
Stage 2
Machine Intelligence
Describes a computer with human-level intelligence in all respects
ASI
Stage 3
Machine Consciousness
A cognitive capacity surpassing the highest human intelligence in nearly every discipline

Figure 3. Artificial Intelligence across its three classifications (Granata, 2023)

Artificial Narrow Intelligence (ANI) demonstrates a high level of competence in narrow activities within the field of artificial intelligence ("Artificial Intelligence and its Application," Onyango). It is particularly good in managing information, as seen in its application in tasks such as retrieving smartphone data through virtual assistants. In contrast, Artificial General Intelligence (AGI) encompasses a wide range of reasoning capabilities and flexibility, similar to the cognitive capacities observed in humans ("Artificial Intelligence and its Application," Onyango), (Tolani & Tolani, 2019). This is exemplified by healthcare-focused robots such as pillo. In the realm of artificial intelligence, Artificial Superintelligence (ASI) represents the pinnacle of AI effectiveness, surpassing human cognitive abilities by actively engaging with intricate concepts, accurately predicting errors, and devising solutions. This is exemplified by the multifaceted humanoid robot "Alpha 2," which contributes to enhancing information security and fortifying system resilience ("Artificial Intelligence and its Application," Onyango), (Tolani & Tolani, 2019), (Sundu & Ozdemir, 2020).

4.2 Security Risks in the Realm of Artificial Intelligence (AI)

Cyberattacks can be classified into discrete areas, including integrity, confidentiality, authenticity, and non-repudiation considerations. Based on the aforementioned concerns, it is apparent that AI security risks might arise in three basic aspects. Such as, ("Artificial Intelligence and its Application," Onyango).

- Within the realm of cybersecurity, espionage refers to the act of obtaining intelligence related to a specific target's information system. This serves as a preliminary step before executing complex cyberattacks. An entity with antagonistic intentions possesses the capability to utilize approaches driven by artificial intelligence in order to thoroughly examine an information management system, consequently deriving detailed insights by leveraging inherent properties such as datasheets ("Artificial Intelligence and its Application," Onyango).
- Sabotage refers to the intentional obstruction of an artificial intelligence (AI) system's ability to function effectively. This can be achieved by manipulating the system's models or overwhelming it with demands that beyond its processing capacity ("Artificial Intelligence and its Application," Onyango).
- Similarly, fraud entails the purposeful manipulation of roles through the misclassification and contamination of data, including the deliberate insertion of fabricated data or orchestrated interactions during system training in order to exert influence on decision-making processes ("Artificial Intelligence and its Application," Onyango).

The harmful application of artificial intelligence (AI) poses a complex set of difficulties to the field of information security, which can be categorized into three main areas: digital threats, physical threats, and political threats ("Artificial Intelligence and its Application," Onyango).

4.2.1 Digital Security

Threats can manifest through the manipulation of individuals within a social context, a phenomenon commonly referred to as social engineering. These threats can be categorized and visualized in the accompanying diagram ("Artificial Intelligence and its Application," Onyango).

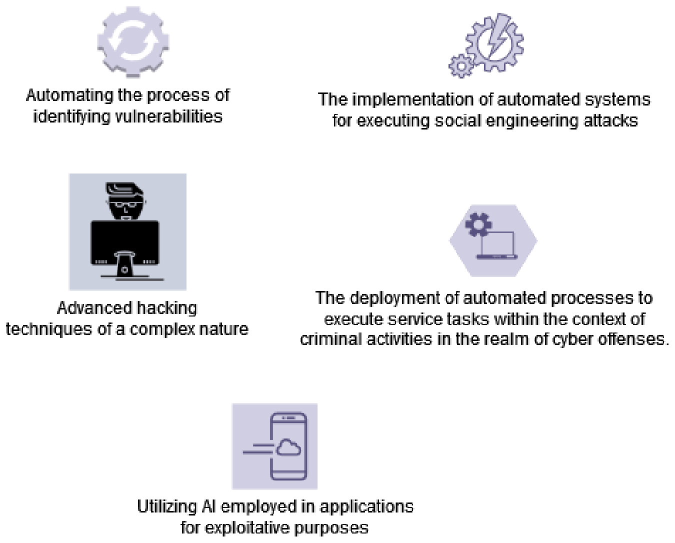
Automating the process of identifying vulnerabilities
The implementation of automated systems for executing social engineering attacks
Advanced hacking techniques of a complex nature
The deployment of automated processes to execute service tasks within the context of criminal activities in the realm of cyber offenses.
Utilizing AI employed in applications for exploitative purposes

Figure 4. Digital Security ("Artificial Intelligence and its Application," Onyango)

Automated social engineering attacks encompass the utilisation of Natural Language Processing (NLP) to emulate the writing style of a certain target, hence enabling AI systems to collect online data pertaining to the subject and afterwards generate malevolent content, such as detrimental links, emails, and webpages ("Artificial Intelligence and its Application," Onyango). The process of identifying system vulnerabilities using artificial intelligence (AI) is dependent on the analysis of past trends in order to detect potential holes that can be exploited by malicious actors in a covert manner ("Artificial Intelligence and its Application," Onyango). Artificial intelligence (AI) has the potential to enhance the efficiency of hacking activities by employing a prioritisation system that focuses on selecting target victims according to their specific vulnerabilities. Moreover, artificial intelligence has the capability to automate operations that cause disruptions in the flow of data, namely in the realm of cybercrimes, such as payment processing. In the field of information security, the utilisation of data poisoning is employed as a means to establish backdoors or breach the security protocols that are integral to artificial intelligence (AI) systems ("Artificial Intelligence and its Application," Onyango).

4.2.2 Physical Security

Security threats can manifest via compromising the physical integrity of a machine, for as through the utilisation of weaponized hard drives ("Artificial Intelligence and its Application," Onyango).

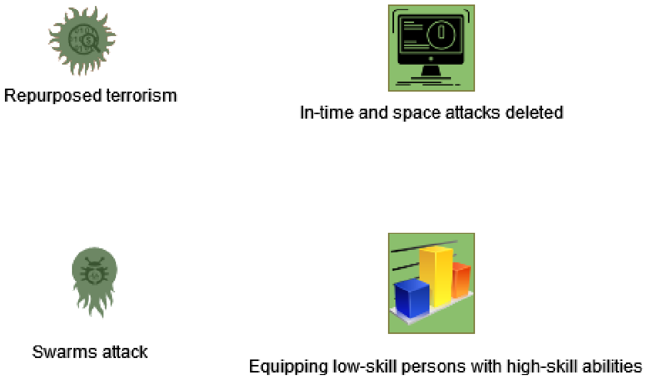
Repurposed terrorism
In-time and space attacks deleted
Swarms attack
Equipping low-skill persons with high-skill abilities

Figure 5. Physical Security ("Artificial Intelligence and its Application," Onyango)

Terrorist repurposing refers to the unauthorised utilisation of commercially available artificial intelligence (AI) devices, such as drones, with the intention of undermining the security of individuals or organisations, hence constituting a possible threat to data storage facilities. The integration of wireless and remote communication functionalities in artificial intelligence (AI) systems facilitates the persistent and automatic targeting of data centres. Furthermore, the use of distributed networks in the field of artificial intelligence (AI) results in the development of autonomous robotic systems that possess the ability to carry out highly coordinated attacks on a significant magnitude. Moreover, artificial intelligence (AI) grants malicious actors with advanced proficiencies, presenting different avenues for carrying out assaults by optimising algorithms, navigating systems, and detecting weaknesses ("Artificial Intelligence and its Application," Onyango).

4.2.3 Political Security

Threats possess a significant impact on society by manifesting itself in various forms, such as profiling, surveillance, and the utilisation of automated disinformation operations ("Artificial Intelligence and its Application," Onyango). AI generates photos and movies with provocative material that is hard to check, enabling fake news.

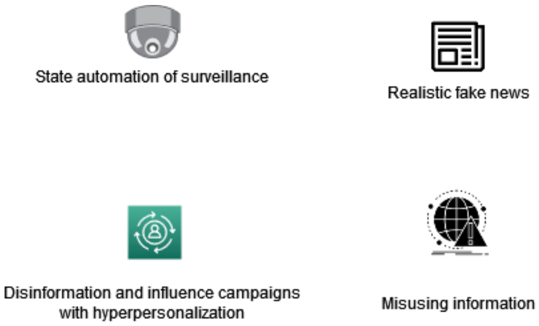
State automation of surveillance
Realistic fake news
Disinformation and influence campaigns with hyperpersonalization
Misusing information

Figure 6. Political Security [33]

Furthermore, AI allows governments to collect and exploit data from individuals and organisations without consent. Third, social network AI recognises harmful influencers that spread personalised falsehoods. Finally, AI's sophisticated algorithms alter data to affect user behaviour, as shown in bot-driven denial-of-information attacks that flood information channels and render data inaccurate ("Artificial Intelligence and its Application," Onyango).

4.3 Benefits and Areas of AI Appliactions in Infosec Management

Artificial Intelligence (AI) assumes a diverse position in augmenting cybersecurity practises. Firstly, it facilitates the development of complete inventories of IT assets, providing accurate insights on the utilisation of users, devices, and applications inside information systems, hence streamlining inventory management (Fozilovich, 2022). Additionally, artificial intelligence (AI)-powered solutions provide timely and up-to-date data about worldwide and organization-specific risks, allowing organisations to efficiently determine the order of importance for implementing security measures. Furthermore, artificial intelligence (AI) plays a crucial role in the assessment of security tools and procedures, contributing to the maintenance of a robust security posture via the identification of vulnerabilities. In addition, artificial intelligence (AI) has the capability to forecast prospective breaches, therefore assisting organisations in the proactive deployment of resources to avoid or mitigate vulnerabilities. In addition, artificial intelligence (AI) technologies play a crucial role in expediting and providing comprehensive responses to security events by effectively detecting underlying causes and implementing measures to avoid future occurrences. Finally, artificial intelligence (AI) plays a crucial role in improving the comprehensibility of cybersecurity systems, facilitating the effective communication of studies and suggestions to diverse parties engaged in the oversight and protection of data. Artificial intelligence (AI) plays a crucial role in enhancing the cyber resilience and security protocols used by organisations ("Artificial Intelligence and its Application," Onyango).

4.4 Summary of AI's Role in Information Security

The efficacy of conventional security procedures in protecting information systems from cyber assaults has shown a growing susceptibility. The prevalence of hackers successfully circumventing security firewalls has grown more frequent, hence highlighting the need for a more sophisticated and strategic approach to the field of cybersecurity (Tolani & Tolani, 2019). Artificial Intelligence (AI) presents a diverse array of efficacious security solutions capable of detecting atypical behaviours inside data management systems. By using machine learning techniques, AI can discern data abnormalities and forecast possible security threats (Everitt et al., 2017). Artificial intelligence (AI) solutions provide the capability to effectively identify and isolate tainted data, hence aiding organisations in the eradication of system vulnerabilities and the prevention of malware assaults. This technology functions across three distinct tiers in the realm of information security management, including prevention and mitigation, detection, and reaction. Artificial intelligence (AI) plays a crucial role in bolstering information security via its ability to better decision-making processes, monitor system activity, and automate jobs, hence enabling fast responses to potential attacks. The flexibility of artificial intelligence (AI) in the domains of data management and security makes it a viable instrument for the development of more secure cyber environments in the future ("Artificial Intelligence and its Application," Onyango), (Everitt et al., 2017).

5. Protective Measures

The concept of security countermeasures spans multiple elements within the domain of information security management (Taylor, 2015). The concept comprises four fundamental elements, namely deterrent, prevention, detection, and cures. Deterrent countermeasures primarily emphasize non-technical approaches, such as the implementation of security regulations and the provision of awareness training, in order to dissuade potential security events. On the other hand, preventive measures cover a range of technologies such as firewalls, intrusion detection systems, encryption, and access controls that are designed to proactively mitigate security breaches (Farahmand et al., 2005). Detection measures encompass the diligent surveillance of suspected vulnerabilities via a range of mechanisms. Remedies, in the context of security breaches, encompass corrective measures implemented subsequent to the occurrence of such breaches. The installation of appropriate countermeasures is necessary in order to lessen the information security risk faced by a company. The task for identifying suitable solutions to mitigate security threats lies with management, albeit requiring diligent managerial oversight (Taylor, 2015), (Goodhue & Straub, 1991), (Taylor & Brice Jr, 2012).

The mere existence of security countermeasures does not inherently ensure a decrease in risks associated with information security. Despite the use of such precautions, the probability of security events continues to be substantial. For example, the efficacy of security policies is compromised when staff do not possess a comprehensive understanding of them. In a similar vein, the inadequacy or incorrect administration of access restrictions can result in the failure to effectively protect computer-based systems. The efficacy of security countermeasures is frequently impacted by human factors, such as errors in installation and configuration (Mattord et al., 2014), (Anderson, 2001).

In order to address these difficulties, it is imperative for responsible management to assess not just the magnitude of risks, but also the feasibility and effectiveness of prospective mitigation strategies (Taylor, 2015), (Farahmand et al., 2005). The alignment between a sensible cost-benefit evaluation and cost-effectiveness may not always be guaranteed, thus requiring a deliberate allocation of resources. As a result, it is imperative for management to make well-informed judgments regarding the prioritization of security threats and the selection of countermeasures that will effectively mitigate risk. Nevertheless, despite previous endeavors to ascertain the most advantageous amounts of expenditure in security countermeasures, a conclusive consensus has yet to materialize. The ultimate determination to enact security countermeasures is a multifaceted process, shaped by limitations in resources and a comprehensive evaluation of hazards within the company (Taylor & Brice Jr, 2012). Given the constraints of limited budgets, companies are required to carefully evaluate concerns pertaining to information security risk management prior to making decisions linked to security. This process entails the identification, prioritization, assessment, and selection of suitable countermeasures to successfully mitigate risks. It recognizes that security decisions can be susceptible to irrational biases, potentially leaving businesses open to information security threats (Yue et al., 2007).

6. Conclusion

Risk assessment plays a crucial role in the framework of Information Security Management. It is imperative for organizations to implement a methodical and meticulously organized approach in evaluating the risks associated with information security pertaining to their assets. Moreover, the evaluation of risks related to information systems has become a crucial topic due to the growing need for resilient information systems and the heightened importance of data protection. In this particular context, risk assessment plays a fundamental role in ensuring the operational integrity of information systems, serving as an essential component within the broader framework of system architecture. The present study commences by providing a comprehensive overview of essential concepts related to information security. Subsequently, it proceeds to examine the historical development and progression of these concepts across time. Through a thorough examination of the present context, this investigation highlights the notable importance of risk assessment in the wider scope of information security. However, it is important to highlight that there are other possible areas that require additional investigation and improvement in the field of risk assessment. One potential area of study involves a comprehensive examination of the underlying complexities present in control methodologies. Moreover, the utilization of risk assessment models and managerial frameworks in various industrial sectors presents potential for uncovering unique intricacies that are distinctive to each sector. These possible pathways present an opportunity to explore and enhance the field of risk assessment, ultimately contributing to the overall improvement of information security standards.

Acknowledgments

Not applicable

Authors contributions

Not applicable

Funding

Not applicable

Competing interests

Not applicable

Informed consent

Obtained.

Ethics approval

The Publication Ethics Committee of the Canadian Center of Science and Education.

The journal’s policies adhere to the Core Practices established by the Committee on Publication Ethics (COPE).

Provenance and peer review

Not commissioned; externally double-blind peer reviewed.

Data availability statement

The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.

Data sharing statement

No additional data are available.

Open access

Copyrights

References

Abbas, H., Magnusson, C., Yngstrom, L., & Hemani, A. (2011). Addressing dynamic issues in information security management. *Information Management & Computer Security*, *19*(1), 5-24. https://doi.org/10.1108/09685221111115836

Anderson, R. (2001, December). Why information security is hard-an economic perspective. In *Seventeenth Annual Computer Security Applications Conference* (pp. 358-365). IEEE.

Asosheh, A., Hajinazari, P., & Khodkari, H. (2013, April). A practical implementation of ISMS. In *7th International Conference on e-Commerce in Developing Countries: with focus on e-Security* (pp. 1-17). IEEE. https://doi.org/10.1109/ECDC.2013.6556730

Bacic, E. M. (1990, December). The Canadian trusted computer product evaluation criteria. In *[1990] Proceedings of the Sixth Annual Computer Security Applications Conference* (pp. 188-196). IEEE.

Behnia, A., Abd Rashid, R., & Chaudhry, J. A. (2012). A survey of information security risk analysis methods. *SmartCR*, *2*(1), 79-94. https://doi.org/10.6029/smartcr.2012.01.007

Bialas, A. (2006). Security of information and services in modern institution and company. *WNT, Warsaw*.

Blakley, B., McDermott, E., & Geer, D. (2001, September). Information security is information risk management. In *Proceedings of the 2001 workshop on New security paradigms* (pp. 97-104). https://doi.org/10.1145/508171.508187

Broderick, J. S. (2006). ISMS, security standards and security regulations. *Information Security Technical Report*, *11*(1), 26-31. https://doi.org/10.1016/j.istr.2005.12.001

Cranor, L. F., & Garfinkel, S. (2005). *Security and usability: designing secure systems that people can use*. " O'Reilly Media, Inc.".

Everitt, T., Goertzel, B., & Potapov, A. (2017). Artificial general intelligence. *Lecture Notes in Artificial Intelligence. Heidelberg: Springer*. https://doi.org/10.1007/978-3-319-63703-7

Farahmand, F., Navathe, S. B., Sharp, G. P., & Enslow, P. H. (2005). A management perspective on risk of security threats to information systems. *Information Technology and Management*, *6*, 203-225. https://doi.org/10.1007/s10799-005-5880-5

Fozilovich, Y. O. (2022). Artificial Intelligence and its Application in Information Security Management. *Central Asian Journal of Theoretical and Applied Science*, *3*(4), 90-97.

Fredriksen, R., Kristiansen, M., Gran, B. A., Stølen, K., Opperud, T. A., & Dimitrakos, T. (2002). The CORAS framework for a model-based risk management process. In *Computer Safety, Reliability and Security: 21st International Conference, SAFECOMP 2002 Catania, Italy, September 10–13, 2002 Proceedings 21* (pp. 94-105). Springer Berlin Heidelberg. https://doi.org/10.1007/3-540-45732-1_11

Galach, A. (2004). Instruction of IT system security management. *Osrodek Doradztwa i Doskonalenia Kadr Publishing House, Gdansk*.

Gehrke, M., Pfitzmann, A., & Rannenberg, K. (1992, September). Information Technology Security Evaluation Criteria (ITSEC)-a Contribution to Vulnerability? In *IFIP Congress (2)* (pp. 579-587).

Goodhue, D. L., & Straub, D. W. (1991). Security concerns of system users: A study of perceptions of the adequacy of security. *Information & Management*, *20*(1), 13-27. https://doi.org/10.1016/0378-7206(91)90024-V

Granata, P. (2023, March 8). The three types of Artificial Intelligence: A glimpse into the future. *DeltalogiX*. Retrieved from https://deltalogix.blog/en/2023/03/08/artificial-intelligence-a-look-at-its-three-types-and-their-possible-future-implications/

Joint Technical Committee ISO/IEC JTC1. Subcommittee SC 27. (2013). *Information Technology--Security Techniques--Information Security Management Systems--Requirements*. ISO/IEC.

Karabacak, B., & Sogukpinar, I. (2005). ISRAM: information security risk analysis method. *Computers & Security*, *24*(2), 147-159. https://doi.org/10.1016/j.cose.2004.07.004

Karapilafis, G. (2015). Implementation of Artificial Intelligence in INFOSEC tasks and applications. *Journal of Applied Mathematics and Bioinformatics*, *5*(3), 113.

Kuzminykh, I., Ghita, B., Sokolov, V., & Bakhshi, T. (2021). Information security risk assessment. *Encyclopedia*, *1*(3), 602-617. https://doi.org/10.3390/encyclopedia1030050

Latham, D. C. (1986). Department of defense trusted computer system evaluation criteria. *Department of Defense*, *198*.

Mattord, H. J., Levy, Y., & Furnell, S. (2014). Factors for measuring password-based authentication practices. *Journal of Information Privacy and Security*, *10*(2), 71-94. https://doi.org/10.1080/15536548.2014.924812

Onyango, O. O. *Artificial Intelligence and its Application to Information Security Management.*

Peixoto, U. I., Casal-Ribeiro, M., Medeiros-Leal, W. M., Novoa-Pabon, A., Pinho, M., & Santos, R. (2022). Scientific and Fisher's Knowledge-Based Ecological Risk Assessment: Combining Approaches to Determine the Vulnerability of Fisheries Stocks. *Sustainability*, *14*(22), 14870. https://doi.org/10.3390/su142214870

Rannenberg, K. (1993, August). Recent Development in Information Technology Security Evaluation-The Need for Evaluation Criteria for Multilateral Security. In *Security and control of information technology in society* (pp. 113-128).

Rot, A. (2008). IT risk assessment: Quantitative and qualitative approach. *Resource*, *283*(March), 284.

Ryba, M., Poniewierski, A., Sulwinski, J., & Górnisiewicz, M. (2009). The methodology for managing the abuse of IT systems. *Information Security Journal: A Global Perspective*, *18*(3), 107-115. https://doi.org/10.1080/19393550902791457

Schmidt, M. (2023). Information security risk management terminology and key concepts. *Risk management*, *25*(1), 2. https://doi.org/10.1057/s41283-022-00108-8

Siponen, M., & Willison, R. (2009). Information security management standards: Problems and solutions. *Information & management*, *46*(5), 267-270. https://doi.org/10.1016/j.im.2008.12.007

Stoneburner, G., Goguen, A., & Feringa, A. (2002). Risk management guide for information technology systems. *Nist special publication*, *800*(30), 800-30. https://doi.org/10.6028/NIST.SP.800-30

Sundu, M., & Ozdemir, S. (2020). The effect of artificial intelligence on management process: challenges and opportunities. *Challenges and Opportunities for SMEs in Industry 4.0*, 22-41. https://doi.org/10.4018/978-1-7998-2577-7.ch003

Susanto12, H., Almunawar, M. N., & Tuan, Y. C. (2011). Information security management system standards: A comparative study of the big five. *International Journal of Electrical Computer Sciences IJECSIJENS*, *11*(5), 23-29.

Szczepankiewicz, E. I., & Szczepankiewicz, P. (2006). Risk analysis in IT environment for the Purpose of Operational Risk Management. Part 3–Strategies of Dealing the Operational Risk. *Monitor Rachunkowosci i Finansow*, *8*.

Szyjewski, Z. (2004). Methodologies of IT projects management. *Placet, Warsaw*.

Task, J. (1993). *Foundations for the Harmonization of Information Technology Security Standards.*

Taylor, R. G. (2015). Potential problems with information security risk assessments. *Information Security Journal: A Global Perspective*, *24*(4-6), 177-184. https://doi.org/10.1080/19393555.2015.1092620

Taylor, R. G., & Brice Jr, J. (2012). Fact or fiction? A study of managerial perceptions applied to an analysis of organizational security risk. *Journal of Organizational Culture, Communications and Conflict*, *16*(1), 1.

Tofan, D. C. (2011). Information security standards. *Journal of Mobile, Embedded and Distributed Systems*, *3*(3), 128-135.

Tolani, M. G., & Tolani, H. G. (2019). The use of artificial intelligence in cyber defense. *International Studies Journal of Engineering and Technology (IRJET)*, *6*(7), 3084-3087.

Volkan Evrin, C. I. S. A., & CRISC, C. (2021). *Risk Assessment and Analysis Methods: Analysis and Quantitative Risk Assessment and Analysis Methods: Qualitative and Quantitative*. (n.d.). ISACA. Retrieved from https://www.isaca.org/resources/isaca-journal/issues/2021/volume-2/risk-assessment-and-analysis-methods

Wawrzyniak, D. (2006). Information security risk assessment model for risk management. In *Trust and Privacy in Digital Business: Third International Conference, TrustBus 2006, Kraków, Poland, September 4-8, 2006. Proceedings 3* (pp. 21-30). Springer Berlin Heidelberg. https://doi.org/10.1007/11824633_3

Wawrzyniak, D. (2007). *Models of IT risk assessment–classical approach and possibilities of its development.*

Yue, W. T., Çakanyıldırım, M., Ryu, Y. U., & Liu, D. (2007). Network externalities, layered protection and IT security risk management. *Decision Support Systems*, *44*(1), 1-16. https://doi.org/10.1016/j.dss.2006.08.009