ISSN-P: 2807-5987

"A comparative study of NIST 800-53 Framework and the ISO 27001 Information Security Frameworks"

ISSN-E: 26632806

ISSN-P: 2807-5987

ABSTRACT

The National Institute of Standards and Technology (NIST) is currently revising its Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations. It's important to note that NIST did not establish this framework to defend private industry. NIST 800-53 best practices have, however, become the de facto standard for private enterprises doing business with the United States federal government as a result of widespread outsourcing to private companies and substantial regulation of businesses. Keep in mind that NIST 800-53 is a superset of ISO 27002, which implies that you will find all of the ISO 27002's components covered by NIST 800-53. " There are some aspects of NIST 800-53 that ISO 27002 does not cover: The additional needs for compliance that NIST over ISO can cover are nicely depicted in the accompanying diagram.

The search was refined according to inclusion criteria to restrict the returned studies to those competent to respond to the aims of this literature review. The initial search was initially undertaken in January 2022, with content retrieved and vetted for inclusion during February 2022 and March 2022. For the sake of including recently published articles, the search was redone in April 2022.

الملخص:

يقوم المعهد الوطني للمعايير والتكنولوجيا (NIST) حاليًا بمراجعة إصداره الخاص 800-53 ، ضوابط الأمان والخصوصية لأنظمة المعلومات الفيدرالية والمنظمات. من المهم ملاحظة أن المعهد القومي للمعايير والتكنولوجيا (NIST) لم يؤسس هذا الإطار للدفاع عن الصناعة الخاصة. ومع ذلك ، أصبحت أفضل ممارسات NIST 800-53 هي المعيار الفعلي للمؤسسات الخاصة التي تتعامل مع الحكومة الفيدرالية للولايات المتحدة نتيجة الاستعانة بمصادر خارجية واسعة النطاق للشركات الخاصة والتنظيم الجوهري للأعمال. ضع في اعتبارك أن NIST 800-53عبارة عن مجموعة شاملة من ISO 27002 ، مما يعني أنك ستجد جميع مكونات ISO 27002 مغطاة بـ NIST 800-53. " هناك بعض جوانب NIST 800-53 التي لا تغطيها ISO 27002: الاحتياجات الإضافية للامتثال التي يمكن أن تغطيها NIST عبر ISO موضحة جيدًا في الرسم التخطيطي المصاحب.

تم تنقيح البحث وفقًا لمعايير التضمين لقصر الدراسات المعادة على تلك المختصة للاستجابة لأهداف مراجعة الأدبيات هذه. تم إجراء البحث الأولي في يناير 2022 ، مع استرداد المحتوى وفحصه لإدراجه خلال فبراير 2022 ومارس 2022. من أجل تضمين المقالات المنشورة مؤخرًا ، أعيد البحث في أبريل 2022.

ISSN-E: 26632806

ISSN-P: 2807-5987

TABLE OF CONTENTS

ISSN-E: 26632806

ISSN-P: 2807-5987

Chapter 1: Project Outlines

1.0. Introduction

Rather than creating and maintaining a unique information risk management framework, many organizations have come to the realization that they would be better served by adopting and maybe customizing an existing framework. This is just one of several choices that must be made. There are a number of complete frameworks that you can choose from depending on your organization's demands.

The National Institute of Standards and Technology (NIST) is currently revising its Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations. It's important to note that NIST did not establish this framework to defend private industry. NIST 800-53 best practices have, however, become the de facto standard for private enterprises doing business with the United States federal government as a result of widespread outsourcing to private companies and substantial regulation of businesses. Keep in mind that NIST 800-53 is a superset of ISO 27002, which implies that you will find all of the ISO 27002's components covered by NIST 800-53. " There are some aspects of NIST 800-53 that ISO 27002 does not cover: The additional needs for compliance that NIST over ISO can cover are nicely depicted in the accompanying diagram.

It is necessary for US federal government suppliers to meet NIST 800-53 requirements in order to pass demanding certification programs such as FISMA (Federal Information Security Management Act) and DIARMF (Department of Defense Information Assurance Risk Management Framework). It's also included in NIST 800-171, Protecting Controlled Unclassified information in nonfederal information systems and organizations as an example of how government contractors should protect their systems. In the eyes of US government contractors, this only serves to reinforce the status of NIST 800-53 as a best practice.

Additionally, NIST 800-53 addresses a slew of other issues not covered by ISO 27002 or the NIST CSF. The controls found in NIST 800-171 / CMMC are based on NIST 800-53. It's typical to see NIST 800-53 in the financial, medical, and government contracting arenas. NIST 800-53, like other NIST publications, is freely available to the general public at no cost.

A non-governmental organization based in Switzerland, the International Organization for Standardization (ISO) is responsible for developing international standards. To retain their IT security publications in the 27000 series of its documentation catalogue, the International Organization for Standardization renamed ISO 17799 to ISO 27002 in 2007. ISO 27002 is a supplementary document that aids in the application of the ISO 27001 standard. Companies can only certify against ISO 27001 and not ISO 27002, which adds to the misunderstanding. However, ISO 27002 outlines the precise controls required to put ISO 27001 into practice. ISO 27001 Appendix A offers an overview of the security controls required to construct an Information Security Management System (ISMS).

As a quick reminder, ISO 27001 establishes the framework for a "Information Security Management System" (such as the creation of a comprehensive IT security program), while ISO 27002 specifies the specific "best practices" for putting together such a comprehensive IT security system. As a result of ISO's information security framework's existence since the mid-1990s, it has become the de facto IT security framework outside of the United States. Multinational organizations and companies that don't have to adhere to US federal restrictions frequently employ ISO 27002. In addition to being "less paranoid," ISO 27002 is also simpler to implement than NIST 800-53.

Security framework ISO 27002 provides coverage for a wide range of common criteria and is widely recognized around the world (e.g., PCI DSS, HIPAA, etc.). Unfortunately, ISO charges for all of its publications, and this applies to ISO 27002 as well.

ISSN-P: 2807-5987

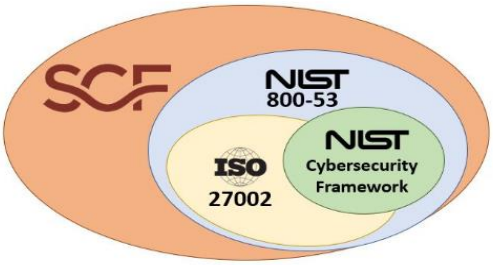

Figure 1: Security framework ISO 27002

Table 1: differences in compliance forge products between NIST CSF and ISO 27002

ComplianceForge Products	NIST CSF	ISO 27002
Cybersecurity & Data Protection Program (**CDPP**) or Digital Security Program (**DSP**)	ID.GV-1 [multiple sections]	5.1.1 [multiple sections]
Supply Chain Risk Management (**SCRM**)	ID.SC-1	15.1.1
Cybersecurity Risk Management Program (**RMP**)	ID.GV-4 ID.RA-5 ID.RM-1 ID.RM-2 ID.RM-3	11.1.4
Cybersecurity Risk Assessment Template (**CRA**)		
Vulnerability & Patch Management Program (**VPMP**)	ID.RA-1 PR.IP-12	12.6.1
Integrated Incident Response Program (**IIRP**)	PR.IP-9	16.1.1
Security & Privacy By Design (**SPBD**)	N/A	N/A
System Security Plan (**SSP**) & **POA&M**	N/A	N/A

ISSN-E: 26632806

ISSN-P: 2807-5987

Cybersecurity Standardized Operating Procedures (**CSOP**)	PR.IP-5 [multiple sections]	12.1.1 [multiple sections]
Continuity of Operations Plan (**COOP**)	RC.RP-1	17.1.2
Secure Baseline Configurations (**SBC**)	PR.IP-1 PR.IP-3	14.1.1
Information Assurance Program (**IAP**)	N/A	14.2.8
Cybersecurity Business Plan (**CBP**)	N/A	N/A

2.0. Research problem

The NIST Cybersecurity Framework and the ISO 27001 standards have a lot in common. As a flexible framework, this guideline can be used by any firm that relies substantially on technology, from standard information systems to the Internet of Things. Using the NIST framework, firms can tailor their cybersecurity measures based on their specific goals and the unique difficulties they encounter.

Information security and risk management are addressed in different ways by NIST and ISO 27001. If an organization already has a cybersecurity strategy in place, those are all factors to consider when making a decision on which cybersecurity solution to implement. The two standards have a significant amount of overlap, which offers organizations with broad guidance and similar protections, no matter which they chose. An Information Security Management System Consultant can assist a corporation in determining which standard to adhere to.

A key source of threats to the security system is the existence of security gaps in its systems, which can jeopardize the confidentiality, safety, and accessibility of the system's most important assets. When employees have access to highly sensitive data, such as accounts and records, they may not be aware of the risks of using these technologies properly, which can lead to the same kinds of problems as the ones described above if they do so with or without intent. Even without a comprehensive risk assessment, administration should have a strategy in place to safeguard assets and minimize threats to them. Organizations need to upgrade their information security systems in accordance with international standards in order to keep up with the times. Step one is a self-assessment known as gap-measurement of the reality of information security (Leem, et al., 2005; Krisanthi, et al., 2014).

The following research question is formulated from the research's main problem:

According to the international standard (ISO/IEC: 27002:2013) and NIST 800-53 Framework, what is the gap in the actual situation of information security in the organizations?

In light of this problem, the following sub-questions arise:

- To what extent are organizations in compliance with the information security requirements of ISO / IEC 27001: 2013 international standards and NIST 800-53 Framework?
- What is the gap between the existing level of information security practices in organizations and the level of information security practices that organizations want to attain according to the criteria of ISO / IEC: 27001: 2013 and NIST 800-53 Framework?
- What controls are the most vulnerable points bringing about potential threats, and what solutions can be recommended to improve them?

ISSN-E: 26632806

ISSN-P: 2807-5987

3.0. The Recommended Solution

It is vital to understand that a cybersecurity framework decision is a business decision rather than a technological decision. Choosing a cybersecurity framework should be guided by your organization's legal, regulatory, and contractual obligations, because this knowledge determines the minimum set of needs essential to:

- Due diligence and due care must be demonstrated in order to avoid being regarded as negligent in terms of "reasonably-expected" security and privacy standards.
- Protect the organization's systems and applications from reasonable risks by implementing the necessary security policies.

The more controls there are, the more difficult it may be to install, but it may not give the necessary security features that the business requires. A company's risk profile dictates how to define "just right," which means taking into account relevant laws, regulations, and contractual obligations in order to support current or projected business activities.

4.0. Clear Statement of the Aim

This comparative study aims mainly to determine the gap in the actual situation of information security in the organizations according to the criteria of ISO / IEC: 27001: 2013 and NIST 800-53 Framework. The advantages and disadvantages of each framework over other will be studied in detail. The selection of appropriate framework will also be investigated along with discussion on how main security controls guidelines can be mapped to each other.

5.0. Clear Statement of the Objectives

- Determine extent to which organizations are in compliance with the information security requirements of ISO / IEC 27001: 2013 international standards and NIST 800-53 Framework
- Determine the gap between the existing level of information security practices in organizations and the level of information security practices that organizations want to attain according to the criteria of ISO / IEC: 27001: 2013 and NIST 800-53 Framework
- Determine the controls are the most vulnerable points bringing about potential threats, and what solutions can be recommended to improve them.

6.0. Project plan

6.1. Clear Tasks Clarification

ID	Task Name
1	Introduction
2	Literature Review
3	Methodology
4	Results and Discussion
5	Final Report Submission

6.2. Tasks Duration

Task	1	2	3	4	5	6	7	8	9	10	11	12
Prepare proposal												
Make research plan												
Literature search										Ref. check		
Critical analysis												
Writing the review				Early draft		Second draft			Final draft			
Selecting method												
Designing research tools												
Draft introduction												

ISSN-E: 26632806

ISSN-P: 2807-5987

Collecting data												
Analyzing data												
Draft method section												
Draft result section												
Draft discussion												
Write final report												
Submit report												
Reflection												

Chapter 2: Literature review

1.0. Background on information security

For modern companies, ensuring the safety, accessibility, and confidentiality of sensitive data is critical, which is why information security solutions have taken on such importance (Krisanthi, et al., 2014; Itradat, et al., 2014; Ermana, F.H. and Tanuwijaya Mastan, I., 2012; Karabacak, B. and Sogukpinar, I., 2006; Leem, et al., 2005). By establishing and implementing information security plans in a proactive and successful manner, they must also pay particular attention to their management (Chang, S.E. and Lin, C.S., 2007). Establishing and implementing systems that address the potential internal and external threats that an organization faces necessitate following specific rules (Krisanthi, et al., 2014; Tipton, H.F. and Krause, M., 2007).

Technical solutions are important for the organization and should be implemented properly to combat threats and risks or to automate some processes, such as using firewalls in organizations systems (Krisanthi, et al., 2014; Chang, S.E. and Lin, C.S., 2007; Tipton, H.F. and Krause, M., 2007; Martins, A. and Elofe, J., 2002). People are required to operate and manage technical solutions; simply implementing information security technical solutions will not suffice. Security measures are only as good as the people who develop and manage them, as well as the administrative policies and practices that govern their use (Martins, A. and Elofe, J., 2002; Andress, M. and Fonseca, B., 2000; Solms, B.V., 2000). Users are constantly interacting with technology and information assets in order to carry out their jobs, and the risks that are user-oriented have a greater influence on the company than external risks (Martins, A. and Elofe, J., 2002; Dhillon, G., 2001; Gaunt, N., 2000; Venter, H.S. and Eloff, J.H.P., 2000).

To safeguard their business and technical infrastructure from information security threats, organizations must implement an integrated strategy that combines information security and organizational culture by establishing security practices and procedures as documented practical and technical bases (Chang, S.E. and Lin, C.S., 2007; Tipton, H.F. and Krause, M., 2007; Martins, A. and Elofe, J., 2002; Dhillon, G., 2001; Andress, M. and Fonseca, B., 2000; Gaunt, N., 2000; Solms, B.V., 2000; Venter, H.S. and Eloff, J.H.P., 2000).

Using procedures that outline the precise steps to be followed in the event of an external security breach, and by applying information security culture, such as the practices that determine the mechanism in which controls are implemented, and working on it by the user, helps to protect against the risks of internal threats and breaches. For this reason, the international organizations sought to adopt specific security policy standards that draw up an integrated policy to put the concept of information security into practice at institutions, from the analysis of risks to the implementation of security controls to minimize these risks (Itradat, et al., 2014; Krisanthi, et al., 2014; Ermana, F.H. and Tanuwijaya Mastan, I., 2012; Ifinedo, P., 2012; Karabacak, B. and Sogukpinar, I., 2006; Leem, et al., 2005).

Any company's risk assessment depends greatly on the nature of their business and the structure of their technology. Organizations' practical and technical aspects must be taken into account in order to identify information security risks and areas of related policy that are applicable to these organizations. The classification of policies is based on their own controls, such as access control and continuity of work and international standards compliance.

Health, information Trust Alliance (HITRUST) programs and services are built on the HITRUST CSF, which is a certifiable framework that provides enterprises worldwide with a comprehensive, adaptable, and efficient approach to regulatory/standards and risk management. This comprehensive security and privacy framework was created in consultation with industry experts in the field of data protection. Due to the fact that HITRUST CSF is both risk and compliance driven, businesses of all sizes, types, and systems can tailor the security and privacy control baselines depending on a wide range of criteria. The organization's information security management program will benefit from HITRUST's integrated approach to data protection compliance since we understand the problems of putting together and managing a wide range of programs. Since then, HITRUST CSF has grown to be an industry-wide standard for information security and privacy.

Information security management strategies have been refined through time. The ISO 7799 standard, the revised ISO 27000 standard, Control Objectives for Information and Related Technologies (COBIT), the Information Technology Infrastructure Library (ITIL), as well as national guidelines for information security, such as NIST 800-53, are among the most important of these.

A growing number of studies have revealed that these standards and recommendations are increasingly being implemented around the world in order to help organizations improve their information security while also meeting the demands of national and international legal and auditing bodies. Implementing an organization's structure for information security management necessitates following a set of security compliance regulations (Candiwan, C., 2014; Itradat, et al., 2014; Al-Mayahi, I. and Sa'ad, P.M., 2012; Karabacak, B. and Sogukpinar, I., 2006).

2.0. Overview of ISO 27000: 2013

As there are common worldwide security standards accessible, they provide a systematic management method for adopting best practice controls to quantify the amount of risk and execute the relevant procedures to safeguard confidentiality, integrity and availability (CIA) (Tipton, H.F. and Krause, M., 2007), NIST 800-53, BS7799 (COBIT), and ITIL (Knapp, et al., 2009). In 1995, the British Standard Institute (BSI) established the BS 7799 standard (Candiwan, C., 2014; Andress, M. and Fonseca, B., 2000; Solms, B.V., 2000). It was in 2000 that ISO 17799 was created from the BS7799 standard. Code of conduct and specifications for an Information Security Management System (ISMS) were defined in ISO 17799 Part 2 (2002). (Tipton, H.F. and Krause, M., 2007; Solms, B.V., 2000).

The worldwide standard for information security management, ISO/IEC 27001, defines a set of controls and standards to establish, implement, operate, monitor, review, maintain, and enhance an information security management system (ISMS). It has been designed to reemphasize the ISO 17799 code with a few amendments and additional controls that will further enhance and improve the ISMS (Tipton, H.F. and Krause, M., 2007; Dey, M., 2007). To replace the first edition of the standard that was issued in 2005, ISO/IEC 27001:2013 was issued.

ISO27001 has a key characteristic that it:

- Information security management, as defined by the ISO27001 standard and the way it is implemented and maintained, is covered by this standard, regardless of company size (Susanto, A. and Shobariah, E., 2016; Candiwan, C., 2014; Mayer, N., 2010; Arnason, S.T. and Willett, K.D., 2007);
- When it comes to information security, a key feature of ISO27001 is that it applies to all kinds of organizations, no matter how large or small they are (Susanto, A. and Shobariah, E., 2016; Candiwan, C., 2014; Mayer, N., 2010; Arnason, S.T. and Willett, K.D., 2007).
- It also identifies the key components of information security management, as well as the methods by which they are implemented and maintained (Itradat, et al., 2014).
- Provides instructions on how to obtain foreign certificates from a third party (Susanto, A. and Shobariah, E., 2016; Dey, M., 2007; Solms, B.V., 2000; Arnason, S.T. and Willett, K.D., 2007).
- Proof that the security controls are in place and functioning as required by the standard was needed (Susanto, A. and Shobariah, E., 2016; Arnason, S.T. and Willett, K.D., 2007).
- An ISMS is a risk management system that strives to establish, implement, run and monitor and maintain the entire management of business risk.

3.0. Overview of NIST 800-53

Security and privacy controls for federal information systems and organizations are recommended by NIST SP 800-53. (excluding those in national security). To simplify NIST 800-53's 272 recommended security measures, NIST has published SP 800-171, a simplified version with 114 controls that contractors can implement. Risk Management Framework (RMF) for information systems, organizations, and persons is developed by NIST SP 800-37. The first NIST publication to cover both security and privacy risk management was produced in response to executive branch mandates to strengthen federal networks and assets. The RMF relies on NIST SP 800-53's control catalogue.

4.0. Critical Analysis

ISO/IEC 27001 was adopted as the foundation for CSF controls because HITRUST recognised that healthcare is global and needed guarantees about the safety of protected information from non-US affiliates. It provides an international standard for the development and maintenance of an information security management system (ISMS) with high-level controls designed to suit practically any company, in any industry, and in any region.

Non-government organisations can also benefit from NIST 800-53 and ISO/IEC 27001 standards for information security, which were originally created for the federal government. Since no single industry is specifically addressed by these frameworks, ISO/IEC 27799 and NIST SP 800-66 both explore how to apply their frameworks to healthcare settings in different documents.

However, the HITRUST CSF provides an integrated set of comprehensive security measures developed from several legal requirements applicable to U.S. healthcare, as well as generally established information security standards and best practices, including as ISO/IEC 27001 and NIST SP 800-53. HITRUST CSF NIST SP 800-53 helps the CSF verify FISMA-compliance, which is commonly required when firms get healthcare funding or contracts from the US government.

As part of the CSF's thorough guidance on the assessment of control maturity and the evaluation of excessive residual risk, the CSF provides extensive support for remediation planning and reporting. Service organization controls (SOC) 2 reporting under the American Institute of Certified Public Accountants (AICPA) Trust Services Principles can also be done using the HITRUST CSF. Since its inception in 2009, the HITRUST CSF has developed and evolved to include more than 40 authoritative sources from around the world and across different industries.

As the regulatory or threat environment changes, HITRUST reviews source frameworks and best practices to keep the CSF current. While ISO/IEC 27001 and NIST SP 800-53 changes are issued less regularly and may not always match new federal or state legislation and regulations, the CSF is updated on an annual basis (e.g., recent omnibus HIPAA rule making or Texas House Bill 300). Maintaining the CSF is an ongoing benefit to healthcare organizations because it saves them from having to develop and implement their own unique frameworks to meet all of these different standards and best practices.

International and domestic standards and best practices form the basis of the CSF, which may be tailored to fit a wide range of organizations and systems of all sizes. The risk factors of an organization and its systems are used to identify the controls that are regarded "in scope," and each of these controls has up to three levels of implementation requirements. As a result, similar enterprises can count on the same degree of security and assurance at all times. The ISO framework does not allow for this level of uniformity because it permits each business to freely select controls without any scrutiny. When it comes to the NIST framework, the "high water mark" is established by the highest impact rating assigned to information stored, processed, or sent by the information system (s). The controls cannot be scaled to the size or kind of company employing the NIST framework by any formal mechanism.

As a result of these frameworks' differing approaches to scaling, organizations can tailor their own specialized restrictions. Even though an organization is of the same type and size, it may not be able to implement a specific control. A company's required controls might be tailored to address a specific risk or to offset the loss of system control.

High-level requirements are provided by ISO/IEC 27001, which can be flexibly adjusted by the enterprise. ISO/IEC 27001, on the other hand, allows for a greater degree of customization by allowing organizations to establish control parameters. Additional risks not considered when NIST defined the baseline, such as insider threats or advanced persistent threats, international legislation and federal or state regulations pertaining to specific types of information, are also expected to be added by organizations in the form of controls or enhancements.

An organization's control standards can also be reduced or eased based on a well-documented explanation that has been accepted by an approving authority. Exceptions only apply to that particular company, but they may have an impact on the risk that is borne by others as well (e.g., business partners and other third parties). Much like HITRUST and other contributing organizations, they started with NIST criteria and built an ISO-based framework before customizing control needs for the healthcare industry as a whole. NIST, on the other hand, does not explicitly demand HITRUST's evaluation and approval of any control specification that deviates from NIST's standard controls. To enable consistent application of information security measures and risk assessment across various enterprises, controlled tailoring is similar to managed scaling.

A control compliance-based framework like NIST or HITRUST is common to both. Using a gap analysis, an organization or system's risk can be determined. A quality program audit is often conducted in a similar manner to an ISO audit, which is a management or process model for the ISMS. Because the effectiveness of the controls the ISMS supports can be certified without being extensively vetted, there is an assurance gap.

NIST, on the other hand, takes a system (bottoms-up) approach to security, whereas HITRUST and ISO take an organizational (top-down) approach. As a result, HITRUST and ISO are able to certify enterprises, although NIST normally does not. In addition, only HITRUST's shared control definition, assessment, and reporting framework formally offers third-party assurance. The HITRUST framework is built on the ISO/IEC 27001 control clauses to assist the implementation and assessment of information security and compliance risk for offshore business associates, while NIST standards are integrated into the CSF.

Across order to ensure global application in a wide range of industry areas, ISO's assessment methodology is designed to be very general. The ISO/IEC 27005 standard offers some pointers for performing risk assessments and analyses, but it makes no recommendations for a particular approach. An information security risk management program can be implemented and maintained using NIST's Risk Management Framework (RMF), which gives detailed recommendations on a variety of areas. Except for NIST SP 800-66 r1, which may be applicable to private entities, the available guidance is aimed solely for the federal government because it is both overly technical and stringent. An information security control assessment approach that is compliant with NIST recommendations is provided by HITRUST. Each control in NIST's and HITRUST's frameworks has thorough assessment information, whereas the ISO framework only gives assessment guidelines for the ISMS in ISO/IEC 27008, which ISMS certification bodies are not obligated to utilize. Control-level assessment guidance is not provided by ISO/IEC 27001 or 27002, which provide further specificity surrounding controls.

Each organization has a distinct set of requirements that must be addressed when selecting a framework. As far as HITRUST is concerned, there is no other framework that can be customized to match the unique requirements of each enterprise. As part of a larger risk management framework, the NIST Framework for Improving Critical Infrastructure Cybersecurity for the healthcare industry is supported by HITRUST's CSF and CSF Assurance Program and is a model implementation of the President's Executive Order on Improving Critical Infrastructure Cybersecurity. It's simple to see why the CSF is undoubtedly the de facto framework for information security compliance and risk management after reviewing the most important features of ISO, NIST, and the CSF as given here.

Chapter 3: Methodology

1.0. Introduction

To make it easier to understand and utilize, this section goes into detail on the methods used to do research that includes information about the materials and tools used, as well as the stages that must be followed in a logical and methodical manner:

- Define the research purpose;
- examination of literature;
- stating of the search strategy;
- data collection and analysis, and finally,
- conclusions and recommendations are the phases involved in problem-solving research.

2.0. Methodology Framework

Descriptive methods will be used to examine the current system and determine its compliance with the international information security standard. Pertinent data will be used to have a clear picture of the all processes and conditions from the relevant responsible individuals (IT department manager, this department is responsible for all data processing operations, Human resource manager and Data Entry consultants), together with the review of documentary evidence in order to verify the compliance level of the main clauses, and the controls of Annex A in the standard.

The vast majority of security frameworks share a large number of controls, although this fact is often overlooked. As a result, businesses end up wasting time and money on unnecessary compliance measures. After completing your ISO 27001 certification, you've accomplished 60% of NIST CSF. If you've adopted NIST CSF, you're already 78 percent of the road to achieving ISO 27001 certification.

Annex A.8.1 of ISO27001, which recognizes asset responsibility, and ID.AM of NIST CSF, which recognizes asset management, both refer to keeping an asset registry. This is an important area of overlap. Control catalogues for NIST frameworks and ISO 27001 Annex A provide 14 control categories with 114 controls, as well as 10 management clauses to aid enterprises through their ISMS implementation process.

Rather than being overly technical, ISO 27001 places greater focus on risk-based management and gives best practices for securing all data. NIST CSF may be more appropriate for firms that are just beginning to create a cybersecurity risk management program or are working to mitigate data breaches. The ISO 27001 gives an excellent certification option for organizations that are operationally mature.

This paper aims to determine the gap in the actual situation of information security in the organizations according to the criteria of ISO / IEC: 27001: 2013 and NIST 800-53 Framework. The advantages and disadvantages of each framework over other will be studied in detail. The selection of appropriate framework will also be investigated along with discussion on how main security controls guidelines can be mapped to each other.

2.1. Research Design

The ability of a systematic literature reviews to summarize current knowledge in a certain topic by picking publications that meet predetermined criteria led to its selection as a method (Oxman 1994; Eriksson and Lindstrom 2005). Information risk management framework appears to have gotten little attention despite a large body of research devoted to it.

Anecdotal reports and a clear operationalization of the notion have both been critiqued in the study of information risk management frameworks. To overcome these issues, the systematic technique used in this literature analysis only included empirical studies that included specific characterization and quantification of the phenomena. (Berry & Houston, 1993)

The development of the review was based on principles that attempt to guarantee that the retrieved information best addresses the research topic and most properly reflects the phenomena under inquiry (Oxman 1994).

The search was refined according to inclusion criteria to restrict the returned studies to those competent to respond to the aims of this literature review. The initial search was initially undertaken in January 2022, with content retrieved and vetted for inclusion during February 2022 and March 2022. For the sake of including recently published articles, the search was redone in April 2022.

Systematic data collection from members of an organization for a specific goal is carried out using this technique (Kraut 1996). The design, implementation, administration, and reporting back of data is critical to the research performance and may even be more essential than the actual results obtained (Kraut 1996).

This was conducted in the form of a systematic literature review by applying Guidelines for Performing Systematic Literature Reviews in Software Engineering introduced by Kitchenham et al. and Webster et al.

The steps in the review technique are below:

- Planning phase: At this point, it should be clear why a comprehensive and unbiased examination of the ISO/IEC 27001 standard and software engineering is needed.
- The second part of the planning was to specify the research questions by evaluating the nature and structure of the questions as mentioned in Section II-A.
- The last stage of the planning process was to establish a review protocol to specify the procedures that will be utilized to undertake the review and limiting the chance of a bias. We've broken our methodology down into four sections: Section II-B explains how we pick studies, Section II-C outlines how we select studies, Section II-D explains how we extract data, and Section II-E explains how we synthesize the data we extract.
- Conducting: The previous phase's research protocol outlined the steps that were implemented in this phase. We began by identifying the original, peer-reviewed studies that might directly address the research concerns. It's time to carefully record what we learned from the original research. Section III concludes with a descriptive synthesis of the primary research that summarizes the findings.
- Section IV of the final report summarizes the review findings presented in the results section.

2.2. Why did we choose this method?

The studies to date from the industry and academics tend to focus on the overall definition of the standard and such ex-positions are unsatisfactory because little is being added to the practicality of the ISMS framework. In order to put the standard into practice, organizations will need more generalizable findings than those found in the many studies

that have already been published. To better understand how companies are dealing with the ISO/IEC27001 standard and the difficulties they are encountering, IT Governance, a provider of IT compliance solutions to businesses, conducted an annual survey.

In the poll, 250 information security experts from 53 countries took part, with the majority of them either certified or striving towards certification (80 percent). Of those polled, 71% reported that they were regularly or occasionally asked by clients or potential clients for proof of their ISO/IEC 27001certification. Certification minimizes the frequency of customer audits because it demonstrates adherence to an internationally recognized standard. More than a third of those polled said they had difficulty deciphering the standard's criteria, while 28% said they had difficulty creating and maintaining the standard documentation. For 22% and 14% of the respondents, the most difficult activities included conducting an information security risk assessment and determining the necessary procedures.

From the commercial side, it is a relatively difficult and costly operation to identify the resources required to implement, measure, and manage information security. It is clear from our literature assessment that ISMS has failed to pique the interest of academics due to the paucity of research and innovative methods. Management systems on information security received very limited observation and research from the academic community despite the considerable demand from organizations in particular for IT, operational and compliance audits.

2.3. How to evaluate the main clauses and controls?

An information security management system (ISMS) is defined by ISO 27001, which is an international standard. An information security strategy based on risk is adopted by the Standard. Identifying and addressing information security issues necessitates the use of appropriate security controls. Annex A of the Standard lays out these measures of control in detail. The 114 controls of ISO 27001 Annex A are organized into 14 categories.

The purpose of this review is to gain a comprehensive understanding of the current state of the art in the ISMS, not to capture every method within it. We acknowledge there could be a number of different relevant approaches that consider other ISMS methodologies such as ISACA COBIT or NIST Cybersecurity Framework, however, the objective of this article is ISO/IEC 27001 standard and to attain a pretty complete conclusion within this issue. Information from the chosen examples should answer our study questions and have a positive impact on the ISO/IEC 27001 standard's development. The initial research of 285 papers were converged by learning their meta-data comprising title, abstract, keywords, and conclusion. A total of 95 papers met our objectives and intentions of our review, which led us to further analyses the complete text of a study.

The methodology used in this study was utilized in both the private and public sectors to investigate these claims. As part of a case study in Saudi Arabia, we defined the propositions and questions for data gathering. In order to assess the present system's compliance with the worldwide standard for information security, the survey questions were designed.

2.4. Data Collection and Analysis

Each journal and conference proceedings were reviewed and assessed by the first author, however, the papers that addressed literature of any type identified as included or excluded were discussed with the other researchers. The researcher responsible for searching the journal or conference applied the detailed inclusion and exclusion criteria to the relevant papers. The automated search strategy was followed in our research to identify the primary studies. The electronic libraries used were:

- Google Scholar
- IEEE Xplore
- Springer
- Science Direct
- Research Gate
- British Library EThOS
- ACM Digital Library
- Abstracts in New Technologies and Engineering
- Web of Science

As part of the literature studies, certain keywords and synonyms were established and included in the research. We worked on keywords and terms that these studies use to specify essential concepts of relevance to ISMS. For the retrieval in the digital libraries, a sophisticated search string was constructed using Boolean ANDs and ORs. The string given below was derived and taken as a basis to apply to the title, keywords, and abstracts of publications

Chapter 4: Results

1.0. Pros and Cons of NIST's CSF and ISO 27001

Since the framework is voluntary, it can be utilized by any company dealing with cyber threats and information breaches, especially in a technology-heavy setting, which makes it a good fit for NIST. Due to its emphasis on technological controls, the NIST CSF is better suited to technology-oriented enterprises.

For example, according to Kosutic, the CSF framework was originally created to meet the needs of the U.S. government's critical infrastructure because of the voluntary nature of the framework (Kosutic, D., 2021). The framework's voluntary nature has the same drawback as the previous one: it doesn't replace proper risk management. It should not be used as a long-term replacement for information security management frameworks, but rather as a guide to help firms build risk management frameworks. Organizations encounter a wide range of threats, vulnerabilities, and other security issues, so there isn't a one-size-fits-all approach to dealing with cyber-attacks and breaches. As a result, the translation and implementation of the technique will need to be tailored to the specific threat and security posture of the firm (Ivkic, I., et al., 2017).

Even if the NIST Cyber Security Framework is not foolproof, Guinn argues that those who choose to ignore or delay implementation of the voluntary guideline, in part or in whole, may miss out on its advantages and benefits. That's because the Framework includes leading practices from various standards bodies that have proven to be successful when implemented, and it may also deliver regulatory and legal advantages that extend well beyond improved cyber security and risk management for organizations that adopt it early (Waxler, J., 2018).

According to Kosutic, ISO/IEC 27001 is an information security standard that was first issued by the International Organization for Standardization in 2005 (Kosutic, D., 2021). Cyber security and risk management frameworks are widely utilized in most enterprises in practically every country, even though they are not mandatory to follow. Information security is discussed as part of a company's broader management and process framework, as outlined by Kosutic (Ivkic, I., et al., 2017).

With the help of ISO 27001, organizations can cut their costs and gain a competitive advantage in the market because of the reduction in expenditures, which is an additional benefit of this security framework. Typically, cyber security is viewed as a burden on the company's budget with no clear way to quantify its value. When it comes to saving money, ISO 27001 provides an outstanding return on investment because it provides an efficient process (Ivkic, I., et al., 2017).

2.0. Similarities between NIST's CSF and ISO 27001

Both the Cyber Security Framework and ISO 27001, according to Kosutic (2014), provide strong techniques for dealing with cyber/information security threats and breaches. In all likelihood, and in fact, it is possible to get outstanding outcomes in dealing with security by implementing either of these techniques. The three pillars of confidentiality, honesty, and availability are the same for both of them. In addition to ISO 270001 and NIST CSF, other standards such as CIS-20, SP 800-53 (security controls), SP 800-37 (risk management recommendations), and ISO 27002 (implementing controls), 27004 (metrics), and 27005 can be used to create an ISMS (risk management).

Despite the fact that CSF's security postures are better suited for tech-companies due to its emphasis on log analytics, incident analytics, and technical controls, the ISO 27001 is better suited for commercial companies due to its inclusion of rigorous documentation that is divided into mandatory documents (statement of applicability, risk assessment methodology guideline, scope of ISMS, risk treatment, access control policy, etc.), both frameworks can be implemented in organizations with varying degrees of technology (password policy document, BYOD policy, change management policy etc.) (Kosutic, D., 2021).

Both frameworks share similarities that can be mapped back to each other, despite their differing design. According to Kosutic, the "Framework Core is divided into Functions (Identify; Protect; Detect; Respond; and Recover), and then into 22 related Categories (e.g., Asset Management; Risk; Management; etc. – very similar to sections in ISO 27001 Annex A), 98 Subcategories (very similar to controls in ISO 27001 Annex A), and for each Subcategory several references are made to other frameworks like ISO 27001; COBIT; NIST SP 800-53; ISA 62443; and CCS." This

division into categories and subcategories allows for greater adaptability and flexibility, as well as bridging the gap between technical, administrative, and policy-related controls. It also makes it much easier to map various controls from various standards to the CSF categories (Kosutic, D., 2021).

3.0. Advantages of NIST's CSF over ISO 27001

With NISTS's Cyber Security Framework, firms can easily deploy it at the enterprise level because of its well-structured and planned format. In addition, the NIST CSF's organized approach can be deemed more user-friendly and simplified, particularly for top management. Cyber risk activities are broken down into five categories: identify, protect, detect and respond to and recover from cyber-attacks. Systematic categorization of security concerns is easier to achieve with these five functionalities. Using references to other frameworks like ISO 27001, COBIT, and others allows CSF combine multiple significant characteristics from various frameworks, which is one of the major advantages of CSF. (Kosutic, D., 2021)

"Detailed technical references that are aimed to provide organizations with a starting point for applying practices to accomplish the Framework's targeted results indicated in the related Subcategory," according to the National Institute of Standards and Technology (U.S.) (Cybersecurity, C.I., 2014). Control schemes like CIS-20, which emphasize the defense-in-depth approach to security, are best suited for CSF implementation.

For the evaluation of an organization's total security posture, CSF implements the notion of current and target profiles. "It is easy to see where the organization is currently in relation to the Framework Core categories and subcategories, and where it intends to be, with Framework Profile (e.g., Current Profile, Target Profile). Here, the holes can be easily identified, and action plans can be devised to close them "in Kosutic writes that is why the framework can be used by not only top management but also intermediate managers and engineers thanks to the concept of breaking it down into discrete functional blocks and profiles. (Kosutic, D., 2021)

4.0. Advantages of ISO 27001 over NIST's CSF

ISO 27001 is one of the most well-known and widely adopted approaches in the United States and around the world. Any firm seeking a foolproof structure for showcasing stakeholders will always turn to ISO 27001. Its reputation speaks for itself. "One of the main benefits of ISO 27001 is that firms can become certified against it," argues Kosutic (Kosutic, D., 2021). By following this guideline, any business may demonstrate to its stakeholders that it can provide a risk management framework that is both safe and effective to its clients, partners, and other interested parties. The PDCA (Plan-Do-Check-Act) Cycle is used as the framework for its operation.

According to Disterer (2016), ISO 27001 is built on a PDCA methodology, which requires planning, execution, and continual monitoring of the established ISMS as well as continuous improvement through corrective measures. However, despite the fact that the PDCA approach isn't explicitly stated in the latest iteration of the standard, it still must be followed. Because ISO 27001 is a certification, organizations can obtain a competitive advantage and customer confidence that can be used as leverage in commercial negotiations by becoming certified against it.

Another advantage of ISO 27001 is that it places a strong emphasis on both necessary and non-mandated documentation, making it easy for management to perform high-level analysis. Unlike Cyber Security Framework, ISO 27001 explicitly outlines which documents and records are needed, and what is the minimum that must be implemented. ISO 27001 also offers the benefit of forcing organizations to specify their duties and the assets and data they are accountable for, enhancing an organization's structure and ensuring the safety of its data and assets. Documentation for incident management and change management as well as BYOD and password policy and access control policy are all heavily emphasized in ISO 27001 certification. This makes it more appropriate for use as a framework for developing one's own ISMS (Information Security Management System). (Kosutic, D., 2021)

Chapter 5: Summary of Findings

Security framework selection is more about company strategy than it is about technology. The selection of a cybersecurity framework must be guided by the legal, regulatory, and contractual obligations of the company, as that knowledge provides the minimum set of needs needed to:

- Showing evidence of "reasonably-expected" security and privacy policies will help you avoid being labeled as careless.
- Make sure the systems, applications, and processes are protected from legitimate threats by implementing effective risk management procedures.

NIST 800-171 and CMMC requirements cannot be met by the NIST Cybersecurity Framework or ISO 27001/27002. According to NIST 800-171 (Appendix D), the security standards of NIST 800-171 for Controlled Unclassified Information (CUI) relate to those of NIST 800-53 and ISO 27001/27002. There are exceptions to this rule, such as when the ISO 27001/27002 framework fails to meet all of NIST 800-171's standards. It is critical to understand the level of content each framework provides since this directly effects the available security and privacy controls that exist "out of the box" without having to bolt-on content to meet specific demands.

From cybersecurity policies and standards paperwork to NIST 800-171 compliance checklists to program-level documentation like "near turnkey" incident response, risk management or vulnerability management program documents, there are a variety of low-cost solutions available.

ISO 27002 is essentially a subset of NIST 800-53 where the fourteen (14) sections of ISO 27002 security controls fit within the twenty (20) families of NIST 800-53 rev5 security controls. In addition to the controls described in ISO 27002, the NIST CSF is a subset of NIST 800-53. Parts of ISO 27002 and NIST 800-53 are incorporated into the NIST CSF; however, both are not exhaustive. Smaller businesses that need to adhere to a set of "best practices" can use the NIST CSF, whereas larger businesses or those with unique compliance requirements should use ISO 27002 and NIST 800-53. To fulfill PCI DSS, you would need to use ISO 27002 or NIST 800-53 as a framework, unless you wanted to add extra controls to the NIST CSF to make it work. Is that incorrect? No, but when you start bolting onto frameworks, things get a little more complicated.

When it comes to software development, the SCF can be described as a framework for all other frameworks. There are more than 100 policies and frameworks included in the SCF that span NIST CSF, ISO 27002, NIST 800-53, and more. Even while many of these popular cybersecurity frameworks focus on the same basic components, they differ in terms of both content and presentation. It's critical to realize that each framework has advantages and disadvantages before making a final decision.

Both the NIST CSF and the ISO 27001 frameworks for cybersecurity risk management are highly effective. The NIST CSF framework and ISO 27001 standards are both simple to apply for any firm. The definitions and codes used in these frameworks are fairly interchangeable. With the help of these frameworks, organizations may more easily share information regarding cybersecurity concerns across departments and with external parties. It's recommended to go with ISO 27001 if you're an operationally mature firm looking for certification, whereas NIST CSF may be better if you're just beginning to establish a cybersecurity risk management plan or are trying to recover from data breaches.

A third-party audit to obtain ISO 27001 certification can be expensive, but it can improve the company's reputation as a reliable corporation to stakeholders. The NIST CSF does not offer such certification. Unlike the ISO 27001, the NIST CSF is offered for free, which is another reason why an upstart could want to start their cybersecurity risk management program with NIST CSF before moving on to ISO 27001.

ISO 27001 is a good option for mature enterprises that are under pressure from the outside to be certified. It is possible, however, that enterprises are not yet ready to invest in an ISO 27001 certification or that the firm is at a point where it would benefit from the explicit evaluation methodology provided by the NIST Cybersecurity Frameworks. The results of a NIST audit can be used to gauge a company's current state before installing stricter cybersecurity controls and safeguards.

The NIST CSF framework can be used as a precursor to the ISO 27001 certification path, which can then be integrated as the firm grows. Growing firms can use NIST CSF to organize their initial assessments of IT security risks. Consider ISO security and compliance certifications if organization currently have the necessary infrastructure in place. For a proactive and efficient information security management system, it doesn't matter if a firm starts with NIST CSF or grows with ISO 27001 standards.

Chapter 6: Conclusion

The National Institute of Standards and Technology (NIST) is currently revising its Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations. It's important to note that NIST did not establish this framework to defend private industry. NIST 800-53 best practices have, however, become the de facto standard for private enterprises doing business with the United States federal government as a result of widespread outsourcing to private companies and substantial regulation of businesses. Keep in mind that NIST 800-53 is a superset of ISO 27002, which implies that you will find all of the ISO 27002's components covered by NIST

800-53. " There are some aspects of NIST 800-53 that ISO 27002 does not cover: The additional needs for compliance that NIST over ISO can cover are nicely depicted in the accompanying diagram.

When it comes to software development, the SCF can be described as a framework for all other frameworks. There are more than 100 policies and frameworks included in the SCF that span NIST CSF, ISO 27002, NIST 800-53, and more. Even while many of these popular cybersecurity frameworks focus on the same basic components, they differ in terms of both content and presentation. It's critical to realize that each framework has advantages and disadvantages before making a final decision.

Both the NIST CSF and the ISO 27001 frameworks for cybersecurity risk management are highly effective. The NIST CSF framework and ISO 27001 standards are both simple to apply for any firm. The definitions and codes used in these frameworks are fairly interchangeable. With the help of these frameworks, organizations may more easily share information regarding cybersecurity concerns across departments and with external parties.

References

- Al-Mayahi, I. and Sa'ad, P.M., (2012). Iso 27001 gap analysis-case study. In *Proceedings of the International Conference on Security and Management (SAM)* (p. 1). The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp).
- Andress, M. and Fonseca, B., (2000). Manage people to protect data. *InfoWorld*, *22*(46), p.48.
- Arnason, S.T. and Willett, K.D., 2007. *How to achieve 27001 certification: An example of applied compliance management*. Auerbach Publications.
- Candiwan, C., (2014). Analysis of ISO27001 implementation for enterprises and SMEs in indonesia. In *Proceedings of the International Conference on Cyber-Crime Investigation and Cyber Security (ICCICS2014), Kuala Lumpur, Malaysia* (Vol. 1719, p. 5058).
- Chang, S.E. and Lin, C.S., (2007). Exploring organizational culture for information security management. *Industrial management & data systems*.
- Cybersecurity, C.I., (2014). Framework for improving critical infrastructure cybersecurity. *Framework*, *1*(11).
- Dey, M., 2007. Information security management-a practical approach. In *AFRICON 2007* (pp. 1-6). IEEE.
- Dhillon, G., (2001). Violation of safeguards by trusted personnel and understanding related information security concerns. *Computers & security*, *20*(2), pp.165-172.
- Disterer, G., (2016). ISO/IEC 27000, 27001 and 27002 for information security management (2013). *Available: DOI*, *10*.
- Ermana, F.H. and Tanuwijaya Mastan, I., (2012). Security audit information system based on the ISO 27001 Standards on PT. *BPR Jatim, STIKOM. Surabaya*.
- Gaunt, N., (2000). Practical approaches to creating a security culture. *International journal of medical informatics*, *60*(2), pp.151-157.
- Ifinedo, P., (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. Computers & Security, 31(1), pp.83-95.
- Itradat, A., Sultan, S., Al-Junaidi, M., Qaffaf, R., Mashal, F. and Daas, F., (2014). Developing an ISO27001 Information Security Management System for an Educational Institute: Hashemite University as a Case Study. *Jordan Journal of Mechanical & Industrial Engineering*, *8*(2).
- Ivkic, I., Wolfauer, S., Oberhofer, T. and Tauber, M.G., (2017), December. On the cost of cyber security in smart business. In *2017 12th International Conference for Internet Technology and Secured Transactions (ICITST)* (pp. 255-260). IEEE.
- Karabacak, B. and Sogukpinar, I., (2006). A quantitative method for ISO 17799 gap analysis. *Computers & security*, *25*(6), pp.413-419.
- Knapp, K.J., Morris Jr, R.F., Marshall, T.E. and Byrd, T.A., (2009). Information security policy: An organizational-level process model. *Computers & security*, *28*(7), pp.493-508.
- Kosutic, D., (2021). *The Impact of Cybersecurity on Competitive Advantage* (Doctoral dissertation, GRENOBLE ECOLE DE MANAGEMENT).
- Krisanthi, G.A.T., Sukarsa, I.M. and Bayupati, I.P.A., (2014). Governance audit of application procurement using COBIT framework. *Journal of Theoretical and Applied Information Technology*, *59*(2), pp.342-351.
- Leem, C.S., Kim, S. and Lee, H.J., (2005). Assessment methodology on maturity level of ISMS. In *International Conference on Knowledge-Based and Intelligent Information and Engineering Systems* (pp. 609-615). Springer, Berlin, Heidelberg.
- Martins, A. and Elofe, J., (2002). Information security culture. In *Security in the information society* (pp. 203-214). Springer, Boston, MA.
- Mayer, N., (2010). A Cluster Approach to Security Im-provement according to ISO/IEC 27001.
- Solms, B.V., (2000). Information security-The third wave? *Computers & security*, *19*(7), pp.615-615.
- Susanto, A. and Shobariah, E., (2016). Assessment of ISMS based on standard ISO/IEC 27001: 2013 at DISKOMINFO Depok City. In *2016 4th International Conference on Cyber and IT Service Management* (pp. 1-6). IEEE.
- Tipton, H.F. and Krause, M., (2007). *Information security management handbook*. CRC press.
- Venter, H.S. and Eloff, J.H.P., (2000). Network security: Important issues. *Network Security*, *2000*(6), pp.12-16.

- Waxler, J., (2018). *Prioritizing Security Controls Using Multiple Criteria Decision Making for Home Users* (Doctoral dissertation, The George Washington University).

Appendices

Appendix 1

Table 1 provides a mapping from the security controls in NIST Special Publication 800-53 to the security controls in ISO/IEC 27001. Please review the introductory text above before employing the mappings in Table 1.

TABLE 1: MAPPING NIST SP 800-53 TO ISO/IEC 27001

NIST SP 800-53 CONTROLS		ISO/IEC 27001 CONTROLS *Note: An asterisk (*) indicates that the ISO/IEC control **does not fully satisfy** the intent of the NIST control.*
AC-1	Access Control Policy and Procedures	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.9.1.1, A.12.1.1, A.18.1.1, A.18.2.2
AC-2	Account Management	A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.5, A.9.2.6
AC-3	Access Enforcement	A.6.2.2, A.9.1.2, A.9.4.1, A.9.4.4, A.9.4.5, A.13.1.1, A.14.1.2, A.14.1.3, A.18.1.3
AC-4	Information Flow Enforcement	A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3
AC-5	Separation of Duties	A.6.1.2
AC-6	Least Privilege	A.9.1.2, A.9.2.3, A.9.4.4, A.9.4.5
AC-7	Unsuccessful Logon Attempts	A.9.4.2
AC-8	System Use Notification	A.9.4.2
AC-9	Previous Logon Notification	A.9.4.2
AC-10	Concurrent Session Control	None
AC-11	Device Lock	A.11.2.8, A.11.2.9
AC-12	Session Termination	None
AC-13	**Withdrawn**	---
AC-14	Permitted Actions without Identification or Authentication	None
AC-15	**Withdrawn**	---
AC-16	Security and Privacy Attributes	None
AC-17	Remote Access	A.6.2.1, A.6.2.2, A.13.1.1, A.13.2.1, A.14.1.2
AC-18	Wireless Access	A.6.2.1, A.13.1.1, A.13.2.1
AC-19	Access Control for Mobile Devices	A.6.2.1, A.11.1.5, A.11.2.6, A.13.2.1
AC-20	Use of External Systems	A.11.2.6, A.13.1.1, A.13.2.1
AC-21	Information Sharing	None
AC-22	Publicly Accessible Content	None
AC-23	Data Mining Protection	None
AC-24	Access Control Decisions	A.9.4.1*
AC-25	Reference Monitor	None
AT-1	Awareness and Training Policy and Procedures	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
AT-2	Literacy Training and Awareness	7.3, A.7.2.2, A.12.2.1
AT-3	Role-Based Training	A.7.2.2*
AT-4	Training Records	None

NIST SP 800-53 CONTROLS		ISO/IEC 27001 CONTROLS *Note: An asterisk (*) indicates that the ISO/IEC control **does not fully satisfy** the intent of the NIST control.*
AT-5	**Withdrawn**	---
AT-6	Training Feedback	None
AU-1	Audit and Accountability Policy and Procedures	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
AU-2	Event Logging	None
AU-3	Content of Audit Records	A.12.4.1*
AU-4	Audit Log Storage Capacity	A.12.1.3
AU-5	Response to Audit Logging Process Failures	None
AU-6	Audit Record Review, Analysis, and Reporting	A.12.4.1, A.16.1.2, A.16.1.4
AU-7	Audit Record Reduction and Report Generation	None
AU-8	Time Stamps	A.12.4.4
AU-9	Protection of Audit Information	A.12.4.2, A.12.4.3, A.18.1.3
AU-10	Non-repudiation	None
AU-11	Audit Record Retention	A.12.4.1, A.16.1.7
AU-12	Audit Record Generation	A.12.4.1, A.12.4.3
AU-13	Monitoring for Information Disclosure	None
AU-14	Session Audit	A.12.4.1*
AU-15	**Withdrawn**	---
AU-16	Cross-Organizational Audit Logging	None
CA-1	Assessment and Authorization Policies and Procedures	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
CA-2	Control Assessments	A.14.2.8, A.18.2.2, A.18.2.3
CA-3	Information Exchange	A.13.1.2, A.13.2.1, A.13.2.2
CA-4	**Withdrawn**	---
CA-5	Plan of Action and Milestones	8.3, 9.2, 10.1*
CA-6	Authorization	9.3*
CA-7	Continuous Monitoring	9.1, 9.2, A.18.2.2, A.18.2.3*
CA-8	Penetration Testing	None
CA-9	Internal System Connections	None
CM-1	Configuration Management Policy and Procedures	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
CM-2	Baseline Configuration	None
CM-3	Configuration Change Control	8.1, A.12.1.2, A.14.2.2, A.14.2.3, A.14.2.4
CM-4	Impact Analyses	A.14.2.3
CM-5	Access Restrictions for Change	A.9.2.3, A.9.4.5, A.12.1.2, A.12.1.4, A.12.5.1
CM-6	Configuration Settings	None
CM-7	Least Functionality	A.12.5.1*
CM-8	System Component Inventory	A.8.1.1, A.8.1.2
CM-9	Configuration Management Plan	A.6.1.1*

ISSN-P: 2807-5987

NIST SP 800-53 CONTROLS		ISO/IEC 27001 CONTROLS *Note: An asterisk (*) indicates that the ISO/IEC control **does not fully satisfy** the intent of the NIST control.*
CM-10	Software Usage Restrictions	A.18.1.2
CM-11	User-Installed Software	A.12.5.1, A.12.6.2
CM-12	Information Location	None
CM-13	Data Action Mapping	None
CM-14	Signed Components	None
CP-1	Contingency Planning Policy and Procedures	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
CP-2	Contingency Plan	7.5.1, 7.5.2, 7.5.3, A.6.1.1, A.17.1.1, A.17.2.1
CP-3	Contingency Training	A.7.2.2*
CP-4	Contingency Plan Testing	A.17.1.3
CP-5	**Withdrawn**	---
CP-6	Alternate Storage Site	A.11.1.4, A.17.1.2, A.17.2.1
CP-7	Alternate Processing Site	A.11.1.4, A.17.1.2, A.17.2.1
CP-8	Telecommunications Services	A.11.2.2, A.17.1.2
CP-9	System Backup	A.12.3.1, A.17.1.2, A.18.1.3
CP-10	System Recovery and Reconstitution	A.17.1.2
CP-11	Alternate Communications Protocols	A.17.1.2*
CP-12	Safe Mode	None
CP-13	Alternative Security Mechanisms	A.17.1.2*
IA-1	Identification and Authentication Policy and Procedures	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
IA-2	Identification and Authentication (Organizational Users)	A.9.2.1
IA-3	Device Identification and Authentication	None
IA-4	Identifier Management	A.9.2.1
IA-5	Authenticator Management	A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.3
IA-6	Authentication Feedback	A.9.4.2
IA-7	Cryptographic Module Authentication	A.18.1.5
IA-8	Identification and Authentication (Non-Organizational Users)	A.9.2.1
IA-9	Service Identification and Authentication	None
IA-10	Adaptive Identification and Authentication	None
IA-11	Re-authentication	None
IA-12	Identity Proofing	None
IR-1	Incident Response Policy and Procedures	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1 A.18.1.1, A.18.2.2
IR-2	Incident Response Training	A.7.2.2*
IR-3	Incident Response Testing	None
IR-4	Incident Handling	A.16.1.4, A.16.1.5, A.16.1.6
IR-5	Incident Monitoring	None

ISSN-E: 26632806

ISSN-P: 2807-5987

NIST SP 800-53 CONTROLS		ISO/IEC 27001 CONTROLS *Note: An asterisk (*) indicates that the ISO/IEC control **does not fully satisfy** the intent of the NIST control.*
IR-6	Incident Reporting	A.6.1.3, A.16.1.2
IR-7	Incident Response Assistance	None
IR-8	Incident Response Plan	7.5.1, 7.5.2, 7.5.3, A.16.1.1
IR-9	Information Spillage Response	None
IR-10	**Withdrawn**	---
MA-1	System Maintenance Policy and Procedures	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
MA-2	Controlled Maintenance	A.11.2.4*, A.11.2.5*
MA-3	Maintenance Tools	None
MA-4	Nonlocal Maintenance	None
MA-5	Maintenance Personnel	None
MA-6	Timely Maintenance	A.11.2.4
MA-7	Field Maintenance	None
MP-1	Media Protection Policy and Procedures	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
MP-2	Media Access	A.8.2.3, A.8.3.1, A.11.2.9
MP-3	Media Marking	A.8.2.2
MP-4	Media Storage	A.8.2.3, A.8.3.1, A.11.2.9
MP-5	Media Transport	A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.5, A.11.2.6
MP-6	Media Sanitization	A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7
MP-7	Media Use	A.8.2.3, A.8.3.1
MP-8	Media Downgrading	None
PE-1	Physical and Environmental Protection Policy and Procedures	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
PE-2	Physical Access Authorizations	A.11.1.2*
PE-3	Physical Access Control	A.11.1.1, A.11.1.2, A.11.1.3
PE-4	Access Control for Transmission Medium	A.11.1.2, A.11.2.3
PE-5	Access Control for Output Devices	A.11.1.2, A.11.1.3
PE-6	Monitoring Physical Access	None
PE-7	**Withdrawn**	---
PE-8	Visitor Access Records	None
PE-9	Power Equipment and Cabling	A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3
PE-10	Emergency Shutoff	A.11.2.2*
PE-11	Emergency Power	A.11.2.2
PE-12	Emergency Lighting	A.11.2.2*
PE-13	Fire Protection	A.11.1.4, A.11.2.1
PE-14	Environmental Controls	A.11.1.4, A.11.2.1, A.11.2.2
PE-15	Water Damage Protection	A.11.1.4, A.11.2.1, A.11.2.2
PE-16	Delivery and Removal	A.8.2.3, A.11.1.6, A.11.2.5
PE-17	Alternate Work Site	A.6.2.2, A.11.2.6, A.13.2.1
PE-18	Location of System Components	A.8.2.3, A.11.1.4, A.11.2.1

ISSN-E: 26632806

NIST SP 800-53 CONTROLS		ISO/IEC 27001 CONTROLS *Note: An asterisk (*) indicates that the ISO/IEC control **does not fully satisfy** the intent of the NIST control.*
PE-19	Information Leakage	A.11.1.4, A.11.2.1
PE-20	Asset Monitoring and Tracking	A.8.2.3*
PE-21	Electromagnetic Pulse Protection	None
PE-22	Component Marking	A.8.2.2
PE-23	Facility Location	A.11.1.4, A.11.2.1
PL-1	Planning Policy and Procedures	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
PL-2	System Security and Privacy Plans	7.5.1, 7.5.2, 7.5.3, 10.1, A.14.1.1
PL-3	**Withdrawn**	---
PL-4	Rules of Behavior	A.7.1.2, A.7.2.1, A.8.1.3
PL-5	**Withdrawn**	---
PL-6	**Withdrawn**	---
PL-7	Concept of Operations	8.1, A.14.1.1
PL-8	Security and Privacy Architectures	A.14.1.1*
PL-9	Central Management	None
PL-10	Baseline Selection	None
PL-11	Baseline Tailoring	None
PM-1	Information Security Program Plan	4.1, 4.2, 4.3, 4.4, 5.2, 5.3, 6.1.1, 6.2, 7.4, 7.5.1, 7.5.2, 7.5.3, 8.1, 9.3, 10.2, A.5.1.1, A.5.1.2, A.6.1.1, A.18.1.1, A.18.2.2
PM-2	Information Security Program Leadership Role	5.1, 5.3, A.6.1.1
PM-3	Information Security and Privacy Resources	5.1, 6.2, 7.1
PM-4	Plan of Action and Milestones Process	6.1.1, 6.2, 7.5.1, 7.5.2, 7.5.3, 8.3, 9.2, 9.3, 10.1
PM-5	System Inventory	None
PM-6	Measures of Performance	5.3, 6.1.1, 6.2, 9.1,
PM-7	Enterprise Architecture	None
PM-8	Critical Infrastructure Plan	None
PM-9	Risk Management Strategy	4.3, 4.4, 6.1.1, 6.1.2, 6.2, 7.5.1, 7.5.2, 7.5.3, 9.3, 10.2
PM-10	Authorization Process	9.3, A.6.1.1*
PM-11	Mission and Business Process Definition	4.1
PM-12	Insider Threat Program	None
PM-13	Security and Privacy Workforce	7.2, A.7.2.2*
PM-14	Testing, Training, and Monitoring	6.2*
PM-15	Security and Privacy Groups and Associations	7.4, A.6.1.4
PM-16	Threat Awareness Program	None
PM-17	Protecting Controlled Unclassified Information on External Systems	None
PM-18	Privacy Program Plan	None
PM-19	Privacy Program Leadership Role	None

NIST SP 800-53 CONTROLS		ISO/IEC 27001 CONTROLS *Note: An asterisk (*) indicates that the ISO/IEC control **does not fully satisfy** the intent of the NIST control.*
PM-20	Dissemination of Privacy Program Information	None
PM-21	Accounting of Disclosures	None
PM-22	Personally Identifiable Information Quality Management	None
PM-23	Data Governance Body	None
PM-24	Data Integrity Board	None
PM-25	Minimization of Personally Identifiable Information Used in Testing, Training, and Research	None
PM-26	Complaint Management	None
PM-27	Privacy Reporting	None
PM-28	Risk Framing	4.3, 6.1.2, 6.2, 7.4, 7.5.1, 7.5.2, 7.5.3
PM-29	Risk Management Program Leadership Roles	5.1, 5.3, 9.2, A.6.1.1
PM-30	Supply Chain Risk Management Strategy	4.4, 6.2, 7.5.1, 7.5.2, 7.5.3, 10.2*
PM-31	Continuous Monitoring Strategy	4.4, 6.2, 7.4, 7.5.1, 7.5.2, 7.5.3, 9.1, 10.1, 10.2
PM-32	Purposing	None
PS-1	Personnel Security Policy and Procedures	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
PS-2	Position Risk Designation	None
PS-3	Personnel Screening	A.7.1.1
PS-4	Personnel Termination	A.7.3.1, A.8.1.4
PS-5	Personnel Transfer	A.7.3.1, A.8.1.4
PS-6	Access Agreements	A.7.1.2, A.7.2.1, A.13.2.4
PS-7	External Personnel Security	A.6.1.1, A.7.2.1*
PS-8	Personnel Sanctions	7.3, A.7.2.3
PS-9	Position Descriptions	A.6.1.1
PT-1	Personally Identifiable Information Processing and Transparency Policy and Procedures	None
PT-2	Authority to Process Personally Identifiable Information	None
PT-3	Personally Identifiable Information Processing Purposes	None
PT-4	Consent	None
PT-5	Privacy Notice	None
PT-6	System of Records Notice	None
PT-7	Specific Categories of Personally Identifiable Information	None
PT-8	Computer Matching Requirements	None
RA-1	Risk Assessment Policy and Procedures	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2

NIST SP 800-53 CONTROLS		ISO/IEC 27001 CONTROLS *Note: An asterisk (*) indicates that the ISO/IEC control **does not fully satisfy** the intent of the NIST control.*
RA-2	Security Categorization	A.8.2.1
RA-3	Risk Assessment	6.1.2, 8.2, A.12.6.1*
RA-4	**Withdrawn**	---
RA-5	Vulnerability Monitoring and Scanning	A.12.6.1*
RA-6	Technical Surveillance Countermeasures Survey	None
RA-7	Risk Response	6.1.3, 8.3, 10.1
RA-8	Privacy Impact Assessments	None
RA-9	Criticality Analysis	A.15.2.2*
RA-10	Threat Hunting	None
SA-1	System and Services Acquisition Policy and Procedures	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, 8.1, A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
SA-2	Allocation of Resources	None
SA-3	System Development Life Cycle	A.6.1.1, A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.6
SA-4	Acquisition Process	8.1, A.14.1.1, A.14.2.7, A.14.2.9, A.15.1.2
SA-5	System Documentation	7.5.1, 7.5.2, 7.5.3, A.12.1.1*
SA-6	**Withdrawn**	---
SA-7	**Withdrawn**	---
SA-8	Security Engineering Principles	A.14.2.5
SA-9	External System Services	A.6.1.1, A.6.1.5, A.7.2.1, A.13.1.2, A.13.2.2, A.15.2.1, A.15.2.2
SA-10	Developer Configuration Management	A.12.1.2, A.14.2.2, A.14.2.4, A.14.2.7
SA-11	Developer Testing and Evaluation	A.14.2.7, A.14.2.8
SA-12	**Withdrawn**	---
SA-13	**Withdrawn**	---
SA-14	**Withdrawn**	---
SA-15	Development Process, Standards, and Tools	A.6.1.5, A.14.2.1
SA-16	Developer-Provided Training	None
SA-17	Developer Security and Privacy Architecture and Design	A.14.2.1, A.14.2.5
SA-18	**Withdrawn**	---
SA-19	**Withdrawn**	---
SA-20	Customized Development of Critical Components	None
SA-21	Developer Screening	A.7.1.1
SA-22	Unsupported System Components	None
SA-23	Specialization	None
SC-1	System and Communications Protection Policy and Procedures	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2

NIST SP 800-53 CONTROLS		ISO/IEC 27001 CONTROLS *Note: An asterisk (*) indicates that the ISO/IEC control **does not fully satisfy** the intent of the NIST control.*
SC-2	Separation of System and User Functionality	None
SC-3	Security Function Isolation	None
SC-4	Information In Shared System Resources	None
SC-5	Denial-of Service-Protection	None
SC-6	Resource Availability	None
SC-7	Boundary Protection	A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.3
SC-8	Transmission Confidentiality and Integrity	A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3
SC-9	**Withdrawn**	---
SC-10	Network Disconnect	A.13.1.1
SC-11	Trusted Path	None
SC-12	Cryptographic Key Establishment and Management	A.10.1.2
SC-13	Cryptographic Protection	A.10.1.1, A.14.1.2, A.14.1.3, A.18.1.5
SC-14	**Withdrawn**	---
SC-15	Collaborative Computing Devices and Applications	A.13.2.1*
SC-16	Transmission of Security and Privacy Attributes	None
SC-17	Public Key Infrastructure Certificates	A.10.1.2
SC-18	Mobile Code	None
SC-19	**Withdrawn**	None
SC-20	Secure Name/Address Resolution Service (Authoritative Source)	None
SC-21	Secure Name/Address Resolution Service (Recursive or Caching Resolver)	None
SC-22	Architecture and Provisioning for Name/Address Resolution Service	None
SC-23	Session Authenticity	None
SC-24	Fail in Known State	None
SC-25	Thin Nodes	None
SC-26	Decoys	None
SC-27	Platform-Independent Applications	None
SC-28	Protection of Information at Rest	A.8.2.3*
SC-29	Heterogeneity	None
SC-30	Concealment and Misdirection	None
SC-31	Covert Channel Analysis	None
SC-32	System Partitioning	None
SC-33	**Withdrawn**	---
SC-34	Non-Modifiable Executable Programs	None

ISSN-P: 2807-5987

NIST SP 800-53 CONTROLS		ISO/IEC 27001 CONTROLS *Note: An asterisk (*) indicates that the ISO/IEC control **does not fully satisfy** the intent of the NIST control.*
SC-35	External Malicious Code Identification	None
SC-36	Distributed Processing and Storage	None
SC-37	Out-of-Band Channels	None
SC-38	Operations Security	A.12.x
SC-39	Process Isolation	None
SC-40	Wireless Link Protection	None
SC-41	Port and I/O Device Access	None
SC-42	Sensor Capability and Data	A.11.1.5*
SC-43	Usage Restrictions	None
SC-44	Detonation Chambers	None
SC-45	System Time Synchronization	None
SC-46	Cross Domain Policy Enforcement	None
SC-47	Alternate Communications Paths	None
SC-48	Sensor Relocation	None
SC-49	Hardware-Enforced Separation and Policy Enforcement	None
SC-50	Software-Enforced Separation and Policy Enforcement	None
SC-51	Hardware-Based Protection	None
SI-1	System and Information Integrity Policy and Procedures	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
SI-2	Flaw Remediation	A.12.6.1, A.14.2.2, A.14.2.3, A.16.1.3
SI-3	Malicious Code Protection	A.12.2.1
SI-4	System Monitoring	None
SI-5	Security Alerts, Advisories, and Directives	A.6.1.4*
SI-6	Security and Privacy Function Verification	None
SI-7	Software, Firmware, and Information Integrity	None
SI-8	Spam Protection	None
SI-9	**Withdrawn**	---
SI-10	Information Input Validation	None
SI-11	Error Handling	None
SI-12	Information Management and Retention	None
SI-13	Predictable Failure Prevention	None
SI-14	Non-Persistence	None
SI-15	Information Output Filtering	None
SI-16	Memory Protection	None
SI-17	Fail-Safe Procedures	None

ISSN-E: 26632806

NIST SP 800-53 CONTROLS		ISO/IEC 27001 CONTROLS *Note: An asterisk (*) indicates that the ISO/IEC control **does not fully satisfy** the intent of the NIST control.*
SI-18	Personally Identifiable Information Quality Operations	None
SI-19	De-identification	None
SI-20	Tainting	None
SI-21	Information Refresh	None
SI-22	Information Diversity	None
SI-23	Information Fragmentation	None
SR-1	Supply Chain Risk Management Policy and Procedures	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.15.1.1, A.18.1.1, A.18.2.2
SR-2	Supply Chain Risk Management Plan	A.14.2.7*
SR-3	Supply Chain Controls and Processes	A.15.1.2, A.15.1.3*
SR-4	Provenance	A.14.2.7*
SR-5	Acquisition Strategies, Tools, and Methods	A.15.1.3
SR-6	Supplier Assessments and Reviews	A.15.2.1
SR-7	Supply Chain Operations Security	A.15.2.2*
SR-8	Notification Agreements	None
SR-9	Tamper Resistance and Detection	None
SR-10	Inspection of Systems or Components	None
SR-11	Component Authenticity	None
SR-12	Component Disposal	None

ISSN-P: 2807-5987

Appendix 2

Table 2 provides a mapping from the security requirements and controls in ISO/IEC 27001 to the security controls in Special Publication 800-53.[1] Please review the introductory text provided above before employing the mappings in Table 2.

TABLE 2: MAPPING ISO/IEC 27001 TO NIST SP 800-53

ISO/IEC 27001 REQUIREMENTS AND CONTROLS	NIST SP 800-53 CONTROLS *Note: An asterisk (*) indicates that the ISO/IEC control does not fully satisfy the intent of the NIST control.*
ISO/IEC 27001 Requirements	
4. Context of the Organization	
4.1 Understanding the organization and its context	PM-1, PM-11
4.2 Understanding the needs and expectations of interested parties	PM-1
4.3 Determining the scope of the information security management system	PM-1, PM-9, PM-28
4.4 Information security management system	PM-1, PM-9, PM-30, PM-31
5. Leadership	
5.1 Leadership and commitment	PM-2, PM-3, PM-29
5.2 Policy	All XX-1 controls
5.3 Organizational roles, responsibilities, and authorities	All XX-1 controls, PM-2, PM-6, PM-29
6. Planning	
6.1 Actions to address risks and opportunities	
6.1.1 General	PM-1, PM-4, PM-6, PM-9
6.1.2 Information security risk assessment	PM-9, PM-28, RA-3
6.1.3 Information security risk treatment	RA-7
6.2 Information security objectives and planning	PM-1, PM-3, PM-4, PM-6, PM-9, PM-14, PM-28, PM-30, PM-31
7. Support	
7.1 Resources	PM-3
7.2 Competence	PM-13
7.3 Awareness	AT-2, PS-8
7.4 Communication	PM-1, PM-15, PM-28, PM-31
7.5 Documented information	
7.5.1 General	All XX-1 controls, CP-2, IR-8, PL-2, PM-4, PM-9, PM-28, PM-30, PM-31, SA-5
7.5.2 Creating and updating	All XX-1 controls, CP-2, IR-8, PL-2, PM-4, PM-9, PM-28, PM-30, PM-31, SA-5
7.5.3 Control of documented information	All XX-1 controls, CP-2, IR-8, PL-2, PM-4, PM-9, PM-28, PM-30, PM-31, SA-5
8. Operation	

[1] The use of the term *XX-1 controls* in mapping Table 2 refers to the set of security controls represented by the first control in each 800-53 control family, where *XX* is a placeholder for the two-letter family identifier.

ISSN-E: 26632806

ISSN-P: 2807-5987

ISO/IEC 27001 REQUIREMENTS AND CONTROLS	NIST SP 800-53 CONTROLS *Note: An asterisk (*) indicates that the ISO/IEC control does not fully satisfy the intent of the NIST control.*
8.1 Operation planning and control	CM-3, PL-7, PM-1, SA-1, SA-4
8.2 Information security risk assessment	RA-3
8.3 Information security risk treatment	CA-5, PM-4, RA-7
9. Performance evaluation	
9.1 Monitoring, measurement, analysis, and evaluation	CA-1, CA-7, PM-6, PM-31
9.2 Internal audit	CA-1, CA-2, CA-5, CA-7, PM-4
9.3 Management review	CA-6, PM-1, PM-4, PM-9, PM-10, PM-29
10. Improvement	
10.1 Nonconformity and corrective action	CA-5, PL-2, PM-4, PM-31, RA-7
10.2 Continual improvement	PM-1, PM-9, PM-30, PM-31
ISO/IEC 27001 Controls	
A.5 Information Security Policies	
A.5.1 Management direction for information security	
A.5.1.1 Policies for information security	All XX-1 controls
A.5.1.2 Review of the policies for information security	All XX-1 controls
A.6 Organization of information security	
A.6.1 Internal organization	
A.6.1.1 Information security roles and responsibilities	All XX-1 controls, CM-9, CP-2, PS-7, PS-9, SA-3, SA-9, PM-2, PM-10
A.6.1.2 Segregation of duties	AC-5
A.6.1.3 Contact with authorities	IR-6
A.6.1.4 Contact with special interest groups	SI-5, PM-15
A.6.1.5 Information security in project management	SA-3, SA-9, SA-15
A.6.2 Mobile devices and teleworking	
A.6.2.1 Mobile device policy	AC-17, AC-18, AC-19
A.6.2.2 Teleworking	AC-3, AC-17, PE-17
A.7 Human Resources Security	
A.7.1 Prior to Employment	
A.7.1.1 Screening	PS-3, SA-21
A.7.1.2 Terms and conditions of employment	PL-4, PS-6
A.7.2 During employment	
A.7.2.1 Management responsibilities	PL-4, PS-6, PS-7, SA-9
A.7.2.2 Information security awareness, education, and training	AT-2, AT-3, CP-3, IR-2, PM-13
A.7.2.3 Disciplinary process	PS-8
A.7.3 Termination and change of employment	
A.7.3.1 Termination or change of employment responsibilities	PS-4, PS-5

ISSN-E: 26632806

ISSN-P: 2807-5987

ISO/IEC 27001 REQUIREMENTS AND CONTROLS	NIST SP 800-53 CONTROLS *Note: An asterisk (*) indicates that the ISO/IEC control does not fully satisfy the intent of the NIST control.*
A.8 Asset Management	
A.8.1 Responsibility for assets	
A.8.1.1 Inventory of assets	CM-8
A.8.1.2 Ownership of assets	CM-8
A.8.1.3 Acceptable use of assets	PL-4
A.8.1.4 Return of assets	PS-4, PS-5
A.8.2 Information Classification	
A.8.2.1 Classification of information	RA-2
A.8.2.2 Labelling of Information	MP-3, PE-22
A.8.2.3 Handling of Assets	MP-2, MP-4, MP-5, MP-6, MP-7, PE-16, PE-18, PE- 20, SC-8, SC-28
A.8.3 Media Handling	
A.8.3.1 Management of removable media	MP-2, MP-4, MP-5, MP-6, MP-7
A.8.3.2 Disposal of media	MP-6
A.8.3.3 Physical media transfer	MP-5
A.9 Access Control	
A.9.1 Business requirement of access control	
A.9.1.1 Access control policy	AC-1
A.9.1.2 Access to networks and network services	AC-3, AC-6
A.9.2 User access management	
A.9.2.1 User registration and de-registration	AC-2, IA-2, IA-4, IA-5, IA-8
A.9.2.2 User access provisioning	AC-2
A.9.2.3 Management of privileged access rights	AC-2, AC-3, AC-6, CM-5
A.9.2.4 Management of secret authentication information of users	IA-5
A.9.2.5 Review of user access rights	AC-2
A.9.2.6 Removal or adjustment of access rights	AC-2
A.9.3 User responsibilities	
A.9.3.1 Use of secret authentication information	IA-5
A.9.4 System and application access control	
A.9.4.1 Information access restriction	AC-3, AC-24
A.9.4.2 Secure logon procedures	AC-7, AC-8, AC-9, IA-6
A.9.4.3 Password management system	IA-5
A.9.4.4 Use of privileged utility programs	AC-3, AC-6
A.9.4.5 Access control to program source code	AC-3, AC-6, CM-5
A.10 Cryptography	
A.10.1 Cryptographic controls	
A.10.1.1 Policy on the use of cryptographic controls	SC-13
A.10.1.2 Key Management	SC-12, SC-17
A.11 Physical and environmental security	
A.11.1 Secure areas	

ISSN-E: 26632806

ISSN-P: 2807-5987

ISO/IEC 27001 REQUIREMENTS AND CONTROLS	NIST SP 800-53 CONTROLS *Note: An asterisk (*) indicates that the ISO/IEC control does not fully satisfy the intent of the NIST control.*
A.11.1.1 Physical security perimeter	PE-3*
A.11.1.2 Physical entry controls	PE-2, PE-3, PE-4, PE-5
A.11.1.3 Securing offices, rooms and facilities	PE-3, PE-5
A.11.1.4 Protecting against external and environmental threats	CP-6, CP-7, PE-9, PE-13, PE-14, PE-15, PE-18, PE-19, PE-23
A.11.1.5 Working in secure areas	AC-19(4), SC-42*
A.11.1.6 Delivery and loading areas	PE-16
A.11.2 Equipment	
A.11.2.1 Equipment siting and protection	PE-9, PE-13, PE-14, PE-15, PE-18, PE-19, PE-23
A.11.2.2 Supporting utilities	CP-8, PE-9, PE-10, PE-11, PE-12, PE-14, PE-15
A.11.2.3 Cabling security	PE-4, PE-9
A.11.2.4 Equipment maintenance	MA-2, MA-6
A.11.2.5 Removal of assets	MA-2, MP-5, PE-16
A.11.2.6 Security of equipment and assets off-premises	AC-19, AC-20, MP-5, PE-17
A.11.2.7 Secure disposal or reuse of equipment	MP-6
A.11.2.8 Unattended user equipment	AC-11
A.11.2.9 Clear desk and clear screen policy	AC-11, MP-2, MP-4
A.12 Operations security	
A.12.1 Operational procedures and responsibilities	
A.12.1.1 Documented operating procedures	All XX-1 controls, SA-5
A.12.1.2 Change management	CM-3, CM-5, SA-10
A.12.1.3 Capacity management	AU-4, CP-2(2), SC-5(2)
A.12.1.4 Separation of development, testing, and operational environments	CM-4(1), CM-5*
A.12.2 Protection from malware	
A.12.2.1 Controls against malware	AT-2, SI-3
A.12.3 Backup	
A.12.3.1 Information backup	CP-9
A.12.4 Logging and monitoring	
A.12.4.1 Event logging	AU-3, AU-6, AU-11, AU-12, AU-14
A.12.4.2 Protection of log information	AU-9
A.12.4.3 Administrator and operator logs	AU-9, AU-12
A.12.4.4 Clock synchronization	AU-8
A.12.5 Control of operational software	
A.12.5.1 Installation of software on operational systems	CM-5, CM-7(4), CM-7(5), CM-11
A.12.6 Technical vulnerability management	
A.12.6.1 Management of technical vulnerabilities	RA-3, RA-5, SI-2, SI-5
A.12.6.2 Restrictions on software installation	CM-11

ISSN-E: 26632806

ISO/IEC 27001 REQUIREMENTS AND CONTROLS	NIST SP 800-53 CONTROLS *Note: An asterisk (*) indicates that the ISO/IEC control does not fully satisfy the intent of the NIST control.*
A.12.7 Information systems audit considerations	
A.12.7.1 Information systems audit controls	AU-5*
A.13 Communications security	
A.13.1 Network security management	
A.13.1.1 Network controls	AC-3, AC-17, AC-18, AC-20, SC-7, SC-8, SC-10
A.13.1.2 Security of network services	CA-3, SA-9
A.13.1.3 Segregation in networks	AC-4, SC-7
A.13.2 Information transfer	
A.13.2.1 Information transfer policies and procedures	AC-4, AC-17, AC-18, AC-19, AC-20, CA-3, PE-17, SC-7, SC-8, SC-15
A.13.2.2 Agreements on information transfer	CA-3, PS-6, SA-9
A.13.2.3 Electronic messaging	SC-8
A.13.2.4 Confidentiality or nondisclosure agreements	PS-6
A.14 System acquisition, development and maintenance	
A.14.1 Security requirements of information systems	
A.14.1.1 Information security requirements analysis and specification	PL-2, PL-7, PL-8, SA-3, SA-4
A.14.1.2 Securing application services on public networks	AC-3, AC-4, AC-17, SC-8, SC-13
A.14.1.3 Protecting application services transactions	AC-3, AC-4, SC-7, SC-8, SC-13
A.14.2 Security in development and support processes	
A.14.2.1 Secure development policy	SA-3, SA-15, SA-17
A.14.2.2 System change control procedures	CM-3, SA-10, SI-2
A.14.2.3 Technical review of applications after operating platform changes	CM-3, CM-4, SI-2
A.14.2.4 Restrictions on changes to software packages	CM-3, SA-10
A.14.2.5 Secure system engineering principles	SA-8
A.14.2.6 Secure development environment	SA-3*
A.14.2.7 Outsourced development	SA-4, SA-10, SA-11, SA-15, SR-2, SR-4
A.14.2.8 System security testing	CA-2, SA-11
A.14.2.9 System acceptance testing	SA-4, SR-5(2)
A.14.3 Test data	
A.14.3.1 Protection of test data	SA-15(9)*
A.15 Supplier Relationships	
A.15.1 Information security in supplier relationships	

ISO/IEC 27001 REQUIREMENTS AND CONTROLS	NIST SP 800-53 CONTROLS *Note: An asterisk (*) indicates that the ISO/IEC control does not fully satisfy the intent of the NIST control.*
A.15.1.1 Information security policy for supplier relationships	SR-1
A.15.1.2 Address security within supplier agreements	SA-4, SR-3
A.15.1.3 Information and communication technology supply chain	SR-3, SR-5
A.15.2 Supplier service delivery management	
A.15.2.1 Monitoring and review of supplier services	SA-9, SR-6
A.15.2.2 Managing changes to supplier services	RA-9, SA-9, SR-7
A.16 Information security incident management	
A.16.1 Managing of information security incidents and improvements	
A.16.1.1 Responsibilities and procedures	IR-8
A.16.1.2 Reporting information security events	AU-6, IR-6
A.16.1.3 Reporting information security weaknesses	SI-2
A.16.1.4 Assessment of and decision on information security events	AU-6, IR-4
A.16.1.5 Response to information security incidents	IR-4
A.16.1.6 Learning from information security incidents	IR-4
A.16.1.7 Collection of evidence	AU-4, AU-9, AU-10(3), AU-11*
A.17 Information security aspects of business continuity management	
A.17.1 Information security continuity	
A.17.1.1 Planning information security continuity	CP-2
A.17.1.2 Implementing information security continuity	CP-6, CP-7, CP-8, CP-9, CP-10, CP-11, CP-13
A.17.1.3 Verify, review, and evaluate information security continuity	CP-4
A.17.2 Redundancies	
A.17.2.1 Availability of information processing facilities	CP-2,CP-6, CP-7
A.18 Compliance	
A.18.1 Compliance with legal and contractual requirements	
A.18.1.1 Identification of applicable legislation and contractual requirements	All XX-1 controls
A.18.1.2 Intellectual property rights	CM-10
A.18.1.3 Protection of records	AC-3, AC-23, AU-9, AU-10, CP-9, SC-8, SC-8(1), SC-13, SC-28, SC-28(1)

ISSN-P: 2807-5987

ISO/IEC 27001 REQUIREMENTS AND CONTROLS	NIST SP 800-53 CONTROLS *Note: An asterisk (*) indicates that the ISO/IEC control does not fully satisfy the intent of the NIST control.*
A.18.1.4 Privacy and protection of personal information	Appendix J Privacy controls
A.18.1.5 Regulation of cryptographic controls	IA-7, SC-12, SC-13, SC-17
A.18.2 **Information security reviews**	
A.18.2.1 Independent review of information security	CA-2(1), SA-11(3)
A.18.2.2 Compliance with security policies and standards	All XX-1 controls, CA-2
A.18.2.3 Technical compliance review	CA-2

ISSN-E: 26632806