Revista de Informática Teórica e Aplicada - RITA - ISSN 2175-2745
Vol. 31, Num. 2 (2024) 43-55

RESEARCH ARTICLE

Framework for Security Risk Assessment (FSRA) and Fuzzy Risk Inference System (FRIS) based on Standard ISO/IEC 27002:2022

Framework para Security Risk Assessment (FSRA) e Fuzzy Risk Inference System (FRIS) Baseado no Padrão ISO/IEC 27002:2022

Diógenes Antonio Marques José[1]*, Douglas Schmitz Dupski[2], Kembolle Amilkar[3]

Abstract: Information security is a critical aspect for organizations, and a problem in this regard consists of knowing the level of vulnerability in which organizations. Therefore, this article aims to present a Cybersecurity Framework (FSRA) based on the ISO/IEC 27002:2022 standard. In addition, a Fuzzy Risk Inference System (FRIS) is presented, which uses FSRA controls - Security Practices (SP), Software (S), and People (P) as input, a total of 93 sub-items. A FRIS output is the Security Risk (SR) in which the organization is due to non-compliance or partial compliance with FSRA controls. Thus, if each control is fully met, its entry value in the FRIS will be 100%. Otherwise, it will be proportional. Therefore, when the FRIS returns the SR, whose output values can be Low (13% to 39.99%), Medium (40% to 59.99%), or High (60% to 100%), the security analyst can measure the risk security, in which the organization is located, according to ISO/IEC 27002:2022 and from that know where to act and how to act.
Keywords: Cybersecurity — ISO/IEC 27002:2022 — Fuzzy Logic — Framework — Cyber Threats

Resumo: A segurança da informação é um aspecto crítico para as organizações, e um problema neste sentido consiste em conhecer o nível de vulnerabilidade em que se encontram as organizações. Portanto, este artigo tem como objetivo apresentar um Framework de Segurança Cibernética (FSRA) baseado na norma ISO/IEC 27002:2022. Além disso, é apresentado um Sistema de Inferência de Risco Fuzzy (FRIS), que utiliza controles FSRA – Práticas de Segurança (SP), Software (S) e Pessoas (P) como entrada, um total de 93 subitens. Uma saída do FRIS é o Risco de Segurança (SR) em que a organização se deve à não conformidade ou conformidade parcial com os controles do FSRA. Assim, se cada controle for integralmente atendido, seu valor de entrada no FRIS será de 100%. Caso contrário, será proporcional. Portanto, quando o FRIS retorna o Risco de Segurança (RS), cujos valores de saída podem ser Baixo (13% a 39,99%), Médio (40% a 59,99%) ou Alto (60% a 100%), o analista de segurança pode medir o risco de segurança, onde a organização está localizada, de acordo com a ISO/IEC 27002:2022 e a partir disso saber onde agir e como agir.
Palavras-Chave: Cibersegurança — ISO/IEC 27002:2022 — Lógica Fuzzy — Framework — Ameaças Cibernéticas

[1] *Universidade do Estado de Mato Grosso (UNEMAT), Rua A N30, Bairro São Raimundo, Barra do Bugres, Mato Grosso, CEP 78390-000, Brazil*
[2] *Universidade do Estado de Mato Grosso (UNEMAT), Rua A N30, Bairro São Raimundo, Barra do Bugres, Mato Grosso, CEP 78390-000, Brazil*
[3] *Ministério Público do Estado de Mato Grosso (MPMT), Setor D, Centro Politico e Administrativo, Cuiabá, Mato Grosso, CEP 78049-928, Brazil*
*__Corresponding author__: dioxfile@unemat.br
DOI: https://doi.org/10.22456/2175-2745.136309 • **Received:** 19/10/2023 • **Accepted:** 27/06/2024
CC BY-NC-ND 4.0 - This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License.

1. Introduction

Information security is a critical aspect of organizations. With the rise of cyber threats and the increasing complexity of systems, adopting practical approaches to identify, analyze and assess security risks is essential. Therefore, the security risk assessment *framework* emerges as an essential tool, providing guidelines and methods to deal with challenges in protecting digital data. A digital security *framework* allows for a systematic and comprehensive approach, considering threats,

vulnerabilities, and potential impact. In this way, by defining a clear *framework* for risk assessment, frameworks help organizations to take proactive measures to protect their assets and ensure their business continuity [1].

Furthermore, as per the most recent report by *FortiGuard Labs* [2], *Fortinet's Threat Intelligence and Analysis Lab*, Latin America, and the Caribbean faced more than 360 billion attempted cyberattacks in 2022. Mexico recorded the highest number of attack attempts, with 187 billion, followed by Brazil with 103 billion, Colombia with 20 billion, and Peru with 15.4 billion. These alarming numbers highlight the region's urgent need for robust cybersecurity solutions. Cybersecurity is a critical concern for organizations worldwide as they increasingly rely on digital technologies to conduct their business [3]. Because of this, several security frameworks have been developed to try to mitigate digital attacks [4][5][6], etc. Furthermore, when proposing a framework, it is necessary to follow the information security controls suggested by *ISO/IEC 27002:2022*[1], which provides guidelines and best practices for implementing information security in companies[2]. In this context, a problem encountered in implementing cybersecurity in Brazilian companies (public and private) is discovering the degree of security risk the company faces by failing to meet the minimum requirements for applying the security policies of the *ISO/IEC 27002:2022* standard.

Therefore, the objective of this article is to present the *Framework for Security Risk Assessment (FSRA)* which serves as a minimum information security requirement based on *ISO/IEC 27002:2022* and a *Fuzzy Risk Inference System (FRIS)*[3]. The *FRIS* is designed to estimate the *Security Risk (SR)* faced by the company. To implement *FRIS*, fuzzy logic [7] was used. Fuzzy logic uses a mathematical approach that allows for dealing with uncertainty and imprecision, ideal for the context of cybersecurity that is uncertain and imprecise. As *FRIS* input, the *FSRA* parameters are used: *Security Practices (SP)*, *Software (S)*, and *People (P)*. In this context, the companies' level of compliance with the *FSRA* security parameters was assessed. Based on this assessment, the *Fuzzy Risk Inference System (FRIS)* will provide an estimate of the *Security Risk (SR)* as the output, reflecting the company's adherence to the *FSRA* standards.

Consequently, the proposed framework presents the Security Risk in which a company finds itself due to needing to comply with the minimum controls of the ISO/IEC 27002:2022 standard. Furthermore, the difference in this proposal is to use the most recent ISO/IEC 27002:2022 standard. Moreover, the (FRIS) used by the framework (FSRA) is composed of 19 inference rules based on expert knowledge that prioritizes the Security Practices (SP) control, which is one of the main controls in ISO/IEC 27002:2022. Another contribution of our proposal is the defuzzification methods used: the centroid and the Maximum Average (MoM). These methods provide a more accurate result when assessing the security risk. For instance, when using the centroid, even if the organization complies with 100% of the *FSRA* controls, there will still be a security risk of at least 13%, as in real scenarios where an organization is not 100% secure. In the other direction, when using the Maximum Average defuzzification method (MoM), if the company does not comply with *SP Controls* or complies with less than 20% of them, the organization will be 100% at risk, that is, a cyber attack is imminent.

After exhaustively testing the *FRIS* through scripts that generate random entries, five thousand entries, the *FRIS* was tuned. The results showed several possibilities of security risks classified as *low*, *medium*, and *high*, and this *Security Risk* indicates whether the company urgently needs to improve its security practices according to *ISO/IEC 27002:2022*. Thus, to facilitate the use of this framework, a *web* application was developed in which the organization's security analyst can automatically check the level of *Security Risk* in which the organization under his responsibility is found. Consequently, this application is available on *GitHub* for download at the following link: FSRA.

The remainder of this article is divided as follows: Section 2 presents related works; Section 3 presents the description of the proposal and the methodology (materials and methods) employed in the development and testing of *FSRA* and *FRIS*; Section 4 presents the results and discussion; and, finally, in Section 5, conclusions, and possibilities for future work are presented.

2. Related Works

Sendi et al. [8] propose *FEMRA*, an organizational risk assessment *framework*. It comes as a response to the absence of detailed guidelines in the *NIST* and *ISO 27001* standards. Using fuzzy logic and expert systems, *FEMRA* offers a structured, quantitative approach to risk assessment, representing each risk with a numerical value. It allows security professionals to identify and compare risks and create efficient strategies to mitigate them, improving organizations' implementation of the *Information Security Management System (ISMS)*. Consequently, the work in question uses the *ISO/IEC 27001 standard*, while our approach uses the *ISO/IEC 27002:2022 standard*. Furthermore, *FEMRA* uses a single defuzzification method in its *FIS* (e.g., the centroid), and our proposal uses two methods (e.g., the centroid and the *Maximum Average Method (MoM)*) which makes our *FIS* more accurate.

Newcomb and Hammell [6] present a *framework* based on fuzzy logic, called *FLUF*, intended to support defense and decision-making related to security risks. *FLUF* was effectively used to prioritize cyber defense alerts. The results showed that, with *FLUF*, a high-priority alert could be attended to in a few minutes. Furthermore, this *framework*'s architecture and rules have significantly contributed to automated cybersecurity decision-making. Therefore, this work uses the ISO/IEC 27001 standard. However, our approach

[1] Three types: Preventive, Detective, and Corrective. For more details see https://www.abntcatalogo.com.br/.

[2] https://www.iso.org/standard/75652.html.

[3] *FRIS* was built after consultation with a cybersecurity expert.

uses the ISO/IEC 27002:2022 standard. Furthermore, *FLUF* uses a single defuzzification method in its FIS (e.g., the centroid), and our proposal uses two methods (e.g., the centroid and the *MoM*) which makes our FIS more robust.

Alali et al. [9] describe the importance of a robust cyber risk assessment in the face of the growing threat of Internet crime. Therefore, they propose a risk assessment model using the *Mamdani fuzzy inference system*, considering vulnerability, threat, probability, and impact factors. The methodology demonstrates the power of fuzzy inference systems to control risk assessment. The results indicate a risk assessment of 53.8% (rated as a Medium) that requires attention. The conclusion reinforces the need for each system to keep its components at controlled risk to avoid failures and data loss, underlining the importance of active involvement and meeting the needs of end users. Thus, the FIS proposed in this work, as well as FSRA/FRIS, our proposal, does not cover all aspects of cybersecurity and cybercrime issues. However, although the authors carried out a detailed analysis of the feasibility of the proposal (e.g., on MATLAB) it was not based on multiple inputs, for example, a thousand different inputs.

In [10], a tool based on the theory of fuzzy sets is presented to prioritize *Information Security Controls (ISC)* in organizations. The method involves the application of a questionnaire to determine the initial relevance of the *ISC* and subsequent analysis using fuzzy logic. This process provides a more detailed and accurate assessment of *ISC*s, supporting their effective selection. The main contribution of this work is the introduction of a methodology based on the *Fuzzy Set Theory* for a comprehensive evaluation of *ISC*. The research concludes by stating the need for effective information security platforms to prevent fraud and violations. The proposed methodology can help evaluate and properly implement *ISC* in organizations.

Othmano et al. [11] apply fuzzy logic in risk assessment to analyze generic threats in the *firewall* of an educational institution. The proposal is a new *Network Security Risk Assessment (ASRR)* model, which involves the identification of organizational assets, threats, risks, and using natural language. Furthermore, the study demonstrates that a *firewall* is crucial to network security. It emphasizes the need for a robust support system and risk assessment plan to deal with potential threats. The results showed that the *firewall* faced moderate threats, indicating an acceptable risk. This assessment made it possible to identify the need for specific measures to deal with the anticipated threats. The study contributed to a better understanding of the institution's security environment and the development of effective data protection strategies.

Hsieh et al. [4] proposed a risk assessment model based on fuzzy logic for software development projects. The objective was to offer project managers a more effective tool to assess and manage the risks inherent in these projects. The result was the development of a *Fuzzy Risk Assessment Index (IARF)* that considers risk attributes such as the organizational environment, users, security requirements, project complexity, team/planning, and control. The *IARF* was aggregated using a fuzzy weighted average, and, as an illustration, a case study was carried out to assess the risk of an electronic toll collection project. Therefore, the results showed that the proposed model could efficiently help managers deal with complexity, uncertainty, and imprecision in the risk assessment of software development projects.

Shreeve et al. [12] analyzed managers' decision-making with little technical experience in cybersecurity. In this way, security objectives were identified, and consequently, a reasoning model was developed that demonstrates how these teams make decisions based on logic, risk management, and security goals. The results showed that managers can make informed choices in cybersecurity, although they can benefit from increased knowledge in this area. Furthermore, the survey showed that including cybersecurity experts in the decision, teams was also recommended to provide additional expertise during decision-making.

In [5], a unified approach is proposed, using fuzzy set theory, for forecasting risk in assets to assess the effectiveness of existing controls. In addition, machine learning classifiers and the *Comprehensive Assessment Model (MAA)* were applied as an aid. Experimental results showed that fuzzy set theory effectively assesses asset criticality, and machine learning classifiers have exemplary performance in predicting different types of risks. Furthermore, the *MAA* approach demonstrated better effectiveness of specific controls in reducing risks. The validity and acceptability of the proposed *framework* and the tool are confirmed through a case study and *feedback* from *stakeholders*. The results showed the importance of this approach for effective risk management practice in real-world environments.

In addition to the academic works presented in this section, numerous other software proposals for security risk analysis are available, which can be found at this link: https://cybersecuritynews.com/cybersecurity-risk-management-tools/.

3. Proposal Description

Threats to information security are significant and diverse, with the absence of an information security policy identified as a primary vulnerability to attacks. Additionally, several underlying issues contribute to the need for more strategic planning in digital security. These include a lack of awareness among high-level leaders and a denial that the organization could be a potential target for cybercriminals. Therefore, the lack of a security program can result in several problems, for example, the lack of a data backup strategy, employee misinformation, failure to update security patches, possible *Ransomware* attacks, threats arising from devices not protected, and vulnerabilities associated with remote work [13]. With this in mind, the *FSRA* follows the controls suggested by *ISO/IEC 27002:2022*, integrating a *Fuzzy Risk Inference System (FRIS)* into the security management process. Thus, this proposal aims to assess companies' compliance levels with good practices and security policies by the *ISO/IEC*

27002:2022 standard. The compliance index, derived from the English verb 'to comply', expresses the need to adhere to a specific rule, request, or command. This concept encompasses the obligation to adhere to, comply with, and enforce internal and external regulations imposed on an organization's operations. The focus is on compliance with established standards to promote integrity, legality, and effectiveness in organizational processes [14].

As for the metrics proposed in this study, an information security expert, *Kembolle Amilkar*, was consulted to choose them, who has more than 20 years of experience in intelligence and cybernetic counterintelligence and, in addition, develops work in cybersecurity for the Government of the state of Mato Grosso. Therefore, to create the *FRIS*, three controls of greater importance were defined and that cover the minimum security requirements for organizations[4]. The controls are as follows: **(i) Security Practices (SP)**, consisting of two *ISO/IEC 27002:2022* controls (e.g., Organization Controls and Physical Controls) that describe recommended or required best practices for information security in an organization; **(ii) Softwares (S)** deals with security guidelines for software; and **(iii) People (P)** considers all guidelines aimed at user security.

3.1 Framework for Security Risk Assessment (FSRA)

The structural model provides several guidelines for assessing security risks posed by both internal and external digital threats. The structure is hierarchical in classes that represent the main controls that suffer most in terms of identified threats and that can stop organizations. Points I through III include critical guidelines and security procedures covering inside-to-outside network [15][16][17] protection per *ISO/IEC 27002:2022*. In addition, adding all three controls that make up the *framework* proposal, there are 93 sub-items, 51 in the *Security Practices (SP) control*, 34 in the *Software (S) control*, and 8 in the *People (P) control*. Therefore, only the first sub-items of each control are displayed. For more details, consult the *ISO/IEC 27002:2022* standard at: https://www.iso.org/obp/ui/en/#!iso:std:75652:en.

I. **Security Practices (SP): 5. Organization Controls:** It has 37 sub-items (5.1 to 5.37) aimed at security in organizations. E.g., Policies for information security, Information security roles and responsibilities, and Segregation of duties; **7. Physical Controls:** Contains 14 sub-items (7.1 to 7.14) for mitigating and combating physical threats. E.g., Physical security perimeters and Physical entry.

II. **Software (S): 8. Technological controls:** It has 34 sub-items (8.1 to 8.34) necessary for code management, configuration, and maintenance of technological systems. E.g., User endpoint devices, Privileged access rights, Information access restriction, and Access to source code.

III. **People (P): 6. People Control:** Includes eight sub-items (6.1 to 6.8) essential for safely managing human resources. E.g., Screening, terms, and conditions of employment, Information security awareness, education and training, Disciplinary process, and Responsibilities after termination or change of employment.

[4]According to the cyber security expert consulted, FSRA controls are the minimum security requirements that an organization must comply with to comply with ISO/IEC 27002:2022 and, in this way, guarantee the minimum cyber security requirements against digital threats.

3.2 *FRIS* proposal

This section demonstrates the fuzzy logic application steps on the good practices contained in the *FSRA* presented in Section 3.1. In addition, it is intended to qualify good practices regarding the compliance index in organizations, that is, how much of the *FSRA* the organization complies with. Based on the work of José at. al [18].

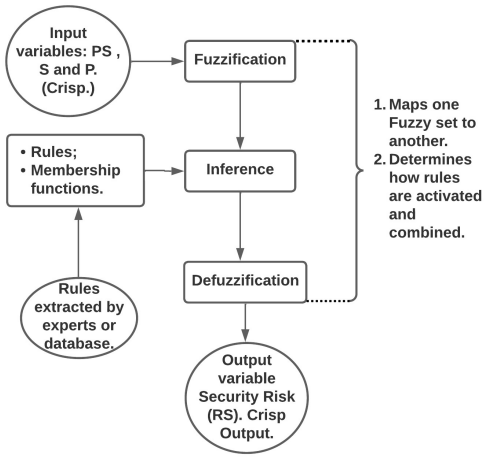
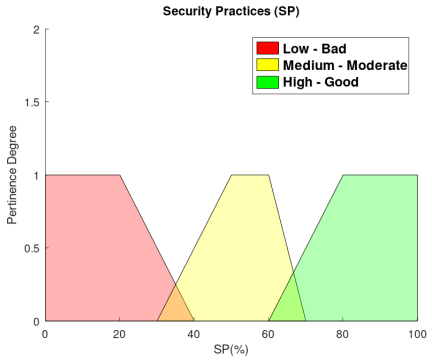


Figure 1. Fuzzy Risk Inference System (FRIS).

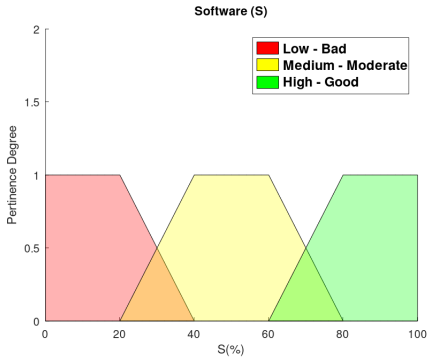
The *FRIS* (Figure 1) is based on fuzzy set theory [7] and comprises three distinct components: Fuzzification, Inference, and Defuzzification. For example, **Fuzzification** maps a non-fuzzy input value, which converts the membership degree of each input variable (e.g., *SP*, *S*, and *P*) into a fuzzy value; **Inference** is responsible for mapping one fuzzy value to another. Inference checks the validity of the *Inference Rules* (Table 1), which consist of sentences of the type **IF A is Good AND B is Medium Then C is Good**, where **IF A is Good AND B is Medium** is the antecedent of the rule, and **Then C is Good** is the consequent. Here, **A**, **B**, and **C** are *Linguistic Variables (LVs)*, **Good** and **Medium** are linguistic concepts expressed as fuzzy sets [19]; and **Defuzzification** converts a fuzzy number into a precise quantity (crisp/real) to be used in decision-making [7].

The *FRIS* addressed in this work is based on the inference model of *Mamdani* [9]. The input variables for the fuzzification process are the following controls *SP*, *S*, and *P*, which are the *Linguistic Variables (LVs)* and correspond, respectively,

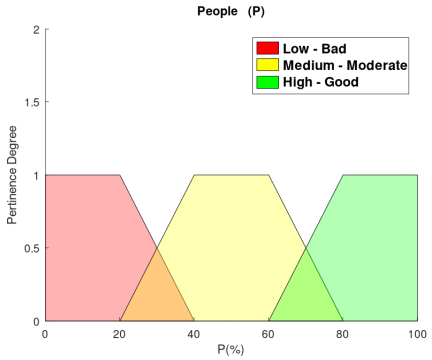
to items **I**, **II**, and **III** of the ***FSRA***. In this context, the system output linguistic variable is the *Security Risk (SR)*. The linguistic terms Low, Medium, and High are used to describe the fuzzy sets of each input variable. For example, the membership functions illustrated in Figure 2(a),(b),(c), and (d) represent these LVs.



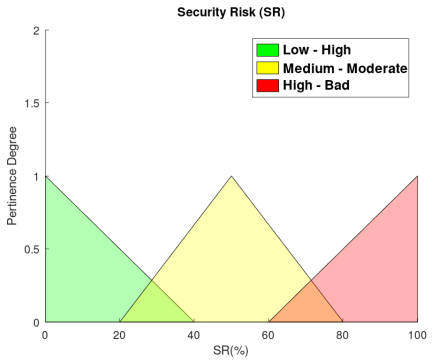
(a) Antecedent variable (SP).



(b) Antecedent variable (S).



(c) Antecedent variable (P).



(d) Consequent variable (SR).

Figure 2. Membership Curves of the Linguistic Variables SP, S, P, and SR.

These membership functions were defined and adjusted based on the expertise of the consulted specialist. According

to the literature, there is no universally applicable method for determining membership functions; the method that best fits the specific problem should be used . Therefore, trapezoidal and triangular curves were selected for constructing the membership functions, as they were better suited to the problem. Equations 1 and 2 represent these curves:

$$\mu_{\text{trap}}(x) = \max\left(\min\left(1, \frac{x-a}{b-a}, \frac{d-x}{d-c}\right), 0\right). \quad (1)$$

$$\mu_{\text{tri}}(x) = \max\left(0, \min\left(1, \frac{x-a}{b-a}, \frac{c-x}{c-b}\right)\right). \quad (2)$$

Additionally, *FRIS* utilizes fuzzy operations of the **AND** type, such as **IF A AND B THEN C**. This operation represents the intersection of two fuzzy sets (e.g., **A** and **B**) characterized by membership functions $\mu_A(x)$ and $\mu_B(x)$. This intersection can be expressed as shown in equation 3:

$$\mu_C(x) = \min\left(\mu_A(x), \mu_B(x)\right). \quad (3)$$

In this scenario, 27 inference rules were generated, considering the three input linguistic values (*Low, Medium, and High*) and three linguistic variables (*LVs*). These rules can be derived using a Simple Arrangement with Repetition. For instance, considering *LVs* as $n = SP, S, P$ and linguistic values as $p = Low, Medium, High$, we have $A, R_{n,p} = |n|^{|p|} \Leftrightarrow A, R_{3,3} = |3|^{|3|} = 27$. However, due to the specific requirements of the problem, only 19 rules were used. This is because the *LV SP*, according to the expert, must lead the rule's consequent to a high-security risk whenever its conformance index is below 40%, which occurs whenever its linguistic concept is *Low* (as explained in item **III** of the Fuzzy Implication Algorithm, Section 3.2.1). Each rule has a consequence related to the security risk, with three possible outcomes: *Low*, *Medium*, or *High*. The developed rules are shown in Table 1.

Table 1. Inference Rules.

Nº	Rules
1	IF SP is Low ⇒ Security Risk is High
2	IF SP is Medium AND S is High AND P is High ⇒ Security Risk is Low
3	IF SP is Medium AND S is Medium AND P is High ⇒ Security Risk is Medium
4	IF SP is Medium AND S is Low AND P is High ⇒ Security Risk is Medium
5	IF SP is Medium AND S is High AND P is Medium ⇒ Security Risk is Medium
6	IF SP is Medium AND S is High AND P is Low ⇒ Security Risk is Medium
7	IF SP is Medium AND S is Medium AND P is Medium ⇒ Security Risk is Medium
8	IF SP is Medium AND S is Medium AND P is Low ⇒ Security Risk is High
9	IF SP is Medium AND S is Low AND P is Low ⇒ Security Risk is High
10	IF SP is Medium AND S is Low AND P is Medium ⇒ Security Risk is High
11	IF SP is High AND S is High AND P is High ⇒ Security Risk is Low
12	IF SP is High AND S is Medium AND P is High ⇒ Security Risk is Low
13	IF SP is High AND S is Low AND P is High ⇒ Security Risk is Medium
14	IF SP is High AND S is High AND P is Medium ⇒ Security Risk is Low
15	IF SP is High AND S is High AND P is Low ⇒ Security Risk is Medium
16	IF SP is High AND S is Medium AND P is Medium ⇒ Security Risk is Medium
17	IF SP is High AND S is Medium AND P is Low ⇒ Security Risk is Medium
18	IF SP is High AND S is Low AND P is Low ⇒ Security Risk is High
19	IF SP is High AND S is Low AND P is Medium ⇒ Security Risk is Medium

Therefore, to generate the consequents of the inference rules, the operation between the predicates is based on the meanings of the linguistic concepts of the *LV's SP*, *S*, and *P*. For example, it was necessary to consider the relevance of these concepts and the logical operations applied to the qualifiers in each predicate. Table 2 provides details on this relevance or significance.

Table 2. Linguistic Concepts of VLs and Their Meaning.

Linguistic Variables	Linguistic Concepts	Qualifier
SP	Low	Bad
SP	Medium	Moderate
SP	High	Good
S	Low	Bad
S	Medium	Moderate
S	High	Good
P	Low	Bad
P	Medium	Moderate
P	High	Good

Thus, the operation on each rule follows the *Fuzzy Implication (FI)* algorithm:

3.2.1 Fuzzy Implication Algorithm

I- If all rules have different linguistic concepts (e.g., **Low, Medium, High**) or the same (e.g., **Low, Low, Low**), for the conclusion of these rules, the **AND** operator is applied sequentially to the qualifiers of each rule (e.g., **Good, Moderate, and Bad**). For example, the rule **6** (Table 1) **IF SP is Medium**^{Moderate}**, AND S is High**^{Good} **AND P is Low**^{Bad} implies that **Security Risk is Medium**^{Moderate}; **II-** If a rule has two linguistic concepts that are both equal to *Medium*, the conclusion of that rule will be *Medium* ***if and only if*** one of the linguistic variables has a linguistic concept that is equal to *High*. For example, rules **3**, **5**, and **16**, Table 1; and **III-** All rules that have the linguistic variable *SP* with a linguistic concept equal to Low^{Bad} will be converted into a single rule with consequent $High^{Bad}$, Table 1. According to the expert consulted, this control is one of the most important and cannot have low adherence by the organization, for instance, minimum adhesion 40%.

This algorithm aims to prevent a single condition from determining the outcome of the rule. The actions performed with the qualifiers for completing the rules are shown in Table 3.

Table 3. Operations on the Qualifiers of Inference Rules.

Qualifier	Operator	Qualifier	Implication	Result
Good	AND	Good	⇒	Good
Good	AND	Moderate	⇒	Good
Good	AND	bad	⇒	Moderate
Moderate	AND	Moderate	⇒	Moderate
Moderate	AND	Bad	⇒	Bad
Bad	AND	Bad	⇒	Bad

The rules' composition results from an aggregation of fuzzy sets, which are generated by the interaction of multiple sentences. The main objective of this process is to create an output value, which will be later used in the defuzzification process. This composition is expressed according to Equation

4.

$$\mu_{B_i'}(y) = \max\left(\min[\mu_{A_{k1}}(x_1), \mu_{A_{k2}}(x_2), \ldots, \mu_{A_{kp}}(x_p)]\mu_{B_i}(y)\right), \quad \forall y \in U_{y_j}. \tag{4}$$

The function $\mu_{B_i'}(y)$ represents the activation of the ith output rule concerning the universe of discourse of the output y. The expression inside the $min[]$ operation, i.e., $\mu_{A_{k1}}(x_1), \mu_{A_{k2}}(x_2)$,..., $\mu_{A_{kp}}(x_p)$, represents the degrees of membership of the antecedents of the rules for the input values $x_1, x_2, \ldots, x_p$. The term $\mu_{B_i}(y)$ is the degree of membership of the rule output i for the value y. This function is calculated for all y values in the universe of discourse of the U_{y_j} output. Therefore, regarding the defuzzification method, we chose to use the *Maximum Average Method (MoM)* and *Centroid* due to their efficiency in manipulating qualitative variables [19]. The equations 5 and 6 represent these calculations, respectively:

1. Maximum Average Method (MoM):

$$\text{MoM} = \frac{\sum(\text{max_values} \times \text{membership_values})}{\sum \text{membership_values}} \tag{5}$$

max_values: These are the maximum membership values for each fuzzy set. These values represent the maximum membership points in each fuzzy set; and **membership_values:** Are the membership values corresponding to each value of max_values. These values indicate the degree of membership assigned to each fuzzy set.

2. Centroid method:

$$\text{Centroid} = \frac{\int_a^b x \cdot \mu(x)\, dx}{\int_a^b \mu(x)\, dx} \tag{6}$$

a **and** b**:** Are the limits of the integration interval on the x axis. These limits determine the range of continuous values for which the membership function is integrated; x**:** Is the continuous variable of the x axis. It represents the values in the integration interval for which the membership function is evaluated; and $\mu(x)$**:** Is the membership function, which assigns a membership degree to each value of x in the integration interval. It describes how much a x value belongs to the fuzzy set under consideration.

The *Maximum Average Method (MoM)* approach does not consider the shape of the output membership functions. In comparison, the *Centroid* presents better measurement regarding the indices of the evaluated outputs. Its implementation takes into account existing information security evaluation methods. Thus, through expert knowledge, values were assigned, on a scale from 0% to 100%, for each linguistic concept of each *FRIS* variable. These values help define the fuzzy sets' discourse universe and their membership functions $\{Low, Medium, and\ High\}$. The resulting ranking is presented in Table 4.

Table 4. The classification of Fuzzy sets by Expert.

Inputs (VLs)	Linguistic Concept	Percentage scale from 0 to 100
SP	High	60 a 100
SP	Medium	30 a 70
SP	Low	0 a 40
S	High	60 a 100
S	Medium	20 a 80
S	Low	0 a 40
P	High	60 a 100
P	Medium	20 a 80
P	Low	0 a 40
SR	High	60 a 100
SR	Medium	20 a 80
SR	Low	0 a 40

3.3 Materials and Methods

This subsection presents the methodology and tools used to evaluate the proposal.

Software: (a.) **MatLab (Version 9.14.0.2254940 - R2023a) Update 2**: This tool was used for numerical programming, data visualization, among others[5]; (b.) **Fuzzy Logic Toolbox (Version 3.1 - R2023a)**: This *MatLab* extension was used to manipulate fuzzy logic concepts and algorithms; (c.) **GNU Octave (Version 8.2.0)**: Used for numerical computation, working as an open source alternative to *MatLab*[6]; (d.) **fuzzy-logic-toolkit (Version 0.4.6)**: This package was employed in GNU Octave to deal with fuzzy logic.

Procedures for *FRIS* evaluation: (a.) All sub-items of each control, *Linguistic Variable*, have the same weight. *FRIS* is composed of three input Linguistic Variables - *(SP)*, *(S)*, and *(P)*, which are the *FSRA* controls to be fulfilled by organizations. In this context, the value of each input variable is assigned as follows - *the value 100% will be divided by the number of sub-items of the control, i.e., if the organization fulfills 25 sub-items, for example, the sub-items of the control Security Practices (SP), then the value of this variable for entry into FRIS will be* $\cong 49.02\%$. *This value represents the ratio of selected items to the total number of items in the control*; (b.) The linguistic variable *(SR)* is the output variable, and its value is the security risk resulting from running *FRIS*; (c.) After going through phases (a.) and (b.), *FRIS* will be calibrated. Calibration consists of improving the membership curves so that the values resulting from defuzzification, *Security Risk (SR)*, are optimal. To do this, we created a *Shell Script* to generate *five thousand (5000)* entries for the three linguistic variables *SP*, *S*, and *P* of the *FSRA* controls (e.g., *Security Practices*, *Software*, and *People*). After that, we use these inputs in the *Fuzzy Risk Inference System (FRIS)* and check the results with the expert. If the results match reality, according to the expert, we maintain the membership curves, otherwise, we modify the values of the curves and repeat the tests.

[5] https://www.mathworks.com/products/matlab.html.
[6] https://octave.org/.

3.3.1 Applied Tests

The main component of the proposal is a system written in a programming language compatible with both *MatLab* and *GNU Octave*, Figure 3(a). Thus, with the aid of this algorithm, it was possible to calibrate *FRIS*, especially about the evaluation of the rules, Figure 3(b) and Table 1.

```
[Input1]
Name='SP'
Range=[0 100]
NumMFs=3
MF1 = 'Low' :  'trapmf', [-1 0 20 40]
MF2=  'Medium' :  'trapmf', [30 50 60 70]
MF3=  'High'  :  'trapmf', [60 80 100 101]
[Input2]
Name='S'
Range=[0 100]
NumMFs=3
MF1 = 'Low' :  'trapmf', [-1 0 20 40]
MF2=  'Medium' :  'trapmf', [20 40 60 80]
MF3=  'High'  :  'trapmf', [60 80 100 101]
[Input3]
Name='P'
Range=[0 100]
NumMFs=3
MF1 = 'Low' :  'trapmf', [-1 0 20 40]
MF2=  'Medium' :  'trapmf', [20 40 60 80]
MF3=  'High'  :  'trapmf', [60 80 100 101]
[Output1]
Name = 'SR'
Range = [0 100]
NumMFs = 3
MF1 = 'Low'  : 'trimf', [-1 0 40]
MF2 = 'Medium' : 'trimf', [20 50 80]
MF3 = 'High' : 'trimf', [60 100 101]
```

(a) FRIS.

```
[Rules]
1 0 0, 3 (1) : 1
2 3 3, 1 (1) : 1
2 2 3, 2 (1) : 1
2 1 3, 2 (1) : 1
2 3 2, 2 (1) : 1
2 3 1, 2 (1) : 1
2 2 2, 2 (1) : 1
2 2 1, 3 (1) : 1
2 1 1, 3 (1) : 1
2 1 2, 3 (1) : 1
3 3 3, 1 (1) : 1
3 2 3, 1 (1) : 1
3 1 3, 2 (1) : 1
3 3 2, 1 (1) : 1
3 3 1, 2 (1) : 1
3 2 2, 2 (1) : 1
3 2 1, 2 (1) : 1
3 1 1, 3 (1) : 1
3 1 2, 2 (1) : 1
```

(b) Inference Rules.

Figure 3. *FRIS* Code and Inference Rules for *MatLab* and GNU Octave. In This Context, in (b), 1 is *Low*, 2 is *Medium*, and 3 is *High*. Thus, in general, the three numbers before the comma represent the antecedents of the rule, while the number after the comma represents the consequent, or conclusion, of the rule.

As previously mentioned, *scripts* automatically generated inputs and outputs in *FRIS*. That is, five thousand entries were generated. However, Table 5 only displays the first ten entries. Thus, to demonstrate the operation and applicability of *FRIS*, the *Linguistic Values (LVs)*: (69.642, 68.389, 49.512) were selected, extracted from Table 5 line 6. These values correspond to the $\{SP, S, P\}$ variables. Consequently, the activated rules were the following: 5, 7, 14, and 16, Table 1. In this context, after calculating *SR* (e.g., in *Gnu Octave*), with the defuzzification methods *Centroid* and *MoM*, the values of *SR* are as shown in Figures 4 and 5:

```
Linguistics Variables (SP, S and P):

Risk Security (Centroid), SR = 37.941
>>
```

Figure 4. Defuzzification with Centroid.

```
Linguistics Variables (SP, S and P):

Risk Security (MoM), SR = 50
>>
```

Figure 5. Defuzzification with MoM.

Figures 4 and 5 show the Security Risk (SR) generated using two different defuzzification methods: centroid and MoM. The tool used to extract the SR was *Gnu Octave*, running on the Linux Mint 21 operating system.

Table 5. FRIS Tests in *MatLab* and Octave.

Inputs			Output Centroid (SR)		Output MoM (SR)	
SP	S	P	*MatLab*	Octave	*MatLab*	Octave
14.977	72.953	39.520	87.000	86.671	100.000	100.000
13.524	23.945	64.813	87.000	86.671	100.000	100.000
57.719	4.0320	70.259	63.142	62.877	50.000	50.000
27.922	79.766	34.692	85.435	85.169	92.500	92.424
45.737	87.691	93.276	13.547	13.830	4.000	4.0404
69.642	68.389	49.512	37.696	37.945	50.000	50.000
19.053	46.688	61.999	87.000	86.671	100.000	100.000
38.060	9.7400	17.072	83.948	83.692	88.500	88.383
57.060	71.371	1.3090	61.654	61.416	50.000	50.000
42.567	55.809	59.000	50.000	50.000	50.000	50.000

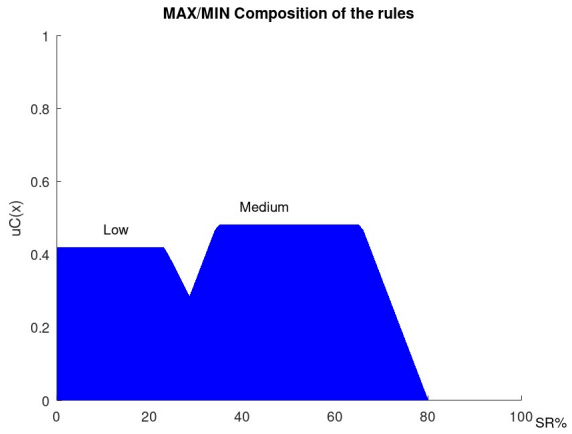
This example corresponds to the application of Equation 4 for the composition of the consequents of the rules, also known as the method of *Mamdani*. Therefore, the graphical representation of the composition of the activated rules can be seen in Figure 6(a).

This figure illustrates the universe set constituted by the outputs of *FRIS* for rules 5, 7, 14, and 16. For example, when performing a manual calculation, with the values *69.642, 68.389, 49.512*, and using the defuzzification method of *Cen-*

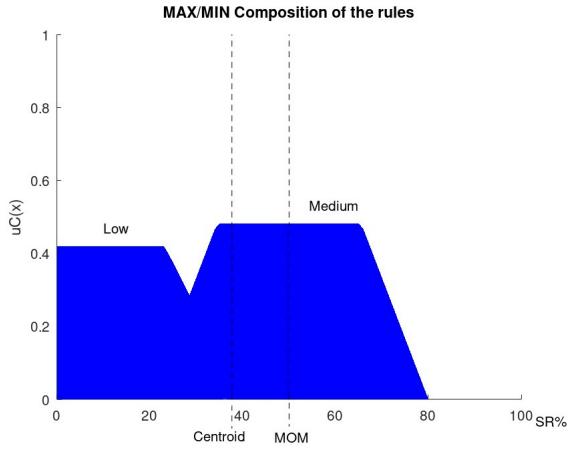
troid, the measure is as follows:

$$Centroid = \frac{(0.420 \times 23) + (0.482 \times 50)}{0.420 + 0.482} = 37.42 \quad (7)$$

Thus, the graphical representation of *SR* is as shown in Figure 6(b).



(a) Composition without the Security Risk.



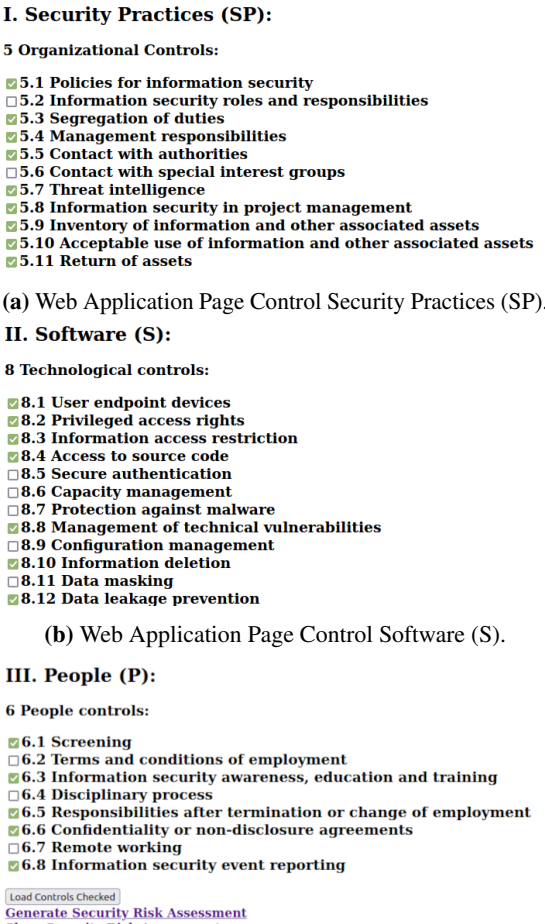
(b) Composition with Security Risk.

Figure 6. Defuzzification with Centroid and MoM Methods.

Thus, if this example were based on a real organization, it would have a *Low Security Risk*, in the case of the *Centroid* method and *Medium* with the *MoM* method.

4. Results and Discussion

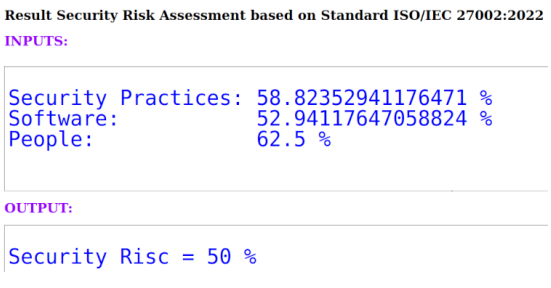
As discussed in Section 3.3, our proposal (*FRIS/FSRA*) was calibrated using a *Shell Script* that generated random values for the Linguistic Variables (SP, S, and P), totaling five thousand different values. These automatically generated values (see Table 5) served as input for *FRIS*, implemented in *MATLAB* code (Figure 3). *FRIS* was executed with these inputs to adjust the membership curves (Figure 2(a)(b)(c)(d)), ensuring optimal results, such as for the Linguistic Variable *SR*. To facilitate the use of our proposal, we developed a *web* application (Figure 7(a)(b)(c)(d)) allowing the Chief Information Security Officer (*CISO*) to visually indicate compliance with sub-items of *FSRA* controls according to *ISO/IEC 27002:2022*. After marking all relevant sub-items, the CISO can click the *Load Control Checked* button (Figure 7(c)) to incorporate these into *FRIS*. Subsequently, the *CISO* generates the Security Risk by clicking the *Generate Security Risk Assessment* link, followed by viewing the results through the *Show Security Risk Assessment* link (Figure 7(c)), which opens a new *web* page displaying percentages for each marked control (SP, S, and P) and the resulting Security Risk (*SR*), Figure 7(d).



(a) Web Application Page Control Security Practices (SP).

(b) Web Application Page Control Software (S).

(c) Web Application Page Control People (P).



(d) Web Application Page Show Security Risk (SR).

Figure 7. Graphical User Interface FRIS/FSRA.

Instructions for installing and using the application are

available at *GuitHub*[7]. In this context, Figure 7, is only illustrative, that is, not all sub-items of the controls that must be marked appear. Furthermore, to validate our proposal in a production environment, it was tested in a company with more than a thousand IT users. Thus, *CISO* had access to the application (e.g., via *GitHub*) and performed a test obtaining the following score: *Security Practices (SP)⟶ 64.71%*, *Software (S)⟶ 47.1%*, *People (P)⟶ 0.0%*, and *Security Risk (SR)⟶ 69,128%*. As a result, this company, due to not complying with certain sub-items of *FSRA* controls, has a 69,128% chance of suffering a cyber attack on its IT system. The results can be seen as shown in Figure 8.

Result Security Risk Assessment based on Standard ISO/IEC 27002:2022

INPUTS:

```
Security Practices: 64.70588235294117 %
Software:           47.05882352941176 %
People:             0 %
```

OUTPUT:

```
Security Risc = 69.128 %
```

Figure 8. FRIS Test Result Applied.

However, due to confidentiality reasons, the name of the company was not disclosed. Thus, if the reader wants to know the details of the test, they must contact *CISO* at this email guerra.ata@gmail.com. Therefore, as shown by Figure 8 the *CISO* can now take specific actions to mitigate the company's weaknesses and, in this way, reduce the security risk the company finds itself in due to not complying with certain *ISO/IEC 27002:2022* controls. Furthermore, we compared our proposal with *FEMRA* [8]. The choice of *FEMRA* is because it is structurally very similar to this proposal. Consequently, this comparison took into account the following criteria: **(i)** the number of membership curves; **(ii)** the number of *FRIS/FEMRA* input subitems; **(iii)** the number of experts consulted; **(iv)** the number of inference rules created; and **(v)** results.

(i): Regarding the membership curves, both our proposal and *FEMRA* have the same quantity. That is, *FRIS* has four membership curves (Figure 2(a)(b)(c)(d)) with three *fuzzy* sets each (e.g., *Low*, *Medium*, and *High*). For example, curves ⇒ *Security Practices (SP)*, *Software (S)*, *People (P)*, and *Security Risk (SR)*. *FEMRA* has the following curves ⇒ *Threat Effect*, *Vulnerability Effect*, *Asset Value*, and *Risk Assessment*;

(ii): *FRIS* has 93 subitems of four *ISO/IEC 27002:2022* [17] controls (e.g., 5. Organizational Controls, 6. People controls, 7. Physical controls, and 8. Technological controls), while *FEMRA* has one hundred and eighteen sub-items of five controls/domains based on the Zachman Framework [20] (e.g., Business View, Logical View (Software), Logical View (Data), Logical View (Network), and Physical View);

(iii): To develop *FRIS*, only one expert with extensive experience in cybersecurity, *web application*, and *software* was consulted. In addition, the expert consulted is also a member of the *Open Web Application Security Project (OWASP)*[8] and a security analyst at the Public Ministry of the State of Mato Grosso[9]. On the other hand, the *FEMRA* article refers to the consultation of three experts, for example, an expert in *software*, an expert in *computer network assets*, and an expert in *web applications*;

(iv): *FRIS* has nineteen inference rules (Table 5) as explained in Section 3 Subsection 3.2. On the other hand, *FEMRA* has eleven inference rules, for example, there are rules with one[10], two[11], and up to three[12] predicates. It is observed, based on the inference rules, that the most important Linguistic Variable of *FEMRA* is *Threat_Effect* and this is equivalent to the Linguistic Variable *Security Practices* of *FRIS*. Furthermore, in the article there is no explanation of how the authors arrived at the number of eleven inference rules;

(v): A test was carried out to compare the results between our proposal and *FEMRA*. To carry out the test, we made an equivalence between the Linguistic Variables, for example, we equated *Security Practices* with *Threat Effect*, *Software* with *Vulnerability Effect*, and *People* with *Asset Value*. After that, we use the input values from *FEMRA* (as described in [8], pg. 6) as input to *FRIS*. However, *FEMRA* has two linguistic variables that have different value ranges, for example, from zero (0) to nine (9), while the equivalent variables in *FRIS* are zero (0) to one hundred (100). So, to solve this problem we made a rule of three to find the corresponding value for the linguistic variables of *FRIS*. For example, if the input value of the *FEMRA Asset Value* linguistic variable is *6.92*, then the corresponding value for the *FRIS People* linguistic variable will be *76.89*. Furthermore, another issue that must be taken into consideration is the fact that the linguistic variables of *FEMRA Threat Effect* and *Vulnerability Effect* have values inversely proportional to the corresponding variables of *FRIS*. That is, if the variables in *FEMRA* reach their maximum values, their corresponding variables

[7] https://github.com/dioxfile/FSRA-FRIS

[8] https://owasp.org/.

[9] https://mpmt.mp.br/.

[10] *Rule 1: if (Threat_Effect = Low) then Risk_Effect = Low* [8].

[11] *Rule 5: if (Threat_Effect = High and Asset_Value = Low) then Risk_Effect = Medium* [8].

[12] *Rule 11: if (Threat_Effect = High and Vulnerability_Effect = High and Asset_Value = High) then Risk_Effect = High* [8].

in *FRIS* will have their minimum values. Therefore, we use the following criterion, if the Linguistic Variable in *FEMRA Vulnerability Effect* is filled with the value 91.66 then the value of its equivalent in *FRIS* will be $100 - 91.66 = 8.34$. In this context, we apply the same criteria to the linguistic variable *Threat Effect* and its equivalent *Security Practices*. Table 6 presents the values of each linguistic variable in *FRIS* and *FEMRA*.

Therefore, when evaluating the results of Table 6 it is possible to observe that most of the values resulting from both proposals are very close except for lines 3, 4, and 5 in which *FRIS* has a *Security Risk Medium* between 40.2% and 50% and *FEMRA* has a *Risk Assessment Medium* between 18.3% and 19.2%. This is because *FEMRA*'s membership curve considers that the *Medium* value ranges from zero to one hundred and, in this context, any value above zero and less than one hundred will also be *Medium*, with a lesser or greater degree of pertinence. Therefore, ***pertinence*** is close to 40% in *Medium* and below 70% in *Low*. On the other hand, in *FRIS* it is only *Medium* with ***pertinence*** between 75% and 100%. Furthermore, as shown in Table 6 the consequent of *FRIS* (e.g., Security Risk) is in a single set *fuzzy*, that is, it is either *Low* or *Medium* or *High*. However, the consequent of *FEMRA* is always in two sets *fuzzy*, either *Low* and *Medium* or *Medium* and *High*.

For this reason, the *FRIS*, integrated with *FSRA*, proved to be efficient and reliable in assessing information security risks, and its results were obtained taking into account several tests with different inputs (e.g., Table 5). Therefore, when performing a comparison between the defuzzification methods, *MoM* (Equation 5) and *Centroid* (Equation 6), it was observed that *Centroid* obtained more accurate values for security risk assessment when the organization complies with more than 60% of *FSRA*. On the other hand, *MoM* is most efficient when the organization complies with up to 40% of *FSRA*. For example, for extreme values, that is, the organization meets all 93 sub-items of the three controls ((SP) 100%, (S) 100%, and (P) (P) 100%)) or the organization does not meet any of the 93 sub-items of the three controls ((SP) 0%, (S) 0%, and (P) 0%)), there are the following security risks, respectively, 13.325% and 100%. Therefore, if the organization meets 100% *FSRA* it still has a 13.325% chance of suffering a security attack, the lowest rate. However, if the organization does not comply with *FSRA*, the risk of suffering an attack is inevitable, 100%.

In the other *FRIS* test situations, for example, *FSRA* compliance values above 40% up to 60%, the two defuzzification methods had similar results, and both one and the other can be used to calculate the security risk. It can be observed in Table 5[13], which demonstrates the variation of the outputs obtained by the defuzzification methods *Centroid* and *MoM*. For example, the values of the input parameters **SP = 42,567%**, **S = 55,809%**, and **P = 59,000%** (e.g., Table 5 line 10) resulted in the following security risk, **50**%, using the methods *Centroid* and *MoM*. Therefore, these results highlight the usefulness of integrating *FRIS* with *FSRA* for accurately assessing security risks. In this context, *FRIS* provides flexibility when using different defuzzification methods, adapting to the input parameters' specific characteristics. Additionally, it is important to emphasize that, during the inference of *FRIS*, the **SP** variable was prioritized, which represents the most important security control of *framework*. Therefore, when *FRIS* receives values below 40% for this variable, the *MoM* method defuzzification the output, taking advantage of its greater sensitivity. In addition, *FRIS* can be used in conjunction with other assessment methods such as: *Qualitative Risk Analysis* [21]; *Scenario-Based Risk Assessment* [22]; *Asset-Based Risk Assessment* [16], *FEMRA* [8], and *Risk Matrix* [23].

Therefore, the use of *FSRA/FRIS* does not guarantee complete security against cyber threats for the organization. However, it significantly simplifies the task of enhancing cybersecurity.

4.1 Proposal Contributions

The main contributions of our proposal are: **(1)** it's based on the ISO/IEC 27002:2022 standard, the most recent; **(2)** it presents a framework, FSRA, which contains the minimum security requirements that an organization must comply with; **(3)** the proposed fuzzy inference system, FRIS, uses two defuzzification methods, centroid and Maximum Average (MoM), which adds greater accuracy to our proposal; **(4)** the main contribution of FRIS is the representation of each control in the FSRA as a numeric value. Thus, when the *CISO* uses our proposal, it is possible to know what level of cybersecurity risk the organization is at and, therefore, check which FSRA security controls are not being complied with by the organization. This way, the security analyst will know where to act and how to act; **(5)** a *web* application is made available that can help the security analyst to mitigate the organization's weaknesses related to non-compliance with ISO/IEC 27002:2022 security controls, link: https://github.com/dioxfile/FSRA-FRIS.

4.2 Proposal Limitations

The main limitations of our proposal are: **(1)** even if all security controls are met, this does not guarantee that the organization is one hundred percent safe against cyberattacks. That is, our approach is just an aid tool to help security analysts mitigate cyberattacks and not a definitive solution; **(2)** our approach uses only one fuzzy inference system, different from the proposal described in [9] which uses two FIS and can, as a result, obtain better outcomes; **(3)** fuzzy logic is a very efficient tool for assessing cybersecurity risks. However, it provides many compositions and defuzzification methods. Consequently, as we have not tested all the possibilities that fuzzy logic can offer, we cannot guarantee that our choice of FIS is the most appropriate; **(4)** the *web* application should only be managed by an information security expert (*CISO*) familiar with *ISO/IEC 27002:2022* controls. Only such an expert can accurately assess and interpret the results, knowing precisely where and how to intervene based on the analysis.

[13]Test results, as well as code used in *MatLab* and *GNU Octave*, are available on *GitHub*: https://github.com/dioxfile/FSRA-FRIS.

Table 6. Comparison of Security Risk Analysis between FRIS and FEMRA.

Inputs FRIS			Inputs FEMRA			Output FRIS (SR)	Output FEMRA (RA)
SP [0-100]	S [0-100]	P [0-100]	Threat Effect [0-9]	Vulnerability Effect [0-100]	Asset Value [0-9]	Security Risk [0-100]	Risk Assessment [0-100]
23.11	8.34	76.88	6.92	91.66	6.92	86.4 (High)	83.6 (Medium/High)
16.00	55.34	100.00	7.56	44.66	9.00	86.7 (High)	83.6 (Medium/High)
46.66	55.34	100.00	4.80	44.66	9.00	50.0 (Medium)	18.3 (Low/Medium)
65.77	50.00	100.00	3.08	50.00	9.00	40.2 (Medium)	18.8 (Low/Medium)
44.44	50.00	100.00	5.00	50.00	9.00	50.0 (Medium)	19.2 (Low/Medium)
44.44	40.00	100.00	5.00	60.00	9.00	50.0 (Medium)	45.6 (Low/Medium)
39.11	36.67	60.44	5.48	63.33	5.44	55.8 (Medium)	57.1 (Medium/High)
70.22	26.67	55.55	2.68	73.33	5.00	50.0 (Medium)	46.0 (Low/Medium)
67.55	20.00	100.00	2.92	80.00	9.00	50.0 (Medium)	48.7 (Low/Medium)
23.11	20.00	100.00	6.92	80.00	9.00	86.4 (High)	83.7 (Medium/High)

Author Contributions

The authors contributed as follows: Diógenes Antonio Marques José developed the *Fuzzy Logic* models, worked on writing the article, and developed the *web application* to test the proposal; Douglas Schmitz Dupski worked on the testing and building *FRIS GitHub*; and Kembolle Amilkar developed the role of specialist consultant in Cybersecurity and *ISO/IEC 27002:2022* for the construction of *FRIS*.

5. Conclusions

This work addressed the current cybersecurity scenario and proposed a *framework (FSRA)* that helps to estimate security risks in organizations, based on *ISO/IEC 27002:2022*. The security risk here is the possibility of the organization suffering a cyberattack. Therefore, a *Fuzzy Risk Inference System (FRIS)* was presented capable of assessing the level of compliance of companies concerning compliance with the security policies of controls *Security Practices (SP)*, *Software (S)*, and *People (P)* of the *FSRA*, which has 93 sub-items to be fulfilled. In this context, the importance of the *ISO/IEC 27002:2022* standard was highlighted, which provides practical guidelines for implementing and managing crucial security policies for using *IT* resources in organizations. Thus, the main contributions of this work were: the creation of a security framework based on the ISO/IEC 27002:2022 standard; and the use of two defuzzification methods, for example, *Centroid* and *MoM*. This mix of the two defuzzification methods improves the sensitivity of *FRIS* when assessing the organization's security risk.

Furthermore, the *FRIS* proposed is composed of 19 inference rules based on expert knowledge, for instance: Security Practices (*SP*), Software (*S*), and People (*P*). Consequently, the *Security Risk (SR)* is the output of the system. Thus, *SR* indicates that the company faces three levels of Security Risk (*Low*, *Medium*, and *High*), with *Low* corresponding to approximately 13% (even if the company complies with all recommended controls, there remains a residual security risk), *Medium* ranging from 40% to 59.99%, and *High* from 60% to 100%. In addition, with these results in hand, the security analyst can improve the organization's security policies by increasing the organization's compliance rate in complying with *ISO/IEC 27002:2022*.

This study opened up a range of possibilities for future research. An important direction is to expand this proposal to cover all *ISO/IEC 27002:2022* controls. It would allow for a more comprehensive risk assessment, leveraging expert knowledge and fuzzy logic to more effectively and accurately infer risks. In addition, another key future objective is to improve compatibility between different platforms used in information security risk assessment. This advance may provide a more fluent integration of the methods presented in this study with already established systems[14].

References

[1] OGLIH, V.; PATOKA, H. Formation of information security system under conditions of uncertainty of influence of destabilization factors on the basis of neurofacle networks. *Economic Scope*, 2022. Disponível em: <https://journals.indexcopernicus.com/search/article?articleId=3637567>.

[2] Fortinet. *Fortinet relata que a América Latina foi alvo de mais de 360 bilhões de tentativas de ataques cibernéticos em 2022*. 2023. Available in: <https://t.ly/nQoIG>.

[3] MATHEW, D. A. R. Cyberbiosecurity as the foremost biological weapon to the digital world. *International Research Journal of Innovations in Engineering and Technology*, 2022. Disponível em: <https://irjiet.com/common_src/article_file/1644220918_e9b80512a6_6_irjiet.pdf>.

[4] HSIEH, M.-Y.; HSU, Y.-C.; LIN, C.-T. Risk assessment in new software development projects at the front end: a fuzzy logic approach. *Journal of Ambient Intelligence and Humanized Computing*, Springer, v. 9, p. 295–305, 2018. Disponível em: <https://link.springer.com/article/10.1007/s12652-016-0372-5>.

[5] KURE, H. *An Integrated Cybersecurity Risk Management (I-Csrm) Framework for Critical Infrastructure Protection*. Tese (Doutorado) — University of East London, 2021. Disponível em: <https://repository.uel.ac.uk/item/89ww3>.

[6] NEWCOMB, E. A.; HAMMELL, R. Fluf: Fuzzy logic utility framework to support computer network defense decision making. p. 1–6, 2016. Disponível em: <https://ieeexplore.ieee.org/document/7851582>.

[7] ZADEH, L. Fuzzy sets. *Information and Control*, v. 8, n. 3, p. 338–353, 1965. ISSN 0019-9958. Disponível

[14] https://cybersecuritynews.com/cybersecurity-risk-management-tools/.

em: <https://www.sciencedirect.com/science/article/pii/S001999586590241X>.

[8] SENDI, A. S. et al. Femra Fuzzy expert model for risk assessment. *IEEE*, p. 48–53, 2010. Disponível em: <https://ieeexplore.ieee.org/document/5476890>.

[9] ALALI, M. et al. Improving risk assessment model of cyber security using fuzzy logic inference system. *Computers & Security*, Elsevier, v. 74, p. 323–339, 2018. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0167404817302006>.

[10] OTERO, A. R. et al. A fuzzy logic-based information security control assessment for organizations. *IEEE*, p. 1–6, 2012. Disponível em: <https://ieeexplore.ieee.org/document/6417640>.

[11] OTHMAN, N. A. A.; ALI, F. H. M.; LATIF, N. A. Risk assessment for cisco pix-525 firewall: Fuzzy logic approach. *IEEE*, p. 65–69, 2013. Disponível em: <https://ieeexplore.ieee.org/document/6836549>.

[12] SHREEVE, B. Making sense of the unknown: How managers make cyber security decisions. *ACM Transactions on Software Engineering and Methodology*, v. 32, 2022. Disponível em: <https://dl.acm.org/doi/10.1145/3548682>.

[13] ROCHA, H. O. d. Principais ameaças de segurança encontradas no ambiente virtual nas organizações. *Ministério da Justiça e Segurança Pública do Brasil*, 2022. Disponível em: <http://dspace.mj.gov.br/handle/1/9920>.

[14] CLARA, A. M. C. Verificação de conformidade regulatória dos processos de governança de ti: um estudo de caso de uma empresa pública. *Universidade de Brasília - Biblioteca Central*, 2017. Disponível em: <https://repositorio.unb.br/handle/10482/32060>.

[15] Programa de Privacidade e Segurança da Informação (PPSI). *Guia do Framework de Privacidade e Segurança da Informação*. 2022. Brasília, novembro de 2022. v 1.1 . Disponível em: <https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ppsi/guia_framework_psi.pdf>.

[16] (PPSI), P. de Privacidade e Segurança da I. *Política de Gestão de Ativos*. 2023. Brasília, março de 2023. v 2.2. Disponível em: <https://t.ly/Dnkpw>.

[17] International Organization for Standardization. *ISO/IEC 27002: Information technology - Security techniques - Code of practice for information security controls*. Geneva, 2013. Disponível em: <https://www.iso.org/standard/54533.html>.

[18] JOSé, D. A. M. et al. Olsr fuzzy cost (olsr-fc): an extension to olsr protocol based on fuzzy logic and applied to avoid selfish nodes. *Revista de Informática Teórica e Aplicada*, v. 26, n. 1, p. 60, 2019. ISSN 0103-4308. Disponível em: <https://seer.ufrgs.br/rita/article/view/RITA-VOL26-NR1-60>.

[19] SILER, W.; BUCKLEY, J. J. *Fuzzy Expert Systems and Fuzzy Reasoning*. Hoboken, New Jersey: John Wiley & Sons, Inc., 2005. Disponível em: <https://cdn.preterhuman.net/texts/science_and_technology/artificial_intelligence/Fuzzy%20Expert%20Systems%20and%20Fuzzy%20Reasoning%20-%20William%20Siler.pdf>.

[20] John A. Zachman. *Zachman Framework*. 2008. Available in: <https://zachman-feac.com/zachman/about-the-zachman-framework>. Acesso em: 18 jun. 2024.

[21] ROSS, R. *Guide for Conducting Risk Assessments*. Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD, 2012. Disponível em: <https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final>.

[22] ISO; IEC. *ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection — Guidance on managing information security risks*. 2022. Disponível em: <https://www.iso.org/obp/ui/#iso:std:iso-iec:27005:ed-4:v1:en>.

[23] SUDOSKI, B. S. et al. Um estudo de caso de desenvolvimento de políticas de segurança da informação, com base nas normas abnt nbr iso/iec: 27000, para uma instituição de soluções tecnológicas. *Repositório Institucional da UFSC*, Florianópolis, SC, 2018. Disponível em: <https://repositorio.ufsc.br/handle/123456789/192167>.