Computers & Security 157 (2025) 104584

Contents lists available at ScienceDirect

Computers & Security

journal homepage: www.elsevier.com/locate/cose

Full Length Article

Enhancing cybersecurity in the judiciary: Integrating additional controls into the CIS framework

Renato Solimar Alves [a], Jady Pamella Barbacena da Silva [a], Luiz Antonio Ribeiro Junior [a,c], Rafael Rabelo Nunes [a,b,d,*]

[a] Professional Postgraduate Program in Electrical Engineering (PPEE), Department of Electrical Engineering, College of Technology, University of Brasília (UNB), Brasília 70910-900, Federal District, Brazil
[b] Faculty of Economics, Administration, Accounting, and Public Policy Management, Department of Administration, University of Brasília (UNB), Brasília 70910-900, Federal District, Brazil
[c] Computational Materials Laboratory, Computational Materials Science Laboratory (LCCMat), Institute of Physics, University of Brasilia (UNB), Brasília 70910-900, Federal District, Brazil
[d] UniAtenas University Center, Paracatu 38602-018, Minas Gerais, Brazil

ARTICLE INFO

Keywords:
Critical security controls
Cybersecurity measures
Data protection
Information security management
Judicial system security
Operational risk management
Threat mitigation
Strategies
Tailoring

ABSTRACT

The Judiciary faces considerable challenges protecting its critical operations from cyber threats in an increasingly digital and vulnerable landscape. This article explores the need to enhance information security practices beyond basic security controls to address operational and technological risks targeting the Judiciary. Intending to propose an expansion of the security controls suggested by the CIS Controls framework, this article focuses on critical areas such as information security management, personnel management, and technological requirements specific to the judicial context. Through qualitative analysis and consultations with experts in the field, preventive and corrective measures were identified, encompassing effective communication practices, mental health programs, and a strong culture of integrity complemented by advanced cybersecurity technologies. The results highlight the need for additional, comprehensive controls ranging from physical security to digital protection, promoting an integrated approach to risk management. The contributions of this article extend to establishing a strengthened foundation for security controls, creating a more effective defense mechanism against emerging threats, and ensuring the sustainability and efficiency of court operations. This article contributes to the evolution of security strategies in the Judiciary, with direct practical implications for risk mitigation and the protection of information assets. The work contributes to the debate on information security in the Judiciary and how to adapt and expand the application of the CIS framework.

1. Introduction

The Judiciary plays a fundamental role in social stability and harmony, ranging from the control of constitutionality and legality, the administration of judicial deposits and precatory payments to the management of the electoral process in Brazil (Alves, 2024; Amaral, 2020).

With the constant handling of confidential information from individuals and organizations (Rast, 2023), robust strategies are needed to protect this sensitive data from potential attackers.

The evolution of the judicial system has been driven by the adoption of digital technologies in court proceedings, resulting in greater procedural speed and efficiency in the provision of judicial services (Hino and Cunha, 2020; Eltis, 2011; do Carmo Martins, 2021). The COVID-19 pandemic has accelerated this technological transformation, intensifying the adoption of innovations such as videoconferencing, virtual hearings, and electronic customer service (do Carmo Martins, 2021; Conselho Nacional de Justiça (CNJ) 2032).

While computerization has brought undeniable benefits, it has also introduced additional complexities and potential vulnerabilities that require careful management (Moreira et al., 2021). The increased digitization of the judiciary has also increased exposure to cyber-attacks, with worrying records of successful attacks (E. Reina, 2022; Ciso Advisor, 2022).

* Corresponding author.
E-mail address: rafaelrabelo@unb.br (R.R. Nunes).

https://doi.org/10.1016/j.cose.2025.104584
Received 18 March 2025; Received in revised form 10 June 2025; Accepted 23 June 2025
Available online 25 June 2025

This concern about information security risks goes beyond Brazilian borders, with judicial leaders in the United States highlighting the importance of modernizing the judiciary's computer systems to face cyber threats (Raymond, 2022).

Faced with this reality, it is necessary to guarantee a high level of cyber security as an essential measure to protect not only information but also the integrity of and trust in justice (Moura and Borges, 2022; E. Reina, 2022; Hirata and de Oliveira, 2020). Therefore, judicial bodies must adopt a proactive and strategic approach to mitigating risks by implementing rigorous information and data protection measures (Rast, 2023; Alves et al., 2023).

In this context, the risk assessment process emerges as a tool for identifying, evaluating, and prioritizing the treatment of risks, followed by the development of concrete control strategies to keep risks at acceptable levels (ABNT 2018; Nunes et al., 2021; Lima et al., 2022; Project Management Institute, Inc. (PMI) 2021; Galegale et al., 2017).

The CIS Controls v8 framework offers a comprehensive set of cybersecurity controls that have been used as a reference for the Brazilian judiciary. Still, it is essential to adapt these controls to the specific needs of the Judiciary, which has not been done (Alves, 2024; Conselho Nacional de Justiça (CNJ) 2021). Therefore, this article proposes a baseline of additional security controls aligned with the risks of the Judiciary ecosystem, avoiding the application of generic frameworks that are not aligned with the specificities of this sector (Barnard and Von Solms, 2000).

This article is structured as follows: Section 2 discusses the articles that inspired identifying risk controls specific to the Judiciary, highlighting the importance of an integrated approach covering everything from physical security to cyber protection.

Section 3 then discusses the methodology used to identify the risks related to the activities of the judiciary and survey frameworks and applicable security measures. It then details the process of analysis and categorization of the data obtained.

Section 4 presents the identified business and operational risks and discusses the proposed mitigating controls, highlighting the need for specific preventive and corrective measures.

Section 5 presents the analysis of the results and offers the concluding remarks. It also outlines possible directions for future research in the field of information security within the Judiciary context.

2. Related work

Rover (2015) quantitatively analyzed scientific publications in judicial administration, electronic case processing, and information security, finding that electronic justice is not widely covered in highly relevant journals.

Wanderley (2020) developed a model and created tools to support information security risk management in the Tocantins Court of Justice, carrying out a case study in a data center environment to test the proposed model.

Machado (2018) used an analogy with the banking sector and the Central Bank of Brazil's implementation of the "Basel II" categorization of operational risks to create a taxonomy to classify operational risks in the Judiciary and to establish a common language between bodies to identify and classify these risks.

Barrêto (2021) investigated the implementation of security processes, the formation of the Security Management Committee and the Information Security Policy in the context of the Court of Justice of the State of Tocantins, using the ABNT NBR ISO/IEC 27,002 standard as a tool to identify and analyze the processes incorporated into the Information Security Policy and to assess the level of maturity in information security.

Schwaitzer (2016) focused on ensuring the confidentiality, integrity, and availability of digital archival information generated by the Judiciary, pointing to protection against undue exposure, unauthorized alterations, and premature obsolescence as the main difficulties. The study concludes that the absence of an integrated approach to information security, access, and preservation is a significant problem, highlighting the need to classify information based on its value and legal requirements to mitigate risks and ensure access to information.

Internationally, the "Comitê Conjunto de Tecnologia" (JTC), the "Conferência de Administradores de Tribunais de Justiça Estaduais" (COSCA), the "Associação Nacional de Gestão de Tribunais" (NACM), and the "Centro Nacional de Tribunais Estaduais" (NCSC) have developed a guide with recommendations for the preparation and prevention needed to respond effectively to cyber security incidents. Among the various best practices, the importance of anticipating the potential impact of loss or unauthorized alterations to essential data assets, such as court orders, witness identities, jurors, court recordings, financial transaction data, digital evidence, and personal information, is emphasized (Joint Technology Committee 2019).

Gordon (2020) highlight the importance of cyber security in protecting the judicial process, presenting principles and best practices such as developing robust cyber hygiene, protecting critical assets, drawing up incident communication and response plans, identifying threats based on risk-management specific to the judicial system and the use of cryptography, among others.

Rast (2023) addresses the cyber threats the judiciary and legal professionals face, including generative artificial intelligence, ransomware, phishing, social engineering, data leaks, insecure networks, weak passwords, malware, third-party vulnerabilities, and insider threats. He emphasizes the importance of identifying the causes of risks and conducting risk assessments to protect sensitive data such as court documents and personal information.

In addition, Rast (2023) recommends the adoption of robust security practices, staff training, and continuous monitoring, highlighting multi-factor authentication (MFA), VPNs, endpoint detection and response (EDR) systems, encryption, and regular software updates. Additionally, it was noted that there are articles focused on conducting risk assessments in the specific context of the US criminal justice system, given the established practice of basing prisoner release decisions on risk assessments that consider the likelihood of recidivism. Therefore, decisions guided by risk assessments can be seen as more defensible and credible than more subjective and opaque decision-making processes (Bureau of Justice Assistance, 2023).

Despite these various contributions, no studies were identified that aimed to identify practically what the business or operational risks of the Judiciary's main activities might be, and there was also a gap in the investigation of specific information security controls that could be implemented to deal with risks in the Judiciary. It is with these surveys and the identification of additional security controls specific to the Judiciary that this article aims to contribute.

3. Method

The research was conducted in three phases, as shown in Fig. 1. Each has specific methodologies to address the challenges in mitigating business risks in the Judiciary.

The methodology chosen sought to propose risk mitigation measures applicable to all bodies of the Judiciary, avoiding revealing weaknesses

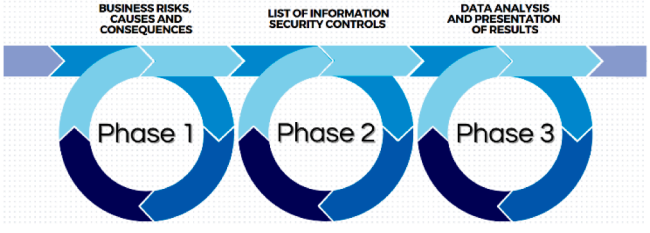


Fig. 1. Phases to identify the best information security controls to be adopted in the Judiciary ecosystem.

or risks specific to the institutions involved.

3.1. Phase 1

Phase 1 identified the primary business risks of the judiciary's core activities, the factors that could generate such risks, and the consequences that could be faced if the risk materialized. This was published in the article by Alves et al. "Judiciário sob ataque hacker: riscos de negócio para segurança cibernética em tribunais brasileiros" (Alves et al., 2023), published in the RISTI journal in 2023.

This phase began with a qualitative approach, carrying out extensive bibliographical research to identify the main activities of the judiciary and the associated risks based on historical events.

To identify business risks relevant to the Judiciary, semi-structured interviews were conducted with eight public managers who have extensive experience in various judicial institutions, including Superior and Regional Courts. The average professional experience among participants was approximately 20 years. Participants included four legal advisors to Supreme Court justices, three IT security managers, and one corporate risk officer.

Each interview followed a predefined script with open-ended questions aimed at exploring real-life situations and risk scenarios. Sessions began with a presentation of the study's objectives, an explanation of the interview structure, and a guarantee of confidentiality to foster candid responses. Contextual information on prominent cybersecurity incidents in the Judiciary, illustrated with media headlines, was provided to prompt reflection and discussion. Interview Questions:

Q1: In your opinion, is it relevant to identify business risks specific to the Judiciary? Why?
Q2: Do you think it is important to identify the potential causes and/or consequences of these risks? Why?
Q3: Have you witnessed any routine or event that, in your view, could represent a risk to the drafting or issuance of a judicial decision? If so, could you describe it?
Q4: Do you believe adequate controls are currently in place to mitigate such risks?
Q5: Based on a preliminary list of risks derived from real incidents, would you like to highlight any additional risks or indicate which ones you consider most critical?
Q6: Are the existing controls in your organization sufficient for handling such risks? Would you suggest any additional controls?

Although these questions were predefined, participants were encouraged to introduce new insights and perspectives freely. The interviews lasted between 90 and 120 min. No structured questionnaires were distributed; only the question set was shared upon scheduling.

Empirical saturation was observed after eight interviews, as answers became repetitive, and no new themes emerged. The collected data were analyzed using the Bow Tie method (ABNT NBR ISO/IEC 31,010), distinguishing causes, business risks, and consequences. Suggested mitigation measures from interviewees were recorded, although not yet addressed at this stage.

The research aimed to characterize the mandatory phases for the risk assessment process and the existence of previous articles identifying the business risks inherent in the Judiciary's core business (Alves et al., 2023).

Phase 1 of the study was completed by obtaining a list of the business risks related to the Judiciary's core activities, which events could cause the risks to materialize (causes), and what consequences could be observed in the event of the risk.

3.2. Phase 2

The objective of phase 2 was to survey the security measures that, if applied, could address the risks identified in the previous phase. This phase involved a more in-depth literature analysis of the most widely used information security frameworks.

A detailed analysis of the causes of the business risks was conducted, comparing them with the list of controls recommended by the security frameworks and the controls that could potentially reduce the probability of each risk occurring or the impact resulting from the materialization of the risk event were listed. Based on this assessment, a security framework was selected to determine the identified controls.

The answers given in the interviews were then reviewed, and the list of controls was supplemented with those proposed by the interviewees to deal with the identified risks. This procedure identified a preliminary set of controls applicable to each risk cause.

A focus group was set up to evaluate the results found. As described by Ribeiro et al. (2021), the focus group is a widely recognized qualitative data collection methodology used in research. This method involves bringing together a group of individuals with knowledge or experience of the topic. The focus group with experts aimed to enrich the study by providing a space for focused discussion, allowing the researcher to gain deeper insights into the participants' perceptions, feelings, and attitudes toward the topic.

The focus group comprised IT managers with significant experience in information security, cyber security, and risk management. These professionals work as managers in various Brazilian judicial institutions. Eight focus group sessions, lasting an average of two hours each, were held to evaluate and validate the controls identified in the preliminary analysis phase.

During these focus group sessions, it became apparent that although the CIS V8 framework was an extensive and robust guide, it did not fully cover some critical operational risks, particularly those not strictly linked to technological issues.

In these cases, the focus group members proposed additional or alternative controls, based on their assessments and experiences, to address the gaps concerning the causes of the identified business risks. In some cases, it was necessary to research additional sources and references from other security guides and standards indicated by the focus group members, which served as a basis for joint discussion of the practices identified and for forming group understandings.

The aim was to propose security measures to mitigate the risks identified that were not covered in the original structure of the framework used as a reference.

This phase was concluded by obtaining a list of controls by combining the controls indicated in the interviews with the preliminary analysis of the framework's controls and the qualitative insights provided by the focus group. This resulted in a more comprehensive risk treatment approach adapted to the specificities of judicial institutions.

3.3. Phase 3

Phase 3 sought to analyze the data obtained and look for ways to present the results to help the agencies define those responsible, priority actions, and improvements that could be pursued.

The aim was to categorize the original controls from the reference framework and those that were additionally proposed, classify the assets and security functions, and determine implementation priorities, ensuring that the results were presented in a clear and applicable way to guide priority actions and improvements.

By conducting a thorough review and analysis of the data collected and evaluating ways of classifying the information, it was possible to identify correlations and priority security measures.

Considering the large volume of information, it was necessary to establish Business Intelligence techniques to present, access, and interpret the data more naturally. For this purpose, the specialized software Power BI and Tableau were used.

Firstly, the security controls were grouped into different categories to understand better the nature or class of each security measure that could be applied.

Next, the types of assets associated with each control identified during the research were classified. This classification of assets proved necessary to serve as a basis for guidance, identify those responsible for implementing the controls, and standardize the information on each control since the chosen framework already implements this classification in its recommended controls.

It was also necessary to classify the additional security controls to the standard of the security functions used by the reference guide. The categorization process also determined the priorities for implementing controls, following the same procedure used to classify the implementation groups (IG1, IG2, and IG3).

The implementation groups are classified into IG1, IG2, and IG3 based on factors such as the complexity of the security measures, the organization's size, and its specific security needs (Stocchetti and Sager, 2023).

Implementing the controls in Implementation Group 1 (IG1) is recommended, as they are more straightforward and less costly, which is essential for implementing more complex measures.

Finally, the results obtained were interpreted and compared with the concepts in the literature and reviews of previous studies to understand what the data represented and how they could be applied to validate the reliability of the results (Conselho Nacional de Justiça 2021).

The methodology adopted sought to propose guidelines for risk mitigation that all the bodies of the Judiciary could use without exposing weaknesses or risks specific to the institutions involved in the various stages of the article.

4. Identification of risks

A comprehensive and detailed analysis of operational risks specific to the Judiciary was carried out, identifying areas not covered by CIS Controls v8.

The results will be presented in order of discovery and classification to demonstrate the need for the additional controls proposed in the article.

4.1. Identifying the main activities of the judiciary

In the judiciary, several essential axes are necessary for the functioning of the judicial system. These involve filing, processing, drafting orders and decisions, and distribution. These activities are observed at all levels of the judicial system.

Table 1 (Alves et al., 2023) lists the grouping of actions that cover all judicial institutions and are fundamental to the final activity of the Judiciary.

4.2. Identification of business risks

Based on the Phase 1 interview, approximately 110 potential business risks associated with the Judiciary were cataloged. However, there was a need to conduct a more thorough assessment to determine more precisely which of these were actual risks.

After completing the phases of data collection through interviews, systematic organization of information, critical evaluation of the elements identified as risks, causes, and consequences, and review by focus group, it was possible to identify and list ten essential risks of business pertinent to the context of the Judiciary.

These risks are listed in Table 2 (Alves et al., 2023).

Table 1
Main activities.

Id	Main Activities
1	Receiving and distributing cases
2	Analyzing and reporting on cases
3	Formulating Judicial Decisions
4	Monocratic or Collegiate Judgment
5	Processing Decisions
6	Execution of Registry Acts
7	Compliance with Orders and Decisions

Main activities of the Judiciary.

4.3. Identifying operational risks

Risks do not exist in isolation but must be understood about an organization's objectives. That said, a risk is only considered significant if it has the potential to adversely affect an activity considered critical to the organization (Crouhy et al., 2014).

In this way, risks that do not influence the desired results are considered irrelevant to an organization's risk analysis.

Considering the business risks identified in this article, it was necessary to understand the factors that can trigger these risks to mitigate them effectively.

Continuing the investigation, a detailed analysis of the potential causes or sources of risk was carried out, identifying operational risks.

This analysis resulted in Table 3, which lists the 40 causes identified for business risks, enabling a better understanding of how certain events can lead to these risks materializing.

Once business risks and the causes of these risks have been identified, it is necessary to understand the relationships between this information. The first analysis concerns understanding the types of existing risks and their categorizations.

The risks related to legal and regulatory uncertainties, strategic failures, and events leading to reputation damage can be grouped as business risks (Chapelle, 2018).

Operational risks are understood through various perspectives and contributions. According to Jallow et al. (2007), these risks are associated with direct and indirect losses resulting from ineffective or faulty internal processes, human errors, inadequate systems, or external events.

Chapelle (2018) defines operational risk in banking institutions as any risk that does not fit into the categories of credit or market, thus covering all non-financial aspects. This definition implies that, for a financial institution, operational risk encompasses elements not directly linked to its primary objectives or its sustainability in the competitive market.

Thus, this conception allows for the assimilation that business risk is associated with the institution's primary functions, while operational risk is related to support or auxiliary functions. This view can be extrapolated to other areas of activity, suggesting a facilitated understanding of operational risk and its relationship with business risk.

Drawing a parallel with the Judiciary, it is suggested that business risks are those intrinsically linked to the primary institutional mission of the justice bodies. A detailed analysis of the causes of business risks reveals that these are predominantly related to internal processes, human resources, and information systems.

Thus, the causes of business risks are operational risks that are closer and related to the dangers of the main activities of the Judiciary.

Table 2
Business risks.

Id	BUSINESS RISKS
1	Early disclosure of votes, rulings, or decisions
2	Leakage of confidential information, protected by secrecy or personal data
3	Unauthorized issuance or amendment of rulings or decisions
4	Interruption of court proceedings
5	Predictability or manipulation of the distribution of cases
6	Loss of information
7	Personal bias or favoritism
8	Unwanted or inappropriate matters in rulings and decisions
9	Legitimate judgments, but based on adulterated elements
10	Spying on other nations, criminal organizations, or illegal influence groups

Business risks of the judiciary.

Table 3
Operational risks.

Id	Operational Risks	Business Risks
1	Copying minutes or files onto personal computers and storage media	1, 2
2	Intentional leakage by people who have access to minutes or files (espionage)	1, 2, 10
3	Compromise of user access credentials	1, 2, 3, 8, 9, 10
4	Compromise of privileged credentials	1, 2, 3, 4, 5, 6, 8, 9, 10
5	Use of unprotected personal computers or insecure networks	1, 2, 3, 8, 9, 10
6	Improper disposal or loss of temporary documents (paper, CD, pen drive, etc.)	1, 2, 10
7	Unauthorized physical access	1, 2, 3, 4, 6, 10
8	Judicial system source code with security vulnerabilities	1, 2, 3, 4, 5, 6, 7, 8, 9, 10
9	Configuration failures in the technological infrastructure environment	1, 2, 3, 4, 5, 6, 7, 8, 9, 10
10	Excessive privileges in the system, where any user can have access to read the minutes	1, 2, 10
11	Cyber attacks or social engineering	1, 2, 3, 4, 5, 6, 7, 8, 9, 10
12	Sharing of decision-makers' passwords	1, 2, 3, 7, 8
13	Data hijacking attacks (double extortion ransomware)	1, 2, 4, 6, 10
14	Unavailability of key people	4, 6
15	Distributed denial of service (DDoS) attacks aimed at damaging the image of managers or authorities in (or tipped for) key positions	4, 7
16	Unavailability of critical systems or massive failures of storage structures due to IT infrastructure failures	4, 6
17	Weakness of the lottery algorithm	5, 7, 9
18	Modification of information in the supply chain (MPF, AGU, Caixa, etc.)	7, 9
19	Dependence on foreign hardware and software technology	4, 5, 6, 10
20	Hardware leaks or espionage	1, 2, 10
21	Distribution of electronic judicial systems, making it difficult to control the security of the source code	1, 2, 3, 5, 7, 10
22	Complexity of security control of all technological layers using foreign technologies (database, middleware, programming language, network, etc.)	2, 3, 5, 7, 10
23	Natural disasters	4, 6
24	Inadequate process for drafting or reviewing votes, decisions, or determinations	3, 7, 8, 9
25	Unavailability of human resources	1, 2, 3, 4, 5, 6, 8, 9, 10
26	Unavailability of material resources	1, 2, 3, 4, 5, 6, 7, 8, 9, 10
27	Business rule that provides for the same workload in each office, making the distribution of cases predictable	5, 7
28	Possibility of changing parties, procedural class, or initial petition after the case has been distributed	5, 7, 9
29	Filing the same lawsuit several times until the case is distributed to the desired judge, giving up on the other lawsuits	5, 7
30	Filing the same lawsuit in different jurisdictions (lis pendens)	5, 7
31	Excessive volume of lawsuits that compromise the response capacity of the courts (predatory litigation)	4, 7
32	Technical incapacity for highly complex matters	1, 2, 4, 5, 9, 10
33	Failure to verify the authenticity of external documents that are inserted into the process	7, 9
34	Intentional modification of information by people who have access to the file	7, 9
35	Influence peddling (judicial lobbying)	1, 2, 7, 10
36	Nepotism	7
37	Suspicion of cabinet members	1, 2, 3, 7, 9
38	Non-compliance with procedural deadlines	7, 9
39	Not knowing all the procedural documents necessary for analysis and judgment	7, 8, 9
40	Unauthorized use of generative AI tools to support the drafting of orders and decisions	2, 8

Operational risks, causes of business risks.

Consequently, it is reasonable to categorize the causes of business risks associated with core functions as operational risks originating from various sources.

Implementing appropriate information security controls is vital to mitigate these intermediate operational risks, directly influencing the business risks with a more significant potential impact.

Fig. 2 illustrates the proposed linkage between information security controls, operational risks that are causes of business risks, and the consequences.

Several risks involve deep issues about integrity and ethics. The Operational Risk of "Judicial system source code with security vulnerabilities" can result in the Business Risk of "Legitimate judgments, however, based on tampered elements."

The consequences of this Business Risk may be "Allocation of financial resources to individuals" and "Impact on the financial market and unfair monetary transactions."

The Operational Risk of "Configuration failures of the technological infrastructure environment" can generate the Business Risk of "Unauthorized issuance or authorization of determinations or decisions," and the consequences of "Damage to the reputation or image of the Judiciary" and "Accountability of public officials."

The operational risk of "Cyberattacks or social engineering" can result in the business risk of "Bias or personal favoritism" and the consequences of "Undermining trust in judicial institutions" and "Allocating financial resources to individuals."

Another example, now with the Operational Risk "Unavailability of material resources," can result in the Business Risk "Judgments, actions, and determinations may be issued late or erroneously" and the consequences "Impact on the financial framework and unfair monetary transactions" and "Accountability of public officials": Systemic failures that lead to delays or errors can also result in the accountability of the responsible managers.

Finally, the Operational Risk of "Compromise of user access credentials" can result in the Business Risk of "Unauthorized issuance or authorization of determinations or decisions," which can generate the consequences of "Damage to the reputation or image of the Judiciary" and "Accountability of public officials."

5. Risk control

The results of the first phase highlighted a wide range of operational risks, the business risks of the final processes of Justice, how the consequences could be faced, and the relationships between all these aspects.

Subsequently, developing an in-depth understanding of the

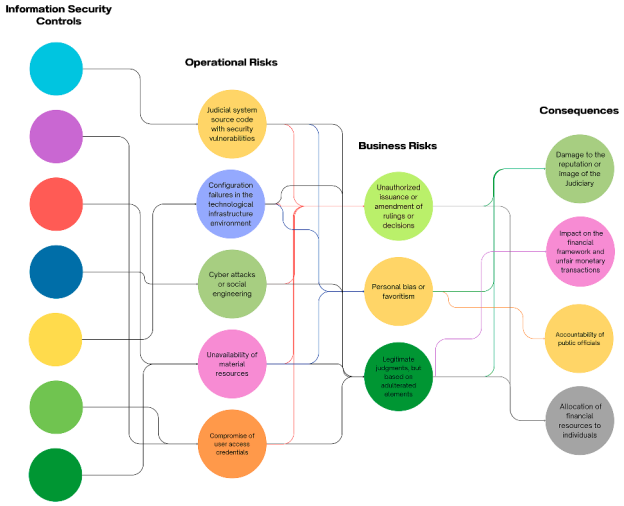


Fig. 2. Causes and consequences of a business risk.

strategies and measures to mitigate the identified risks was necessary. This included implementing preventive and compensatory controls, which are fundamental for effective risk management and strengthening organizational resilience in the face of threats. Applying these controls ensures that risk management is aligned with institutional strategies.

5.1. Controls of the framework

After thoroughly analyzing the various information security frameworks, the CIS Controls framework, in version 8, was defined as the reference for implementing security actions capable of adequately reducing the likelihood and impact of the identified risks.

The Critical Security Controls for Effective Cyber Defense, from the Center for Internet Security (CIS Controls), are priority actions for defense against pervasive cyber threats, i.e., those that easily spread or infiltrate computer systems. They are best cybersecurity practices that help protect organizations from the most common attacks (Lima et al., 2022; Sager and McClain, 2020).

The selection of the CIS Controls framework was based on various decisive factors. Initially, it is notable that CIS claims to adopt the Pareto principle by maximizing efficiency by implementing the most effective and relevant controls, thus avoiding a proliferation of potentially unnecessary measures (Sager and McClain, 2020).

This approach allows organizations to seek the highest level of security while avoiding an extensive number of controls, which could overload management and compromise security effectiveness.

In addition, the set of controls defined in the framework not only represents a compilation of best practices but is based on the expertise of CIS to identify and prioritize the most impactful security actions. Each control covers specific aspects, from vulnerability identification to incident response, thus providing a comprehensive framework to enhance the cyber resilience of organizations (Lima et al., 2022; Sager and McClain, 2020).

Moreover, the CIS Controls have been widely recognized and adopted as a reference guide in major governmental security initiatives. For example, the Court of Auditors of the Union (TCU) uses this framework as a fundamental basis for its cybersecurity audit program (Tribunal de Contas da União 2020).

Similarly, the Digital Government Secretariat incorporates the CIS Controls into the Privacy and Information Security Framework, the primary reference for >250 agencies linked to Gov.br (Roberto et al., 2023).

Furthermore, the National Cybersecurity Strategy of the Judiciary (ENSECPJ) employs version 7 of the CIS controls to protect critical infrastructures and manage identities and access control (Roberto et al., 2023).

The choice of security controls in the CIS Controls v8 focused on directly mitigating the causes of the business risks identified in this work. Each control was meticulously selected to address specific threats or vulnerabilities that, if exploited, could directly impact the operational risks identified.

A total of 232 information security measures were proposed. Of these, 133 (57.33 %) were selected from the controls established by the CIS Controls.

Table 4 presents some of the CIS Controls adopted in the paper. The complete list of all security controls adopted in the paper and derived from the CIS Controls is available at Alves et al. (Alves et al., 2025).

Table 4
Security controls from CIS controls.

Id	Control	Operational Risk
1.1	Establish and maintain a detailed enterprise asset inventory	7, 9, 11, 15, 16, 23
2.1	Establish and maintain a software inventory	2, 9, 11
3.1	Establish and maintain a data management process	1, 2, 5, 6, 24, 34
4.1	Establish and maintain a secure configuration process	5, 9, 11
5.1	Establish and maintain an inventory of accounts	3, 4, 13

Clipping of security controls from CIS controls.

5.2. Additional controls

The CIS Controls approach establishes comprehensive and priority controls to mitigate most risks or effects (Sager and McClain, 2020). However, the CIS framework did not cover all the operational risks identified in the initial phase of the paper, particularly in the areas of physical security and business continuity.

Moreover, recent technological evolution was not addressed, exemplified by innovations such as Secure Access Service Edge (SASE) (Alves, 2024), conditional access based on behavioral patterns, and blockchain technology as a tool for controlling information modifications.

The specificity of the Judiciary sector, associated with managing sensitive data, required the proposition of critical customized controls to mitigate previously identified risks.

It was necessary to propose an additional 99 (42.67 %) complementary controls, introduced in this study, to mitigate risks that the CIS Controls did not initially cover.

Table 5 presents some examples of proposed complementary controls. The complete list of all additional controls for each business risk is available at Alves et al. (Alves et al., 2025).

The literature corroborates that the customization of security measures, known as “tailoring,” is a well-established and widely accepted practice in information security aimed at ensuring the effectiveness and relevance of the measures in specific contexts.

This process allows organizations to adjust standard security controls to reflect their risks, regulatory requirements, and operational characteristics (U. D. of H. Security 2014).

Tailoring involves the assessment of risks, the identification of relevant controls, and the modification of these to suit the specific context. This includes adding, modifying, or removing controls to ensure that security is adequate without being overly restrictive or inadequate for the environment (U. D. of H. Security 2014).

The customization process involved adjusting pre-existing security controls to align with an organization’s or system’s unique needs, assessing risks, identifying relevant controls, and modifying them to fit the specific context.

Thus, the proposed methodology was enriched with the inclusion of controls recommended by interviewed participants and members of focus groups involved in the paper. The multidisciplinary contribution of the focus group, involving professionals from various fields but directly active in judicial bodies, provided a broader and more accurate understanding of the business risks faced by the Judiciary.

The comprehensive approach allowed for the evaluation of challenges and threats, reflecting in identifying more effective mitigation strategies aligned with the specific demands and unique risks faced by the target institutions of this article in their unique realities.

The additional controls proposed were derived from a detailed analysis of the specific needs and operational risks identified in the context of the Judiciary.

Table 5
Additional security controls.

Id	Control	Operational Risk
19.1	Have a mental health program	2, 13, 17, 28, 34
20.1	Develop contingency and succession plans	14, 25, 32
21.1	Manage risks for judicial authorities and establish security protocols	14
22.1	Prioritize the use of civil servants with strong recommendations to handle confidential information	2, 34
23.1	Evaluate professional and economic development	2, 17, 28, 34

Clipping of additional security controls.

The 99 additional controls are divided into ten groups:

- Organizational Environment;
- Competencies;
- Strategy;
- Structure;
- Management;
- Identity and Access;
- Intelligence;
- Work Processes;
- Physical Security;
- Technology.

These controls complement the practices recommended by the CIS Controls, addressing areas particularly relevant to information security in the judicial environment. Here are some key points on how these additional controls were determined:

1) *Operational Risk Analysis*
   The research identified specific operational risks within the Judiciary environment that the CIS Controls did not fully address. This includes risks related to mental health, ethics, effective communication, and the need for flexibility in hiring experts.
2) *Assessment of Specific Needs*
   Considering the unique environment and challenges the Judiciary faces, the study proposed controls that address these specific needs, such as mental health programs and ongoing intelligence efforts to reduce vulnerability to co-optation by malicious agents and promote a culture of ethics and integrity.
3) *Technological Adaptation*
   Recognizing the growing importance of technology in the Judiciary, the study included controls that address information security in a technological context, such as using artificial intelligence and blockchain. This demonstrates an adaptation to technological changes and new methods of work.
4) *Contingency Management and Communication*
   The controls also emphasize the importance of preparation for contingencies and effective communication, highlighting the need for business continuity plans and clear communication about the distribution of processes and the lack of human resources.
5) *Awareness and Supervision*
   Furthermore, the controls reflect an awareness of the risks associated with the distribution of processes and the importance of human supervision and review, especially concerning decisions or documents generated by artificial intelligence.

These additional controls were proposed after careful assessment of the specific risks and needs of the Judiciary, demonstrating an adaptive approach to information security that complements the standard practices recommended by the CIS Controls.

5.3. Classification of controls

Angelini et al. (2022) supports classifying security controls as the first step in defining a cyber risk assessment methodology. The author points out that classifying controls based on their characteristics is fundamental to clarifying their purpose and facilitating interpretation for their implementation.

To improve the effectiveness of security measures, it was essential to categorize the wide range of existing controls, including those relating to CIS Controls. This categorization helps identify and group the most relevant security actions that can be applied according to the purposes and contexts of implementation. It also provides an overview by thematic area of the different types of controls available, guiding managers in selecting the most pertinent measures to achieve specific objectives.

In addition, it is possible to parallelize the implementation of controls based on the classifications since it helps identify those responsible and areas of action, reducing the time to achieve a higher level of information security maturity.

To draw up this classification, one of the references was the taxonomy of operational risk controls in the Judiciary proposed by Machado (2018). However, it was found that the proposed taxonomy would not meet the specific needs of this article. We sought to establish an original nomenclature of control categories at a single level so that managers could more quickly select the thematic area of each control. This evaluation resulted in a classification of the proposed additional controls comprising ten distinct categories, as described below:

1) *Organizational Environment*
   A set of aspects that define the organizational culture or climate involves ethical aspects, personal conflicts, and the conditions that influence how people relate to each other and make decisions.
2) *Competencies*
   The skills, knowledge, attitudes, and experience needed for people to perform their job functions.
3) *Strategy*
   Defining long-term objectives and formulating plans to achieve them.
4) *Structure*
   How the organization is organized, including the hierarchy, the distribution of duties and responsibilities, and the coordination mechanisms between different organizational units.
5) *Management*
   Set plans and actions to execute and monitor the organizational strategy to ensure efficiency, effectiveness, and regulatory compliance. It encompasses management actions at a tactical level.
6) *Identity and Access*
   Controls to manage the identification of who has access to what information and systems within the organization.
7) *Intelligence*
   Human threat intelligence involves collecting, analyzing, and using confidential or open information to anticipate trends and institutional risks and make informed decisions.
8) *Work Processes*
   Controls relate to the set of organized and sequential activities carried out to achieve specific objectives in an organization.
9) *Physical Security*
   It encompasses the measures designed to protect the organization's physical facilities and assets.
10) *Technology*
    The set of tools, systems, and technological infrastructures the organization uses. It includes services, hardware, and software for transmitting, storing, or modifying information.

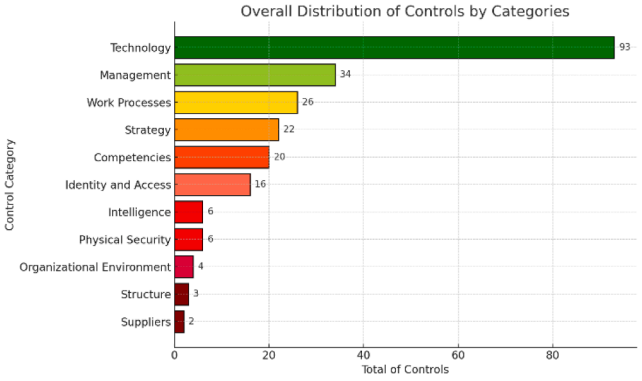


Fig. 3. Comparison between CIS controls and additional controls.

Fig. 3 compares the controls in CIS Controls V8 and the additional controls proposed in this article. Fig. 4 shows the percentage distribution of the CIS framework controls used in the research by category.

The comparison between Fig. 3 shows the proportion of additional controls among the various categories. The reduction in the proportion of technological controls may result from CIS Controls being efficient at indicating technological controls.

The additional controls were drawn up by Judiciary managers with a great deal of practical experience, specifically aimed at tackling specific and critical risks within this context. These measures constitute an invaluable source of detailed actions that are meticulously aligned to the requirements of the judicial sector, providing a precise fit to its unique needs.

Analyzing the categories of Strategy, Management, and Work Processes reveals a deep connection and a complementary relationship between them.

Strategy focuses on governance, defining long-term directions, and developing plans to achieve organizational objectives. This includes everything from policy formulation and strategic planning to stipulating organizational goals underpinning the organization's future direction.

Management controls are more closely related to the supervision and implementation of strategies defined at a higher level. This category encompasses day-to-day management, resource management, decision-making, and operational control, facilitating strategy transition from paper to practice. On the other hand, work process management focuses on optimizing the flow of tasks and maximizing the delivery of value, addressing the execution of various activities and the interaction between different participants in a pragmatic and focused manner.

Although these categories are independent, interdependence and complementarity unite them, contributing to the protection of organizations. More specifically, the relationship between strategy, management, and work processes can be considered a component of an integrated system, offering a holistic view of how the organization works, from strategic conception to practical execution.

Fig. 5 shows the percentage distribution of the proposed Additional Controls by category. Technology represents the largest share, occupying 23.2 % of the total, demonstrating that a substantial proportion of the additional controls are focused on technology, possibly covering software, hardware, and network security.

Organizational Environment, representing 11.1 %, highlights the importance of the work environment, including organizational culture and employee behavior, as part of security controls.

The heat map shown in Fig. 6 indicates the need to apply more technological controls to protect assets: networks, devices, and applications. It can be assumed that these are more complex to defend.

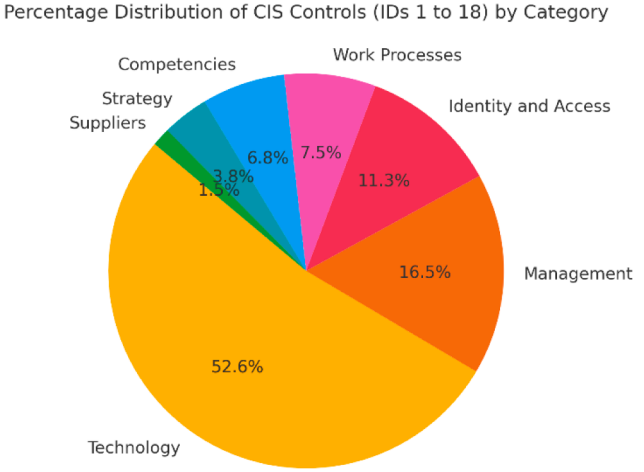


Fig. 4. Distribution of CIS controls V8 control categories.

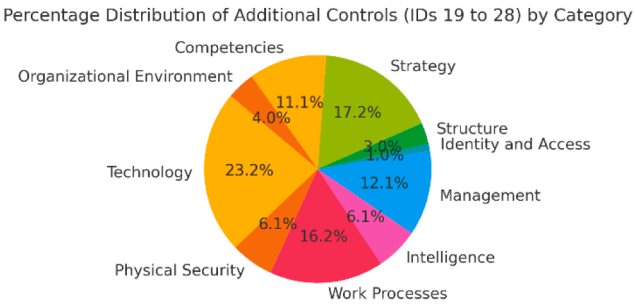


Fig. 5. Distribution of additional control categories.

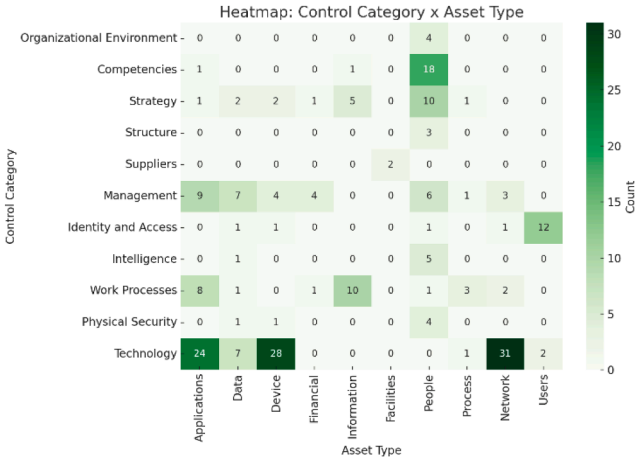


Fig. 6. Distribution of additional control categories.

6. Deployment priorities

Fig. 7 shows that, in the category of controls in Implementation Group 1 (IG1), most of the controls are aimed at training people. This indicates that, of all the controls, information security training should be the initial focus of implementing controls.

Such training covers user awareness, including privileged users, and extends to developers, emphasizing secure development practices.

It also includes security training for infrastructure professionals to prevent insecure configurations in components such as operating systems, network assets, and databases.

Additionally, it involves forming specialized cybersecurity teams and

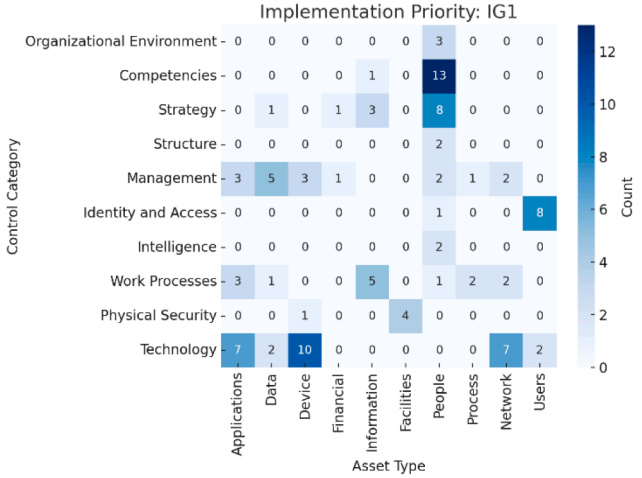


Fig. 7. Distribution of IG1 control categories.

consolidating a comprehensive effort to strengthen the organization's security posture.

In Fig. 8, the second group of priority controls that comprise Implementation Group 2 (IG2) emphasizes network controls.

These controls are essential for mitigating the risk of unauthorized access and ensuring the integrity and availability of the network infrastructure.

Prioritizing these technological controls reflects an understanding of the need to strengthen the technological infrastructure's most vulnerable and critical points, ensuring that the organization's operations remain secure and resilient against cyber-attacks.

In Fig. 9, the third group of priority controls, comprising Implementation Group 3 (IG3), shows more specialized technological controls for applications, devices, and networks. This shows the greater complexity involved in protecting these categories.

7. Analysis of the results

In this article, the initially established hypothesis emphasizes the complexity of the Judiciary's challenges in the information security arena. The research identified a comprehensive collection of security measures beyond the technological sphere, demonstrating the depth and diversity of the controls needed to address the risks intrinsic to fundamental judicial activities.

This finding validates the initial hypothesis and highlights the insufficiency of isolated security control solutions to effectively mitigate the risks raised, emphasizing the indispensability of a multidisciplinary approach.

The article revealed the importance of robust mental health programs, not just as an organizational well-being practice but as a safety factor. Preventive mental health programs minimize the risk of associating employees with malicious actors, sustaining operational integrity and reducing vulnerabilities.

Effective communication between experts and judges was identified as an essential additional control, highlighting the need to clarify technical processes and mitigate misunderstandings. This reinforces the assertiveness of judicial decisions and strengthens the chain of custody of information.

Promoting a culture of ethics and integrity among justice system professionals has emerged as an essential control. Continuous training in these principles is a barrier against undue external and internal influences, maintaining the probity of the judiciary.

The need for independent supervisory and control bodies was also highlighted, functioning as balancing and transparency mechanisms critical for detecting and preventing undue influence and corruption.

Contingency and succession plans were highlighted as fundamental

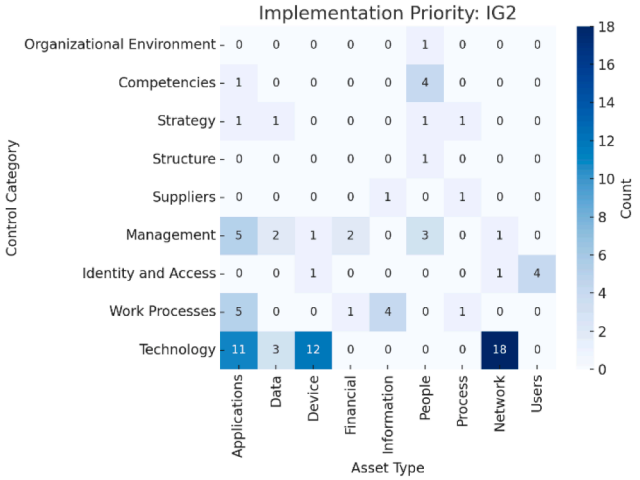


Fig. 8. Distribution of IG2 control categories.

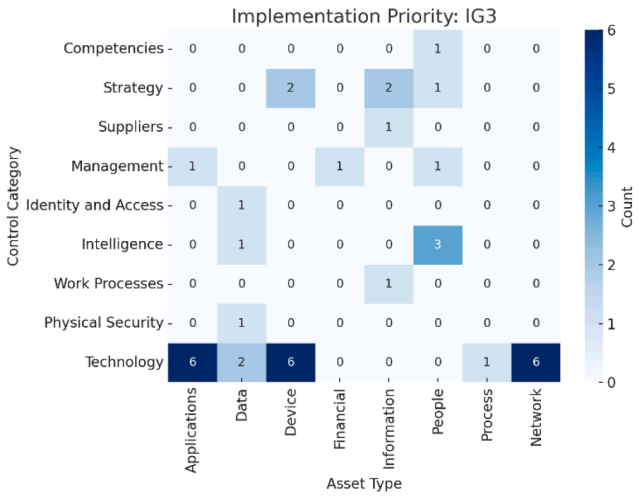


Fig. 9. Distribution of IG3 control categories.

additional controls to guarantee the continuity of judicial operations. Training and creating multidisciplinary teams prepare the system to deal with leadership's temporary or permanent absence, mitigating disruptions to essential services.

Effective communication of human resource shortages was recognized as a key control to prevent delays and overloads in projects and activities. This allows for the agile reallocation of resources and the maintenance of operational productivity.

Flexible hiring of technical experts is a control that addresses the growing complexity of court cases that require specialized knowledge, ensuring well-informed and technically accurate decisions.

The technical training of magistrates and managers is essential to facilitate the interpretation of technical evidence and reports, a control that supports accuracy and fairness in judicial decisions.

Assessing the qualifications of contracted experts ensures that only highly qualified and ethical professionals are selected, contributing significantly to the integrity of the technical analysis and confidence in the evidence presented.

In addition, investment in the training of civil servants not only promotes the development of skills but also serves as a mechanism for retaining knowledge, which is essential for the continuity of operations and information security.

Regular psychological assessments of individuals in key positions ensure that those in charge of sensitive functions can cope with the stress and responsibilities of the job, preventing security breaches.

Time management training for meeting court deadlines is a reasonable control to improve efficiency and prevent procedural delays, contributing to the timely functioning of the judicial system.

The selection of qualified legal advisors is a control that reinforces the quality of the review and preparation of legal documents, which is fundamental for maintaining excellence in judicial production.

Training users in the ethical use of AI prevents the inappropriate application of automated tools and supports the transparency and reliability of processes, mitigating the risk of systemic errors and algorithmic bias.

Rigorous background checks on developers and database administrators (DBAs) who work on the judiciary's critical systems are an essential security measure. This control ensures that only individuals with proven integrity and reliability are responsible for handling sensitive data and vital infrastructure, mitigating the risk of data leaks or manipulation.

Segregation of duties in the programming and maintenance of critical systems establishes a robust layer of internal security. This prevents a single person or group from having excessive control, significantly reducing the chances of code corruption and other forms of system

compromise.

The need for double approval for critical operations introduces a mechanism for checks and balances, increasing the integrity of the decision-making process. This is particularly relevant in information systems where unauthorized changes can have drastic consequences.

Implementing robots or Artificial Intelligence systems to automate the verification of similar lawsuits constitutes an innovative control. This system not only optimizes the detection of redundancies and case conflicts but also contributes to greater consistency and efficiency in the administration of justice, reducing the manual workload and allowing for a more strategic allocation of human resources.

Integrating judicial systems and creating a national database of cases is a significant control that promotes transparency and easier access to procedural information. This not only improves collaboration between different judicial bodies but also enhances the use of data for analysis and informed decision-making, guaranteeing data integrity and the continuity of the legal process throughout the national territory.

Furthermore, partnerships between public bodies and academia are additional controls that promote innovation and the integration of IT solutions, encouraging the development and adoption of advanced technologies within the judiciary.

Encouraging domestic production of information technology is a control that reduces dependence on foreign solutions, addressing security risks associated with international espionage and geopolitical instability.

Creating a national cybersecurity testing laboratory is an additional control that provides independent validation of IT equipment and solutions, essential for confirming their security and effectiveness before large-scale implementation.

As new threats emerge, the Judiciary must continue to evaluate and update its security controls, ensuring an effective defense against emerging risks. This dynamic approach reflects a commitment to the constant evolution of information security, aligned with the unique needs and challenges of the Judiciary.

Additionally, implementing this assessment must be adapted to each body's unique characteristics and context to ensure relevant results, reflecting a qualitative understanding of the risks and consequences for each institution.

In this way, the methodology proposed in this article establishes a bridge between business risks and cyber security control, potentially meeting the recommendation of Eling et al. (2021) regarding integrating cyber risk into the corporate risk management framework.

This integrated approach, which enables the understanding of risks at multiple levels with the effective management of information security controls, promises not only to improve security within the judiciary but also to model a paradigm for risk management and information security in similar contexts, opening up avenues for future research and implementation.

Applying this proposal involves carrying out risk assessments in line with the specific context of each judicial institution. It is essential to consider factors such as organizational culture, positions, functions within the Judiciary's structure, and each entity's risk appetite. This personalized approach is necessary for adapting strategies that meet the needs and particularities of each body, effectively integrating cyber risk into corporate risk management.

The contributions of this article promote innovation in the way technical areas and senior management understand and communicate, establishing a more efficient and productive dialog in the Judiciary. In addition, proposing strategies and practical suggestions offers preventive and mitigating measures for various organizational units. It also directs and optimizes investments in information security and paves the way for further research, strengthening security practices in a judicial environment increasingly dependent on technological solutions.

8. Conclusion

This article contributes to understanding and addressing information security risks in the Judiciary. With a comprehensive methodology aligned with the security practices and standards recognized in the CIS Controls framework and the expertise of the interviewees and the focus group, the article succeeded not only in mapping the main risks for the Judiciary but also in providing a robust and customized set of controls to mitigate them.

This collective and multidisciplinary effort, which emphasized collaboration and critical analysis, brought to light the imperative need to adapt security strategies to the unique specificities of the Judiciary context, aiming not only to protect data but also to preserve the integrity and reliability of the justice system as a whole.

The article achieved its primary objective of establishing a list of reference information security controls in addition to the CIS Controls framework, which proved invaluable for strengthening security within the Judiciary.

By identifying business and operational risks and correlating them with a comprehensive range of security controls, this article offers a practical and effective guide for implementing security strategies adapted to the specific context of the Judiciary.

In this way, it was confirmed that information security goes beyond implementing technological controls, requiring an integrated and multidisciplinary approach involving all levels of the organization.

However, the ever-evolving nature of information security and the constant emergence of new technologies, regulations, and threats emphasize the need for periodic reviews of the security strategies adopted.

This process of continuous review is vital to ensure that security measures remain relevant and effective in the face of changes in the risk landscape.

Thus, the article emphasizes the importance of incorporating 99 additional and complementary controls, highlighting the need for a more robust security approach adaptable to the judiciary's particularities.

The additional controls are focused on information security, personnel management, and technology, highlighting a multidisciplinary and personalized approach to mitigating the Judiciary's operational and business risks.

Finally, this article offers valuable contributions to risk management and information security strategies, especially in the face of the challenges posed by cyber-attacks in the context of the Judiciary.

The findings presented serve as a channel to improve communication and understanding between technical areas and senior management, outlining preventive and mitigating strategies to safeguard the security of judicial institutions and authorities.

This article contributes to the existing literature by offering practical suggestions and laying the foundations for future research that can evaluate the implementation of the proposed security measures and adapt them to different institutional contexts. This ensures continued progress in information security within the Judiciary.

CRediT authorship contribution statement

Renato Solimar Alves: Visualization, Project administration, Investigation, Conceptualization, Writing – original draft, Validation, Methodology, Data curation. **Jady Pamella Barbacena da Silva:** Visualization, Writing – review & editing. **Luiz Antonio Ribeiro Junior:** Writing – review & editing, Conceptualization, Visualization. **Rafael Rabelo Nunes:** Visualization, Supervision, Methodology, Writing – original draft, Validation, Project administration, Conceptualization.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

The authors acknowledge the University of Brasília (UnB) for the financial support provided by the Grant n° 001/2025 DPI/BCE/UnB.

Data availability

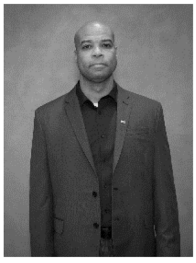
The data access link is provided in the References section.

References

ABNT. NBR ISO 31000: Gestão de riscos - princípios e diretrizes. 2018.
Alves, R.S., 2024. Proposta de uma linha de base de controles de segurança da informação para mitigação dos riscos de negócio do poder judiciário brasileiro. Master's Dissertation. Electrical Engineering Department, University of Brasília, Brasília, DF, Brazil.
Alves, R.S., da Silva, J.P.B., Ribeiro Junior, L.A., Nunes, R.R., 2025. Security controls for judiciary risk management. Zenodo. https://doi.org/10.5281/zenodo.14914626.
Alves, R.S., Georg, M.A.C., Nunes, R.R., 2023. Judiciário sob ataque hacker: riscos de negócio para segurança cibernética em tribunais brasileiros. Revista Iberica de Sistemas e Tecnologias de Informação E56, 344–357.
Amaral, D.M., 2020. O poder judiciário, estrutura e principais funções. Jus Brasil [Online]. Available at: https://www.jusbrasil.com.br/artigos/o-poder-judiciario-estrutura-e-principais-funcoes/861564653. Accessed on: March 31, 2024.
M. Angelini, S. Bonomi, and A. Palma, "A methodology to support automatic cyber risk assessment review." 2022. [Online]. Available at: http://arxiv.org/abs/2207.03269. Accessed on: March 31, 2024.
Bureau of Justice Assistance, "What is risk assessment?" 2023. [Online]. Available at: https://bja.ojp.gov/program/psrac/basics/what-is-risk-assessment. Accessed on: March 31, 2024.
Barnard, L., Von Solms, R., 2000. A formalized approach to the effective selection and evaluation of information security controls. Comput. Secur. 19 (2), 185–194.
Barrêto, M.L.D.A., 2021. Estudo sobre a gestão da política de segurança da informação no Poder Judiciário do estado do Tocantins.
Chapelle, A., 2018. Front matter. Operational Risk Management. John Wiley & Sons, Ltd, pp. i–xxiv. ISBN 9781119548997[Online]. Available at: https://onlinelibrary.wiley.com/doi/abs/10.1002/9781119548997.fmatter. Accessed on: March 31, 2024.
Ciso Advisor, 2022. TJ do Distrito Federal segue fora do ar após ataque no domingo. Ciso Advisor [Online]. Available at: https://www.cisoadvisor.com.br/tj-do-distrito-federal-segue-fora-do-ar-apos-ataque-no-domingo/. Accessed on: March 31, 2024.
Conselho Nacional de Justiça, "Estratégia nacional de segurança cibernética do poder judiciário". 2021. [Online]. Available at: https://atos.cnj.jus.br/files/compilado1402302021061460c7617672ec5.pdf. Accessed on: March 31, 2024.
Conselho Nacional de Justiça (CNJ), 2021. Protocolos e manuais previstos na estratégia nacional de segurança cibernética. CNJ [Online]. Available at: https://atos.cnj.jus.br/files/compilado1402302021061460c7617672ec5.pdf. Accessed on: March 31, 2024.
Conselho Nacional de Justiça (CNJ). "Justiça 4.0 - CNJ portal". CNJ, 2032. [Online]. Available at: https://www.cnj.jus.br/tecnologia-da-informacao-e-comunicacao/justica-4-0/. Accessed on: March 31, 2024.
Crouhy, M., Galai, D., Mark, R., 2014. The Essentials of Risk Management, 2nd Ed. McGraw Hill. ISBN 978-0-07-182115-5.
do Carmo Martins, T., 2021. Acesso à justiça e pandemia. Rev. Jus Navig. 6412. ISSN 1518–4862. [Online]. Available at: https://jus.com.br/artigos/88048. Accessed on: December 23, 2022.
Eling, M., McShane, M., Nguyen, T., 2021. Cyber risk management: history and future research directions. Risk Manag. Insur. Rev. 10 (1), 93–125.
Eltis, K., 2011. The judicial system in the digital age: revisiting the relationship between privacy and accessibility in the cyber context. McGill Law J. Consort. Erud. 56, 289–316. ISSN 0024–9041.
Galegale, N.V., Fontes, E.L.G., Galegale, B.P., 2017. Uma contribuição para a segurança da informação: um estudo de casos múltiplos com organizações brasileiras. Perspect. em Ciênc. Inf. 22 (3), 75–97. https://doi.org/10.1590/1981-5344/2866. JulyISSN 1413–9936. [Online]. Available at:Accessed on: March 31, 2024.
Gordon, D.L.M., 2020. Cybersecurity & the courthouse: safeguarding the judicial process. Wolters Kluwer. ISBN 9781543809756[Online]. Available at: https://books.google.com.br/books?id=DHLJDwAAQBAJ. Accessed on: March 31, 2024.
Hino, M.C., Cunha, M.A., 2020. Adoption of technology in the legal professionals' perspective." Fundação Getulio Vargas. Esc. Direito São Paulo 16. ISSN 23176172.
Hirata, A., de Oliveira, C.G.B., 2020. 39 dias após o ataque cibernético ao STJ - reflexões e desafios. In: Migalhas, 5505 [Online]. Available at: https://www.migalhas.com.br/coluna/migalhas-de-protecao-de-dados/337701/39-dias-apos-o-ataque-cibernetico-ao-stj–reflexoes-e-desafios. Accessed on: March 31, 2024.
Jallow, A.K., Majeed, B., Vergidis, K., Tiwari, A., Roy, R., 2007. Operational risk analysis in business processes. BT Technol. J. 25 (1), 168–177. https://doi.org/10.1007/s10550-007-0018-4. ISSN 1573–1995. [Online]. Available at:Accessed on: March 31, 2024.
Lima, E.D., Moreira, F.R., de Deus, F.E., Nze, G.D.A., de Sousa Junior, R.T.de S., Nunes, R.R., 2022. Avaliação da rotina operacional do operador nacional do sistema elétrico brasileiro (ONS) em relação às ações de gerenciamento de riscos associados à segurança cibernética. RISTI (PORTO), E49, pp. 301–312.
Joint Technology Committee, "Cybersecurity basics for courts". 2019. [Online]. Available at: https://www.ncsc.org/_data/assets/pdf_file/0037/68887/JTC-2021-05-Cybersecurity-QR_Final-Clean.pdf. Accessed on: March 31, 2024.
M.B. Machado, "Taxonomia de eventos de risco operacional do poder judiciário". 2018. [Online]. Available at: http://repositorio.enap.gov.br/handle/1/3399. Accessed on: March 31, 2024.
Moreira, F.R., Da Silva Filho, D., Nze, G.D.A., de Sousa Júnior, R.T., Nunes, R.R., 2021. Evaluating the performance of NIST's framework cybersecurity controls through a constructivist multicriteria methodology. IEEE Access 9, 129605–129618.
Moura, R.M., Borges, L.A., 2022. A impunidade dos hackers que colocaram o judiciário de joelhos. Veja [Online]. Available at: https://veja.abril.com.br/politica/a-impunidade-dos-hackers-que-colocaram-o-judiciario-de-joelhos/. Accessed on: March 31, 2024.
Nunes, R.R., Batista Sidrim Perini, M., Melo Mourão Pinto, 2021. A gestão de riscos como instrumento para a aplicação efetiva do Princípio Constitucional da Eficiência. Revista Brasileira de Políticas Públicas 11 (3).
Project Management Institute, Inc. (PMI), 2021. The standard for risk management in portfolios, programs, and projects. PMI. ISBN 978-1-62825-565-2.
Rast, C., 2023. Cybersecurity Threats to the Judiciary [Online]. Available at: https://www.americanbar.org/groups/judicial/publications/judges_journal/2023/summer/cybersecurity-threats-to-judiciary/. Accessed on: March 31, 2024.
Raymond, N., 2022. Federal judiciary 'vulnerable' to cyberattacks, U.S. lawmakers told. Reuters. May 12[Online]. Available at: https://www.reuters.com/legal/government/federal-judiciary-vulnerable-cyberattacks-us-lawmakers-told-2022-05-12/. Accessed on: March 31, 2024.
Reina, E., 2022a. A onda de invasões hackers às estruturas tecnológicas dos tribunais. Revista Consultor Jurídico. April[Online]. Available at: https://www.conjur.com.br/2022-abr-15/onda-invasoes-hackers-estruturas-tecnologicas-tribunais. Accessed on: March 31, 2024.
E. Reina, "Ameaça Virtual - Em 18 meses, hackers violaram sistemas de tribunais no Brasil a cada 41 dias". 2022b. [Online]. Available at: https://www.conjur.com.br/2022-abr-15/onda-invasoes-hackers-estruturas-tecnologicas-tribunais. Accessed on: May 22, 2022.
Ribeiro, A.C., Demo, G., dos Santos, C.D., 2021. Grupo focal: aplicações na pesquisa nacional em administração. Pretexto 22, 108–128. ISSN 1984–6983.
P. Roberto et al., "Guia do framework de privacidade e segurança da informação", 2023. [Online]. Available at: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ppsi/guia_framework_psi.pdf. Accessed on: March 31, 2024.
Rover, A.J., 2015. O e-judiciário no Brasil: uma bibliometria temática. Conpedi Law Rev. 1, 155.
T. Sager and S. McClain, "CIS controls - auditing, assessing, analyzing: a prioritized approach using the pareto principle." 2020. [Online]. Available at: https://www.cisecurity.org/insights/white-papers/auditing-assessing-analyzing-a-prioritized-approach-using-the-pareto-principle. Accessed on: March 31, 2024.
Stocchetti, V., & Sager, T. "The cost of cyber defense: CIS controls implementation group 1". 2023. [Online]. Available at: https://www.cisecurity.org/insights/white-papers/the-cost-of-cyber-defense-cis-controls-ig1. Accessed on: March 31, 2024.
Tribunal de Contas da União, "Acompanhamento de SegCiber". 2020. [Online]. Available at: https://portal.tcu.gov.br/fiscalizacao-de-tecnologia-da-informacao/atuacao/fiscalizacoes/. Accessed on: March 31, 2024.
Schwaitzer, L.D.B.D.S., 2016. Segurança, Acesso e Preservação da Informação Arquivística do Poder Judiciário. DIREITO E INFORMAÇÃO NA SOCIEDADE EM REDE, p. 403.
U. D. of H. Security, 2014. DHS 4300A Sensitive Systems Handbook - Attachment M - Tailoring NIST 800–53 Security Controls.
D.L. Wanderley, "Um framework para o gerenciamento de riscos em segurança da informação no Poder Judiciário do Tocantins". 2020. [Online]. Available at: http://hdl.handle.net/11612/2388. Accessed on: March 31, 2024.

Renato Solimar Alves (M'24) holds a Master's in Electrical Engineering from the University of Brasília (UnB), focusing on Cybersecurity. He specializes in Systems Engineering and has a degree in Mobile Telecommunications Technology. He works as an Information Technology manager with >15 years of experience in improving and protecting technological resources in the Judiciary. He was part of the Information Security Management Committee of the Judiciary, actively contributing to creating the National Cybersecurity Strategy for the Judiciary (ENSEC-PJ). As a public servant at the Brazilian Justice Council, he played several roles in coordinating information security management and responding to cybersecurity incidents in the Federal Justice system. He is the Director responsible for the division of payment request systems for court-ordered debts at the Federal Regional Court of the 1st Region.

Jady Pamella Barbacena da Silva (MBA'23) is pursuing a Master of Science in Computer and Systems Sciences at the University of Stockholm, Sweden, and another in Cybersecurity and Artificial Intelligence at the University of Brasília, Brazil. She completed two MBAs: the first in Project Management from FGV in 2018 and the second in Innovation Technology and Entrepreneurship Management in 2023. Jady has over a decade of experience managing IT processes and projects. Since 2014, she has worked as an IT Analyst and Manager at the Bank of Brasília (BRB), where she led the implementation of IT asset management processes following ITIL, COBIT, and Lean IT standards. She has been recognized for her contributions to the field with awards like the Efinance 2019 for her strategic project implementations at BRB. Her work with IEEE now includes contributions to the organization's conferences and publications, particularly cybersecurity and artificial intelligence.



Luiz Antonio Ribeiro Junior (PhD'15) holds a bachelor's, master's, doctorate, and postdoctoral degree in Physics from the University of Brasília. He conducted a doctoral internship at Linköping University, Sweden (2013–2015). He was a visiting researcher at the Department of Applied Physics at the University of Campinas (Unicamp, 2022–2023). Currently, he is an assistant professor and the coordinator of the Laboratory of Computational Science of Materials (LCCMat) at the Institute of Physics of the University of Brasília. His expertise lies in Physics, with an emphasis on computational simulation of materials and biomaterials for the development of nanotechnology applications. He is an affiliate member of the Brazilian Academy of Sciences (ABC, 2024–2029).

Rafael Rabelo Nunes (PhD'12) is a professional with a strong background in IT and an active teaching career who seeks to combine technology and people as a driving force for organizational transformation. He is an Adjunct Professor at the University of Brasília, working part-time. He also works in Information Security Risk Management at the Brazilian Supreme Court and as a Professor at UniAtenas University Center. He holds a PhD in Electrical Engineering from the University of Brasília. He graduated in Communication Networks Engineering from the same university, with some courses completed at the University of Porto, Portugal. Additionally, he has a Special Teacher Training Program degree from the Catholic University of Brasília and a Master's degree in Electrical Engineering from the University of Brasília. With over 20 years of experience in Information Technology (IT), he maintains an inseparable academic and professional career. He has previously worked as a Special Advisor to the Presidency, Information Security Manager, Software Development Project Manager, Infrastructure Analyst, and Development Analyst. In the private sector, he worked as a Network Engineer at TIM and Claro and as a Professor at Estácio University Center in Brasília.