Proceedings of the 10th International Conference on Computer and Information Science and Technology (CIST 2025)
Paris, France - August 2025
Paper No. CIST 112
DOI: 10.11159/cist25.112

Streamlining Security: Mapping NIST SP 800-53, SOC 2, and US CJIS Policy to ISO/IEC 27001:2022 for Service Provider SMEs

Damilola Innomesanghan[1], Emmanuel Kiwamu[2], Sergey Butakov[3], and Eslam G. AbdAllah[4]
[1,2,4] Concordia University of Edmonton, Edmonton, Alberta, Canada
[3]Computer Science, Western New England University, Springfield, Massachusetts, USA
Emails: {dinnomes, ekiwamu}@student.concordia.ab.ca; sergey.butakov@wne.edu; eslam.abdallah@concordia.ab.ca

Abstract **-** With the growing complexity of the information security landscape, service provider Small and Medium Enterprises (SMEs) face challenges protecting their information and information assets. Due to the nature of their operations, these organizations are required to handle sensitive customer data and therefore must maintain a robust information security posture that will reflect its readiness to defend against, mitigate and respond to security threats. To tackle these challenges, the adoption of information security standards can help provide organizations with a structured and strategic approach to establish, implement and maintain a strong information security posture. This paper analyzes four prominent information security standards and frameworks: ISO/IEC 27001:2022, NIST SP 800-53 Revision 5, SOC 2, and the US CJIS Security Policy. Through a detailed mapping of the organizational, people, physical, and technological controls of the ISO/IEC 27001:2022 standard, the study identifies areas of alignment, overlap, and divergence among the standards using ISO/IEC 27001:2022 as a baseline. The analysis highlights key differences in scope, implementation approaches, and compliance requirements, offering practical insights for service providers aiming to achieve multi-framework compliance. This work serves as a resource for organizations especially service provider SMEs seeking to integrate these standards while maintaining operational efficiency and regulatory alignment.

Keywords**:** Service Provider SMEs, Information Security Standards, NIST SP 800-53, SOC 2, US CJIS, ISO/IEC 27001:2022, Security Controls

1. Introduction

In an era where digital transformation drives business operations, safeguarding sensitive information has become a critical priority for service provider Small and Medium Enterprises (SMEs) entrusted with vast amounts of customer data making them prime targets for cyber threats. To address this challenge, implementing robust security controls to protect and preserve the confidentiality, integrity, and availability of information and information assets is crucial. The increasing volume and sophistication of cyber threats and the growing complexity of compliance requirements has made it increasingly difficult for service provider SMEs to effectively protect sensitive information and information assets. These SMEs lack the ability to maintain a resilient information security posture due to the lack of preparedness, non-existent security policies, and limited resources and expertise. According to the ISACA reporting in 2018 [1], 42% of organizations lack a formal information security management plan, leaving them highly vulnerable to evolving threats. The lack of preparedness, limited resources, and poor information security posture can lead to considerable losses, like data breaches and many more for these enterprises.

Therefore, this research addresses the challenges SMEs may encounter when implementing numerous standards and frameworks by examining important areas of overlap and divergence between selected information security standards and frameworks. This paper focuses on four prominent information security standards and frameworks: NIST SP 800-53 REV. 5, SOC 2, US CJIS Security Policy, and ISO/IEC 27001:2022. These standards and framework were selected because they collectively address critical aspects of information security, privacy, and compliance. NIST SP 800-53 REV. 5 provides a comprehensive set of security controls, SOC 2 focuses on service organizations, the US CJIS Security Policy is crucial for organizations handling criminal justice information, and ISO/IEC 27001:2022 offers an internationally recognized framework for information security management systems. By conducting a comparative analysis of these frameworks and standards, the study hopes to identify shared requirements and establish an efficient multi-framework compliance approach based on ISO/IEC 27001:2022's control domain areas, such as organizational, people, physical, and technological controls.

2. Literature Review

As an organization, implementing information security standards and frameworks to improve information security posture can be beneficial. Taherdoost [2], highlights that existing and established information standards and frameworks like the ISO 27001 series, NIST and many more can help guide organizations in achieving their information security objectives as well as business objectives. The paper emphasizes that organizations may need to adopt multiple standards, such as the ISO 27001 series, NIST, to effectively meet specific information security needs. Beckers et al. [3] further highlighting that the ISO 27001 is commonly implemented and compared with other information security standards due to its recognition in helping organizations establish and manage a robust and effective information security management system. These standards, however, are not one-size-fits-all because the applicability and implementation of standards and frameworks can differ depending on the organization. For organizations to effectively adopt information security standards, Wangen and Snekkenes [4] explored how integrating Business Process Management (BPM) can help improve Information Security Management. The paper explored how standards like the ISO/IEC 27005:2011 and NIST SP 800-39 can help organizations improve the relationship between security frameworks and organizational processes.

While existing literature and research helps improve the understanding of information security standards and frameworks, their adoption and implementation. There were gaps identified and there is need for more streamlined compliance efforts and to address the challenges organizations are faced with when dealing with compliance of multiple standards. By identifying similarities between the selected standards, SMEs can eliminate redundant work and simplify the compliance process while ensuring a strong and robust information security posture. This will reduce both the implementation time, and the cost associated with meeting the requirements of the complete standards set. The objective of this research is to provide a comprehensive analysis and mapping of widely adopted security standards NIST SP 800-53 REV. 5, SOC 2, US CJIS Security Policy, and ISO/IEC 27001:2022 in key industry sectors demonstrating the benefits of recognizing the similarities between them.

3. Overview of Standards

This section provides an overview of each of the selected standards and frameworks, outlining each standard and providing a comparative table to elaborate on the differences between the standards and frameworks.

3.1. ISO/IEC 27001:2022

ISO/IEC 27001:2022 (Information Security, Cybersecurity and Privacy Protection) is a widely recognized international standard for managing information security part of the ISO27000 series and is an upgraded streamlined version of ISO/IEC 27001:2013. It defines information security requirements for organizations to effectively establish, implement, maintain, and continually monitor and improve an information security management system (ISMS) and provides a structured approach that helps organizations become aware of the risk associated with their business and proactively identify and address weaknesses. ISO/IEC 27001:2022 is organized into ten mandatory clauses that follow ISO's standardized high-level structure. The first few clauses in ISO/IEC 27001:2022 define the scope, context, and key definitions, setting the foundation for an organization to develop its Information Security Management System (ISMS), followed by four control annexes, including the organization, people, physical, and technological controls [5].

3.2. NIST SP 800-53 REV. 5

NIST 800-53 (Security and Privacy Controls for Information Systems and Organizations) is another recognized standard developed and designed by the National Institute of Standards and Technology. This standard is designed as a comprehensive set of security and privacy controls for U.S. federal agencies and contractors [6]. NIST SP 800-53 is a flexible and foundational standard that helps organizations tailor their security controls specifically to their security needs. This standard covers twenty control families, some of which include access control, system and communications protection, Configuration management, incident response, Supply chain risk management, contingency planning, and many more.

3.3. SOC 2 Trust Service Criteria

SOC 2 (System and Organization Controls 2), is a framework designed by the American Institute of Certified Public Accountants (AICPA), provides a set of security criteria for service organizations that handle sensitive customer data. SOC 2 evaluates an organization's controls based on five Trust Service Criteria (TSC): security, processing integrity, confidentiality, availability, and privacy [7]. The trust services criteria outline the desired outcomes that an organization's security control should achieve to meet its specific objectives and provide a flexible approach for evaluation and reporting, regardless of the controls implemented. Also in SOC 2, points of focus were introduced as part of the 2017 SOC 2 Trust Services Criteria (TSC) to provide additional clarity and guidance for organizations and practitioners in applying the trust services criteria during evaluations of system controls.

3.4. US Criminal Justice Information Services (CJIS) Security Policy

US CJIS Security Policy defines the security standards for safeguarding Criminal Justice Information (CJI) throughout its entire lifecycle, encompassing creation, access, modification, transmission, distribution, storage, and destruction [8]. This policy ensures the protection of criminal justice information with stringent security protocols, reducing the risk of unauthorized access and data breaches. This policy governs the security requirements for criminal justice agencies, including state, local, and federal law enforcement entities. This policy covers a wide range of thirteen policy areas, including access control, encryption, audit logging, physical security and many more, to ensure that CJI remains secure from unauthorized access and tampering.

3.5. Differences between Standards and Frameworks

These standards and frameworks discussed do not only share several overarching similarities but also possess unique features that clearly set them apart from each other. These distinguishing characteristics are thoroughly highlighted in Table 1 below. This section delves deeper into the selected standards and frameworks, highlighting their key differences based on a variety of attributes hence helping SMEs make informed decisions about which standards best fit their operational strategy and compliance requirements.

Table 1: Key differences between Information Security Standards

	ISO/IEC 27001:2022	NIST SP 800-53 REV. 5	SOC 2	US CJIS
Description	Provides a framework for establishing, implementing, maintaining, and continually improving an information security management system (ISMS).	The standard lays out security and privacy controls requirements for federal information systems and organizations.	Focused on controls related to security, availability, processing integrity, confidentiality, and privacy of customer data, evaluating how organizations manage data to protect privacy.	Established by the FBI, it provides guidelines and requirements for protecting and sharing sensitive criminal justice information.
Target organizations	Targeted broadly across industries. Suitable for any organization that wants to protect sensitive information and meet client or regulatory requirements regarding information security.	Primarily intended for U.S. federal agencies, contractors, and organizations working with the federal government, but often adopted by private sector entities looking to enhance cybersecurity frameworks.	Geared toward service providers and organizations managing third-party data in the cloud, particularly those in IT, healthcare, and financial services sectors.	Specifically for U.S. law enforcement, criminal justice agencies, and third-party vendors working with these agencies, ensuring they meet strict criminal justice information protection standards.

Structure	Designed into 10 mandatory clauses and 4 Annex control areas which comprises of the people, technological, physical, and organizational controls.	It contains 20+ control families (e.g., access control, incident response, media protection) and supports a customizable, tiered approach based on the organization's risk profile.	Structured into five Trust Services Criteria (TSC): availability, security, confidentiality, processing integrity, and privacy. These 5 Trust Services Criteria are further expanding using SOC 2 Point of Focus.	Comprises of 13 policy areas such as information exchange agreements, incident response, access and many more control requirements for handling criminal justice information.
Certificatio	Certification is possible through an accredited third-party audit, providing formal recognition of compliance with ISO 27001 standards.	Certification is not formally available. Compliance can however be demonstrated through assessments or audits conducted by qualified third-party evaluators.	Formal attestation is provided by a certified auditor, typically a CPA, who issues a SOC 2 report (Type I or Type II) after evaluating the organization's controls.	There is no certification, but compliance is verified through audits by CJIS representatives or law enforcement agency personnel.
Industry	Cross-industry, applicable to any organization seeking to implement robust information security practices.	Primarily U.S. federal agencies and government contractors, though adopted by other industries such as finance, healthcare, and critical infrastructure.	Most common in cloud services, technology, healthcare, and financial sectors where third-party data handling is crucial.	Specific to U.S. criminal justice, law enforcement agencies, and associated vendors.
Availability	Available globally and used internationally. Organizations can access the standard through ISO publications.	Publicly available through NIST's website, accessible to any organization aiming to enhance security measures.	Private standard, though widely accessible for organizations that hire certified auditors to perform SOC 2 assessments.	Publicly available on the FBI Website allowing vendors to access it when collaborating with criminal justice agencies.

4. Overview of Control Areas

This section provides a detailed overview of the various control areas and policy families associated with each standard and framework.

4.1. ISO/IEC 27001:2022 Annex Controls

ISO/IEC 27001:2022 being the most recent version by ISO, is designed and organized into four key domain areas, referred to as Annex controls [5]. The ISO 27001:2022 version is an upgrade of the ISO 27001:2013 which comprises ninety-three controls across four control areas compared to one hundred fourteen controls across fourteen categories of the 2013 version. The ISO27001:2022 four Annex Controls Include:

- Organizational controls (Annex 5): focuses on helping organizations manage the implementation and behaviour of the people, software, hardware and systems that make up the information security management system. This annex comprises of thirty-seven controls, focused on essential components that build an effective information system management system (ISMS).
- People control (Annex 6): focuses on developing policies and procedures to govern how personnel and employees use and handle information and information systems. This control area consists of eight controls focused on ensuring human resource security. Annex 6 emphasizes the importance of implementing policies and processes for personnel background checks, security awareness training, disciplinary procedures, remote working policies, and many more.

- Physical controls (Annex 7): focuses on governing and ensuring a safe physical environment by minimizing the risk associated with organizational physical security. This control area comprises fourteen controls that address essential security issues like clear desk policies, storage procedures, access to information systems, and many more.
- Technological controls (Annex 8): aims to ensure and maintain a secure information system management system and consists of thirty-four controls. This control area was primarily concerned with technological controls such as encryption, firewalls, intrusion detection system (IDS) and intrusion prevention systems (IPS), network security and access control mechanisms, and many more.

4.2. NIST SP 800-53 REV. 5 Control Families

NIST SP 800-53 is an information security standard designed to provide security and privacy controls that will help organizations strengthen their information security posture. NIST SP 800-53 is made up of twenty control families that are designed to give organizations comprehensive steps to protect the various aspects of information security. This standard covers twenty control families, some of which include access control, system and communications protection, configuration management, incident response, supply chain risk management, contingency planning, etc.

4.3. SOC 2 Trust Service Criteria

System and Organization Controls 2 (SOC2) is one of the popular compliance frameworks, and it is designed by the American Institute of Certified Public Accountants (AICPA). SOC 2 is structured and built on five major Trust Service Criteria (TSC), which cover the various components and aspects of information security. These five Trust Service Criteria include:

- Security: This is focused on ensuring that information is adequately protected through the implementation of physical, logical, and administrative controls such as firewalls, IDS/IPS, multi-factor authentication, and many more.
- Availability: focuses on ensuring that information and services are accessible to users whenever it is needed. This criteria involves implementing measures such as implementing and configuring redundant or failover systems, having appropriate data backup in place, and essentially planning for disaster recovery and business continuity, as well as many other measures.
- Processing integrity: focuses on ensuring that the system processing is accurate, timely, valid, and authorized. This involves ensuring that processes are being monitored, and error check and validation processes are implemented.
- Confidentiality: as part of the CIA triad, it ensures that information is protected by implementing the proper security measures to ensure that confidential information is always protected from unauthorized users. This involves implementing security measures like access control, user authentication, and many more.
- Privacy: is another important aspect that is often overlooked; it entails organizations implementing policies and measures to ensure the secure collection, use, retention, disclosure, and disposal of information in the best way possible.

4.4. US CJIS Policy Areas

US Criminal Justice Information Services (CJIS) is a security policy that is designed by the Federal Bureau of Investigation (FBI) and intended to provide organizations with specific guidelines, requirements, and best practices for the protection and sharing of information. US CJIS is designed and structured into thirteen different policy areas and technical requirements, with each policy area having its own sub-policies that make up each policy area [8].The thirteen policy areas include Information exchange agreement, Security awareness training, Incident Response, Auditing and accountability, Access Control, Identification and authentication, Configuration management, Media protection, Physical Protection, System and communication protection and information integrity, Formal audits, Personnel Security, Mobile devices.

5. Detailed Mapping of Control Areas

This section presents detailed table mapping of ISO 27001:2022 controls to NIST SP 800-53 Rev. 5 Policy Families, US CJIS Security Policy, and the Trust Service criteria of SOC2. To perform this comparative analysis, data was collected

and scrutinized to identify overlap and uniqueness between standards from these sources: ISO 27001:2022 [5], NIST SP 800-53 Rev 5 [6], US CJIS Security Policy [8], SOC 2 [7].

5.1. Organizational Controls Mapping to NIST SP 800-53 Rev. 5, US CJIS, and SOC 2

The mapping of ISO/IEC 27001:2022's thirty-seven organizational controls to NIST SP 800-53, US CJIS, and SOC 2 as represented in Appendix I highlights significant similarities. Annex 5 of ISO/IEC 27001:2022 underscores defining roles, responsibilities, and implementing policies for effective information security governance. The mapping reveals a shared emphasis across standards on robust incident management, strong access control policies, and secure information exchange. By leveraging this alignment, service provider SMEs can streamline compliance with multiple frameworks and enhance their information security management systems.

5.2. People Controls Mapping to NIST SP 800-53 Rev. 5, US CJIS, and SOC 2

The comparison of ISO/IEC 27001:2022 people controls to NIST SP 800-53, US CJIS, and SOC 2 in Appendix II reveals significant overlap, with all standards emphasizing personnel controls. Annex 6 of ISO/IEC 27001:2022 outlines managing personnel, their interactions, and handling information, assets, and security systems. The analysis highlights that these standards prioritize mitigating human-related risks, recognizing people as the weakest link in security. Aligning people control requirements helps SMEs establish a strong defense against human-related threats.

5.3. Physical Controls Mapping to NIST SP 800-53 Rev. 5, US CJIS, and SOC 2

Appendix III maps the physical controls of ISO/IEC 27001:2022 (Annex 7) to NIST SP 800-53 Rev. 5, US CJIS, and SOC 2. Annex 7 focuses on safeguarding physical perimeters, equipment, and utilities. The mapping highlights alignment across the standards in emphasizing physical security, environmental protection, asset and workspace security, infrastructure protection, and secure disposal or reuse of equipment. These complementary measures enhance physical security across frameworks.

5.4. Technological Controls Mapping to NIST SP 800-53 Rev. 5, US CJIS, and SOC 2

Appendix IV maps ISO/IEC 27001:2022 Technological Controls (Annex 8) to NIST SP 800-53 Rev. 5, US CJIS, and SOC 2. Annex 8 focuses on securing systems, networks, and data storage, ensuring resilience, data integrity, and access control. These controls align with NIST's system and communications protection, CJIS's data protection, and SOC 2's security and availability criteria. The frameworks collectively highlight the importance of a layered approach to safeguarding digital assets and resources.

6. Challenges with Implementing Multiple Standards and Frameworks

For SMEs the challenge lies in balancing the need to protect sensitive customer data, the constant need to maintain trust and a solid reputation among customers and stakeholders, and the pressure to adhere to multiple frameworks and standards that will ultimately lead to them achieving their objective. One of the biggest challenges SME service providers faces when having to comply and implement multiple standards and frameworks, is limited resources. For example, CrowdComms a UK based tech company's customers were initially interested in ISO 27001 but due to business expansion to the US and to be onboarded as a vendor the organization needed to obtain and maintain SOC 2 but faced the issue of limited resources [11]. In addition to the challenge surrounding the lack of resources, expertise and specialized knowledge in areas like legal, IT, and cybersecurity are essential to effectively implement these standards, but many SMEs cannot afford to hire experts or outsource these services, leaving compliance gaps and leaving these organization susceptible to threats [2].

Furthermore, the complexity of managing and implementing multiple frameworks adds to the challenge for SMEs, as many requirements overlap but are implemented differently across standards [9]. For example, ISO 27001:2022 and NIST 800-53 emphasize the importance of access control to safeguard sensitive data. While ISO 27001 Annex 5.15 focuses on establishing broad access control policies to ensure only authorized personnel can access information, NIST 800-53 goes further by providing detailed controls, such as AC-2, which outlines specific user authentication and role-based access requirements. In addition to this, keeping up with the rapid evolution of regulatory standards also complicates the process of

implementing information security standards and achieving compliance. Regulatory bodies regularly update controls to address emerging threats and technologies, necessitating businesses to adapt their policies, systems, and employee training. For example, ISO 27001 reduced its Annex controls from one hundred fourteen in the 2013 version to ninety-three in the 2022 update [5]. While these changes enhance security, they can place significant strain on organizations, particularly SMEs with limited resources already focused on daily operations.

Another major issue with implementing multiple standards is that compliance initiatives are often time consuming and require substantial effort to assess risks, implement policies, and train employees effectively. For SMEs, this can become a major challenge, as they are often juggling numerous operational priorities with limited resources. Finally, employee training is another crucial aspect of compliance, but it can be particularly burdensome for organizations, especially SMEs with limited staff. Ensuring that employees understand compliance policies and adhere to security practices often requires extensive training programs and regular refresher courses.

6. Recommendation for Multi-Framework/Standard Compliance

To address the highlighted challenges, this section presents some recommendations and practical strategies that will help organizations be able to achieve multi-framework/standard compliance. One of the major steps organizations can take to ensure multi-framework compliance is by conducting a comparative analysis and mapping of standards and frameworks. This helps organizations to effectively plan by mapping out the overlapping areas and unique requirements across the various frameworks and standards [9]. This solution helped CrowdComms streamline their process of achieving both ISO 27001 certification and SOC 2.

Following the development of a unified framework, organizations should always ensure that they approach the standards implementation from a risk-based approach. A risk-based approach is a methodology that focuses on the identification, assessment and mitigation of information security risk based on the likelihood and potential impact on the organization's assets [10]. This is important because most, if not all, information security standards are designed to be implemented from a risk-based approach. Therefore, if the organization adopted an integrated risk management approach or strategy, they would effectively be able to implement risk mitigation and management strategies that align with security measures that exist across the various frameworks and standards. In addition to the recommendations mentioned, working smart can also hugely benefit an organization trying to achieve multi-framework compliance. They can achieve this through the use of automation tools and software. These tools will allow organizations implementation teams to be able to streamline the process of implementing requirements as seen in the CrowdComms case study where they utilized Vanta a compliance automation tool to monitor and maintain adherence to both standards [11].

Achieving compliance with various information security standards can be a task and requires expertise. While organizations try to ensure compliance with multiple frameworks and standards, it is important and non-negotiable that organizations create implementation teams that are cross-functional and can have expertise in the various standards or frameworks, and these teams are able to be trained. This ensures that knowledge is shared and having a cross-functional implementation team will help with the implementation of various frameworks or standards.

7. Conclusion

Information security standards provide SMEs with a structured approach to strengthening their security posture. Using ISO/IEC 27001:2022 as a baseline, this paper examined the alignment and overlapping control areas among major frameworks. The analysis highlighted how these frameworks complement or diverge from one another, providing insights into their respective strengths and limitations in a multi-framework environment. Key findings indicate that while the shared objective of enhancing security is clear, organizations face notable challenges including resource constraints, lack of expertise, and complexity in aligning multiple standards. Addressing these issues requires a strategic approach that includes adopting risk-based thinking, improving documentation, and utilizing automation to simplify compliance. Future research could explore the development of unified control mappings tailored to specific industries, or the creation of compliance frameworks designed specifically for SMEs. Additionally, case studies on successful multi-framework implementations can

provide valuable real-world insights. By focusing on shared controls and aligning efforts with business objectives, SMEs can reduce redundancy, enhance efficiency, and build a more resilient security program.

Acknowledgements

This research is funded by Mitacs Canada (https://www.mitacs.ca/) and Technology North Corporation (https://www.technologynorth.net/)

References

[1] ISACA, "9 in 10 Enterprises Report Gaps Between the Cybersecurity Culture They Have and the One They Want," *ISACA*, Oct. 15, 2018. https://www.isaca.org/about-us/newsroom/press-releases/2018/9-in-10-enterprises-report-gaps-between-the-cybersecurity-culture-they-have-and-the-one-they-want (accessed Dec. 07, 2024).

[2] H. Taherdoost, "Understanding Cybersecurity Frameworks and Information Security Standards—A Review and Comprehensive Overview," *Electronics*, vol. 11, no. 14, p. 2181, Jul. 2022, doi: https://doi.org/10.3390/electronics11142181.

[3] K. Beckers, I. Côté, S. Fenz, D. Hatebur, and M. Heisel, "A Structured Comparison of Security Standards," *Engineering Secure Future Internet Services and Systems*, pp. 1–34, 2014, doi: https://doi.org/10.1007/978-3-319-07452-8_1.

[4] G. Wangen and E. A. Snekkenes, "A Comparison between Business Process Management and Information Security Management," *Annals of Computer Science and Information Systems*, vol. 2, pp. 901–910, Sep. 2014, doi: https://doi.org/10.15439/2014f77.

[5] International Organization for Standardization, "Information security, cybersecurity and privacy protection -Information security management systems - Requirements," Oct. 2022. Available: https://www.iso.org/standard/27001

[6] National Institute of Standards and Technology, "Security and Privacy Controls for Information Systems and Organizations," *Security and Privacy Controls for Information Systems and Organizations*, vol. 5, no. 5, Sep. 2020, doi: https://doi.org/10.6028/nist.sp.800-53r5.

[7] "2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy," *Guide*, pp. 171–220, May 2020, doi: https://doi.org/10.1002/9781119723448.oth2.

[8] "Criminal Justice Information Services (CJIS) Security Policy," *Federal Bureau of Investigation*, Jun. 16, 2020. https://www.fbi.gov/file-repository/cjis_security_policy_v5-9_20200601.pdf/view (accessed Dec. 06, 2024).

[9] F. Djebbar and K. Nordström, "A Comparative Analysis of Industrial Cybersecurity Standards," *IEEE Access*, vol. 11, pp. 85315–85332, 2023, doi: https://doi.org/10.1109/access.2023.3303205.

[10] M. N. Aleksandrov, V. A. Vasiliev, and S. V. Aleksandrova, "Implementation of the Risk-based Approach Methodology in Information Security Management Systems," *2021 International Conference on Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS)*, pp. 137–139, Sep. 2021, doi: https://doi.org/10.1109/ITQMIS53292.2021.9642767.

[11] H. Errico, "How Vanta customers use ISO 27001 and SOC 2 together," *Vanta*, Dec. 11, 2023. https://www.vanta.com/resources/how-to-use-iso-27001-and-soc-2-together (accessed Apr. 07, 2025).