Analysis and Comparison of the NIST SP 800-53 and ISO/IEC 27001:2013

Yevhenii Kurii[1] and Ivan Opirskyy[1]

[1] *Lviv Polytechnic National University, 12 Stepan Bandera str., Lviv, 79000, Ukraine*

Abstract

Managing information security in the organization may be a daunting task, especially considering that it may encompass many areas from physical and network security to human resources security and management of suppliers. This may be especially hard for young specialists or not experienced enough specialists, who may miss some important areas due to lack of practical experience. This is where security frameworks come in handy and put formality into the process of the design and implementation of the security strategy. With a framework in place, it becomes much easier to define the processes and procedures that your organization must take to assess, monitor, and mitigate cybersecurity risk and apply proper controls to protect valuable information. But another problem came up when you are to choose the "just right" framework for your organization taking into account more business-specific characteristics like the context of the organization, area of operation, applicable laws, regulations and contractual obligations, as well as more general ones like framework's maturity, comprehensiveness or popularity. While there are a bunch of different information security frameworks out in the wild, the most commonly-found and preferred by security professionals worldwide are NIST SP 800-53 and ISO/IEC 27001:2013. They combine both the quite comprehensive set of security controls to cover the most important security areas and wide applicability which allows applying these frameworks to all kinds of organizations. But they also have a set of distinct features, that define their relevance to the particular organization. The article is aimed at giving a brief overview of these two most popular security frameworks as well as describing their key characteristics and providing a comparison of their controls.

Keywords

Information security, cybersecurity framework, security controls, information security management system, ISMS, ISO 27001, NIST 800-53, controls mapping.

1. Introduction

To successfully achieve the objectives of implementing cybersecurity at different levels, a range of procedures and standards should be followed. Cybersecurity standards determine the requirements that an organization should follow to achieve cybersecurity objectives and facilitate against cybercrimes [1] and ensure the ongoing management of information security controls.

Additionally, the framework establishes a common language for defining a cybersecurity program, enabling organizations to set risk-based cybersecurity goals at the executive level that can be translated to the operations team [2].

These frameworks are a blueprint for managing and reducing organizational risk. Information security professionals use frameworks to define and prioritize the tasks required to manage the organization's security program. Frameworks are also used to help prepare for compliance and other IT and security audits. When you are choosing from the number of leading information security frameworks, you would primarily assess the number of unique information security controls (requirements) in each of them [3–5].

CPITS-2022: Cybersecurity Providing in Information and Telecommunication Systems, October 13, 2022, Kyiv, Ukraine
EMAIL: yevhenii.o.kurii@lpnu.ua (Y. Kurii); ivan.r.opirskyi@lpnu.ua (I. Opirskyy)
ORCID: 0000-0002-3423-5655 (Y. Kurii); 0000-0002-8461-8996 (I. Opirskyy)

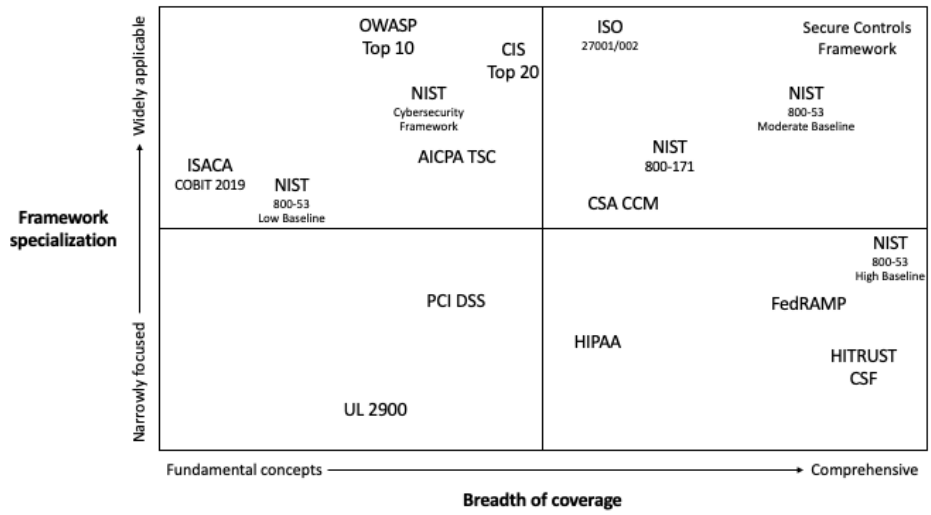

Figure 1: Information security frameworks based on their specialization and coverage

The volume of these controls directly impacts the number of domains covered by that framework. The lesser number of controls in a framework might make it easier to implement, but it also might not provide the necessary coverage that your organization needs from the perspective of administrative, technical, and physical information security practices [6].

This is where defining the applicable and relevant framework is primarily a business decision [7], based on your organization's context and risk profile, which needs to consider applicable laws and regulations, that are required to support existing or planned business processes.

Commonly, this selection process generally leads to adopting one of the following frameworks:

- ISO 27001/002 [8, 9]
- NIST Special Publication 800-53 [10]
- NIST Cybersecurity Framework [11]
- PCI DSS [12]
- CIS Controls [13, 14]
- HITRUST Common Security Framework [15]
- HIPAA [16]
- CSA CCM [17]
- GDPR [18]
- ISO 27701 [19]
- AICPA Trust Services Criteria (SOC 2) [20]
- COBIT [21]

Each information security framework has its own unique specialization and depth of coverage. However, understanding this can help you make an informed decision on the most appropriate framework for your needs. [22, 23] You may even find you need to leverage a metaframework (e.g., the framework of frameworks) to address more complex compliance requirements (e.g., when the organization is holding the personal data of EU citizens and process cardholder data, it should comply with both GDPR and PCI DSS requirements).

A key consideration for choosing an information security framework would be understanding the level of content and robustness each framework offers. This will directly impact the available information security controls within each framework [24].

2. Overview and Comparison between NIST SP 800-53 and ISO/IEC 27001:2013

The Special Publication (SP) 800-53 Security and Privacy Controls for Information Systems and Organizations from the National Institute of Standards and Technology (NIST) is currently in its 5th revision (rev5) dated September 2020. It was initially designed to protect the US federal government, but quickly gained popularity among private industry and now is considered as one of the most popular and respectable information security frameworks in the world. It was partially caused due to the significant outsourcing to private companies that do business with the US federal government.

According to the official web page of the standard “This publication [Special Publication (SP) 800-53] provides a catalog of security and privacy controls for information systems and

Table 1
Key differences between NIST SP 800-53 to ISO 27001

	NIST	ISO
Description	A recognized framework that contains security and privacy controls for information systems and organizations to protect organizational operations and assets with aim to effectively manage risk	An internationally recognized standard that describes how to manage information security in an organization
Target organizations	Was primarily created to help US federal agencies	Can be implemented in any kind of organization, profit or non-profit, private or state-owned, small or large
Structure	Contains 1007 controls broken down into 20 control families	Annex A provides 14 control categories with 114 controls
Complexity	Is very detailed and technical in its nature	Is less technical, with more emphasis on risk-based approach to managing security
Certification	Is voluntary and relies on self-assessment and self-compliance	Enables companies to become certified, relies on independent audit and certification bodies
Availability	Can be freely downloaded from official source	Distributed on the commercial basis through the official website

organizations to protect organizational operations and assets, individuals, other organizations, and the Nation from a diverse set of threats and risks, including hostile attacks, human errors, natural disasters, structural failures, foreign intelligence entities, and privacy risks" [25].

SO 27001 is a well-respected international information security standard that outlines the key processes and approaches a business needs to manage information security risk in a practical way [26]. ISO 27001 consists of the main part and Annex A, that contains the basic overview of the security controls needed to build an Information Security Management System (ISMS). Additionally, there is a separate standard ISO 27002 that provides a detailed description of the specific controls that are necessary to actually implement ISO 27001 (essentially, you can't meet ISO 27001 without implementing ISO 27002). [27, 28]. The important thing about ISO is that it provides the companies with the possibility to undergo an external audit and get certified against ISO 27001.

2.1. Detailed Mapping of Controls

Table 2 provides a mapping from the security controls in NIST Special Publication 800-53 to the security controls in ISO/IEC 27001:2013 [29].

Table 2
Mapping NIST SP 800-53 to ISO 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.*	Effected CIA triad element
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	Confidentiality, Integrity
AC-11	Device Lock	A.11.2.8, A.11.2.9	
AC-12	Session Termination	None	Confidentiality, Integrity
AC-13	**Withdrawn**	---	
AC-14	Permitted Actions without Identification or Authentication	None	Confidentiality, Integrity
AC-15	**Withdrawn**	---	
AC-16	Security and Privacy Attributes	None	Confidentiality, Integrity
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	Confidentiality
AC-22	Publicly Accessible Content	None	Confidentiality
AC-23	Data Mining Protection	None	Confidentiality, Integrity, Availability
AC-24	Access Control Decisions	A.9.4.1*	
AC-25	Reference Monitor	None	Confidentiality
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	Integrity
AT-5	**Withdrawn**	---	
AT-6	Training Feedback	None	Integrity

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	Confidentiality, Integrity, Availability
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	Integrity, Availability
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	Integrity, Availability
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	Integrity
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	Confidentiality
AU-14	Session Audit	A.12.4.1*	
AU-15	**Withdrawn**	---	
AU-16	Cross-Organizational Audit Logging	None	Confidentiality, Integrity
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	Confidentiality, Integrity, Availability
CA-9	Internal System Connections	None	Confidentiality, Integrity, Availability

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	Integrity
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	Integrity
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*	
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	Confidentiality, Integrity, Availability
CM-13	Data Action Mapping	None	Confidentiality, Integrity, Availability
CM-14	Signed Components	None	Integrity
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	Integrity, Availability
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	Confidentiality, Integrity
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	Confidentiality, Integrity
IA-10	Adaptive Identification and Authentication	None	Confidentiality, Integrity
IA-11	Re-authentication	None	Confidentiality, Integrity
IA-12	Identity Proofing	None	Confidentiality, Integrity
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	Availability
IR-4	Incident Handling	A.16.1.4, A.16.1.5, A.16.1.6	
IR-5	Incident Monitoring	None	Confidentiality, Integrity, Availability
IR-6	Incident Reporting	A.6.1.3, A.16.1.2	
IR-7	Incident Response Assistance	None	Confidentiality, Integrity, Availability
IR-8	Incident Response Plan	7.5.1, 7.5.2, 7.5.3, A.16.1.1	
IR-9	Information Spillage Response	None	Confidentiality, Integrity, Availability
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	Integrity, Availability
MA-4	Nonlocal Maintenance	None	Integrity, Availability
MA-5	Maintenance Personnel	None	Integrity, Availability
MA-6	Timely Maintenance	A.11.2.4	
MA-7	Field Maintenance	None	Integrity, Availability
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	Confidentiality
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	Confidentiality
PE-7	**Withdrawn**	---	
PE-8	Visitor Access Records	None	Confidentiality
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	
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	Availability
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	Confidentiality, Integrity, Availability
PL-10	Baseline Selection	None	Confidentiality, Integrity, Availability
PL-11	Baseline Tailoring	None	Confidentiality, Integrity, Availability
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	Integrity, Availability
PM-6	Measures of Performance	5.3, 6.1.1, 6.2, 9.1,	
PM-7	Enterprise Architecture	None	Confidentiality, Integrity, Availability
PM-8	Critical Infrastructure Plan	None	Availability
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	Confidentiality, Integrity
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	Confidentiality, Integrity
PM-17	Protecting Controlled Unclassified Information on External Systems	None	Confidentiality
PM-18	Privacy Program Plan	None	Confidentiality, Integrity
PM-19	Privacy Program Leadership Role	None	Confidentiality, Integrity
PM-20	Dissemination of Privacy Program Information	None	Confidentiality, Integrity
PM-21	Accounting of Disclosures	None	Confidentiality, Integrity
PM-22	Personally Identifiable Information Quality Management	None	Confidentiality, Integrity, Availability
PM-23	Data Governance Body	None	Confidentiality, Integrity, Availability
PM-24	Data Integrity Board	None	Confidentiality, Integrity
PM-25	Minimization of Personally Identifiable Information Used in Testing, Training, and Research	None	Confidentiality, Integrity
PM-26	Complaint Management	None	Confidentiality, Integrity, Availability
PM-27	Privacy Reporting	None	Confidentiality, Integrity, Availability
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	Confidentiality, Integrity, Availability
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	Confidentiality, Integrity
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	Confidentiality, Integrity, Availability
PT-2	Authority to Process Personally Identifiable Information	None	Confidentiality, Integrity, Availability
PT-3	Personally Identifiable Information Processing Purposes	None	Confidentiality, Integrity
PT-4	Consent	None	Integrity
PT-5	Privacy Notice	None	Integrity
PT-6	System of Records Notice	None	Integrity
PT-7	Specific Categories of Personally Identifiable Information	None	Integrity
PT-8	Computer Matching Requirements	None	Integrity

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	
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	Confidentiality, Integrity, Availability
RA-7	Risk Response	6.1.3, 8.3, 10.1	
RA-8	Privacy Impact Assessments	None	Confidentiality, Integrity
RA-9	Criticality Analysis	A.15.2.2*	
RA-10	Threat Hunting	None	Confidentiality, Integrity, Availability
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	Availability
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	Confidentiality, Integrity, Availability
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	Confidentiality, Integrity, Availability
SA-21	Developer Screening	A.7.1.1	
SA-22	Unsupported System Components	None	Integrity, Availability
SA-23	Specialization	None	Availability
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	
SC-2	Separation of System and User Functionality	None	Confidentiality, Integrity
SC-3	Security Function Isolation	None	Confidentiality, Integrity
SC-4	Information In Shared System Resources	None	Confidentiality, Integrity
SC-5	Denial-of Service-Protection	None	Availability
SC-6	Resource Availability	None	Availability
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	Confidentiality, Integrity
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	Confidentiality, Integrity
SC-17	Public Key Infrastructure Certificates	A.10.1.2	
SC-18	Mobile Code	None	Confidentiality, Integrity
SC-19	**Withdrawn**		
SC-20	Secure Name/Address Resolution Service (Authoritative Source)	None	Integrity
SC-21	Secure Name/Address Resolution Service (Recursive or Caching Resolver)	None	Integrity
SC-22	Architecture and Provisioning for Name/Address Resolution Service	None	Integrity
SC-23	Session Authenticity	None	Confidentiality, Integrity
SC-24	Fail in Known State	None	Confidentiality, Integrity
SC-25	Thin Nodes	None	Confidentiality, Integrity, Availability
SC-26	Decoys	None	Confidentiality, Integrity, Availability
SC-27	Platform-Independent Applications	None	Availability
SC-28	Protection of Information at Rest	A.8.2.3*	
SC-29	Heterogeneity	None	Availability
SC-30	Concealment and Misdirection	None	Confidentiality, Integrity, Availability
SC-31	Covert Channel Analysis	None	Confidentiality
SC-32	System Partitioning	None	Confidentiality, Availability
SC-33	**Withdrawn**	---	
SC-34	Non-Modifiable Executable Programs	None	Integrity,
SC-35	External Malicious Code Identification	None	Confidentiality, Integrity, Availability
SC-36	Distributed Processing and Storage	None	Availability
SC-37	Out-of-Band Channels	None	Confidentiality, Integrity, Availability
SC-38	Operations Security	A.12.x	
SC-39	Process Isolation	None	Confidentiality, Integrity, Availability
SC-40	Wireless Link Protection	None	Confidentiality, Integrity
SC-41	Port and I/O Device Access	None	Confidentiality, Integrity
SC-42	Sensor Capability and Data	A.11.1.5*	
SC-43	Usage Restrictions	None	Confidentiality, Integrity
SC-44	Detonation Chambers	None	Confidentiality, Integrity, Availability
SC-45	System Time Synchronization	None	Integrity
SC-46	Cross Domain Policy Enforcement	None	Confidentiality, Integrity, Availability
SC-47	Alternate Communications Paths	None	Availability
SC-48	Sensor Relocation	None	Confidentiality, Integrity
SC-49	Hardware-Enforced Separation and Policy Enforcement	None	Confidentiality, Integrity, Availability
SC-50	Software-Enforced Separation and Policy Enforcement	None	Confidentiality, Integrity, Availability
SC-51	Hardware-Based Protection	None	Confidentiality, Integrity, Availability
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	Confidentiality, Integrity, Availability
SI-5	Security Alerts, Advisories, and Directives	A.6.1.4*	
SI-6	Security and Privacy Function Verification	None	Confidentiality, Integrity
SI-7	Software, Firmware, and Information Integrity	None	Integrity
SI-8	Spam Protection	None	Integrity, Availability
SI-9	**Withdrawn**	---	
SI-10	Information Input Validation	None	Integrity
SI-11	Error Handling	None	Confidentiality, Integrity, Availability
SI-12	Information Management and Retention	None	Confidentiality, Integrity, Availability
SI-13	Predictable Failure Prevention	None	Integrity, Availability
SI-14	Non-Persistence	None	Confidentiality, Integrity, Availability
SI-15	Information Output Filtering	None	Confidentiality, Integrity, Availability
SI-16	Memory Protection	None	Confidentiality, Integrity, Availability
SI-17	Fail-Safe Procedures	None	Confidentiality, Integrity, Availability

SI-18	Personally Identifiable Information Quality Operations	None	Confidentiality, Integrity, Availability
SI-19	De-identification	None	Confidentiality, Integrity
SI-20	Tainting	None	Confidentiality, Integrity
SI-21	Information Refresh	None	Confidentiality
SI-22	Information Diversity	None	Integrity
SI-23	Information Fragmentation	None	Confidentiality, Integrity
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	Confidentiality, Integrity
SR-9	Tamper Resistance and Detection	None	Integrity
SR-10	Inspection of Systems or Components	None	Integrity
SR-11	Component Authenticity	None	Integrity
SR-12	Component Disposal	None	Confidentiality

As may be seen from the table there is an overlapping between the controls from ISO and NIST frameworks. But the most important specifics of these frameworks is that NIST 800-53 can be considered a super-set of ISO 27001. In particular, all the controls from ISO 27001 can be covered by NIST 800-53. However, ISO 27001 does not cover all of the areas of NIST 800-53. From the coverage perspective, NIST 800-53 is more comprehensive and contains much more areas and controls than ISO 27001. While the detailed analysis of the missing controls is out of the scope of this investigation let's take a look at a few examples which would show in which areas NIST, in contrast to ISO, provide more comprehensive coverage of the security-related areas.

[AT-4 Training Records], [AT-6 Training Feedback]. These two controls require the organization to document and monitor information security and privacy training activities, including security and privacy awareness training and specific role-based security and privacy training, retain individual training records, and gather feedback on organizational training results [10]. These could be important indicators of the awareness process effectiveness in the organization. These controls very often are audited by auditors during the ISO 27001 certification process; however, they are not explicitly mentioned in ISO 27001.

[CM-2 Baseline Configuration], [CM-6 Configuration Settings]. These controls force organizations to develop, document, and maintain under configuration control, a current baseline configuration of the system, and configuration settings for components. Baseline configurations for systems and system components include connectivity, operational, and communications aspects of systems. Baseline configurations are documented, formally reviewed, and agreed-upon specifications for systems or configuration items within those systems. Baseline configurations serve as a basis for future builds, releases, or changes to systems and include security and privacy control implementations, operational procedures, information about system components, network topology, and logical placement of components in the system architecture [10]. These controls are important for maintaining the integrity of the security configurations for the systems and components and ensuring the standard configuration for the infrastructure systems and components. Again, these aspects are not explicitly highlighted in the ISO 27001 but commonly are checked during the ISO certification process.

[PE-6 Monitoring Physical Access], [PE-8 Visitor Access Records]. NIST 800-53 requires from organizations to monitor physical access to the facility where the system resides to detect and respond to physical security incidents and to maintain and periodically review visitor access records to the facility where the system resides [10]. These are other examples of controls that are extremely relevant for the protection of the organization's assets. They are especially important for small representative offices that often are lacking baseline security controls established within headquarters and are also quite often emphasized during the ISO certification audits. Nevertheless, they have been overlooked

for a quite long time until the issue of the revised version of the ISO 27002 earlier this year (so they should appear in the new version of the ISO 27001 as well).

[RA-10 Threat Hunting]. Threat hunting is an active means of cyber defense in contrast to traditional protection measures, such as firewalls, intrusion detection and prevention systems, quarantining malicious code in sandboxes, and Security Information and Event Management technologies and systems. Cyber threat hunting involves proactively searching organizational systems, networks, and infrastructure for advanced threats. The objective is to track and disrupt cyber adversaries as early as possible in the attack sequence and to measurably improve the speed and accuracy of organizational responses. [10]. Likewise the previous controls, this one has been also overlooked by the ISO 27001 publications, despite its extreme importance and relevance for the organizations. This inconsistency should be partially eliminated with the new version of the ISO 27001 standard - this year's revised version of ISO 27002 already contains a new control defining requirements for threat intelligence which is an integral part of the threat hunting process.

[PM-18 Privacy Program Plan], [PT-1 Personally Identifiable Information Processing and Transparency Policy and Procedures], [PT-2 Authority to Process Personally Identifiable Information], [PT-4 Consent], [PT-5 Privacy Notice] and other controls related to the protection of personally identifiable information (PII) processing. The defining characteristic of the NIST 800-53 is that it contains a set of controls to address privacy requirements for the processing of PII while ISO 27001 does not specifically address privacy beyond the inherent benefits provided by maintaining the security of PII, therefore we can assume that the ISO 27001 controls do not satisfy privacy requirements with respect to PII processing [29]. From this perspective, NIST has an advantage over ISO 27001 in regard to the protection of the PII processing and may be considered a good basis for GDPR compliance.

3. Conclusion

Understanding both the differences and similarities between these two the most known and adopted security frameworks—ISO 27001 and NIST 800-53 is crucial for implementing an effective information security program that would be tightened to the organization's context and needs and expectations of interested parties.

A common misunderstanding is that companies have to pick one or the other framework and stick with it, or that one is better than the other. In fact, both frameworks can be applied to a single organization due to their synergy and can greatly increase its information security, risk management, and security program.

It is not always necessary to choose between NIST 800-53 and ISO 27001. In fact, the two are complementary and can be used in the same organization. However, if certification is your goal, you should definitely look closer at ISO 27001. Being externally audited and achieving accredited certification against ISO 27001's requirements would likely provide a higher level of confidence among clients and stakeholders and would be a prerequisite for securing certain contracts. Accredited certification to ISO 27001 demonstrates that your organization follows information security best practices, and delivers an independent, expert assessment of whether your valuable information and information assets are adequately protected. At the same time, while implementing the ISO 27001 requirements you still can leverage NIST 800-53 to strengthen the areas that are missing or not sufficiently covered in the ISO.

4. References

[1] H. Taherdoost, Understanding Cybersecurity Frameworks and Information Security Standards—A Review and Comprehensive Overview, 2022. doi: 10.3390/ electronics11142181.

[2] T. Conkle, G. Witte, Improving Cybersecurity through the Use of the Cybersecurity Framework, in 9th International Topical Meeting on Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies, NPIC and HMIT, vol. 3, 2015, pp. 2479–2486.

[3] V. Buriachok, V. Sokolov, P. Skladannyi, Security Rating Metrics for Distributed Wireless Systems, in 8th International Conference on "Mathematics. Information Technologies. Education:" Modern Machine Learning Technologies and Data Science (MoMLeT and DS), vol. 2386, 2019, pp. 222–233.

[4] F. Kipchuk, et al., Assessing Approaches of IT Infrastructure Audit, in IEEE 8th

International Conference on Problems of Infocommunications, Science and Technology, PICST, 2021. doi: 10.1109/picst54195.2021.9772181.
[5] I. Kuzminykh, et al., Investigation of the IoT Device Lifetime with Secure Data Transmission, Internet of Things, Smart Spaces, and Next Generation Networks and Systems, 2019, pp. 16–27. doi: 10.1007/978-3-030-30859-9_2.
[6] NIST Cybersecurity Framework vs ISO 27001/27002 vs NIST 800-53 vs Secure Controls Framework. URL: https://www.complianceforge.com/faq/nist-800-53-vs-iso-27002-vs-nist-csf-vs-scf
[7] A. Zahoor, et al., Information Security Management Needs More Holistic Approach: A Literature Review, 2016. doi: 10.1016/j.ijinfomgt.2015.11.009
[8] ISO/IEC 27001: Information Technology—Security Techniques—Information Security Management Systems—Requirements, 2013, https://www.iso.org/standard/54534.html.
[9] ISO/IEC 27002: Information Technology—Security Techniques—Code of Practice for Information Security Controls, 2013, https://www.iso.org/standard/54533.html.
[10] (2020) Security and Privacy Controls for Information Systems and Organizations Special Publication (SP) 800-53 Rev 5, U.S. Department of Commerce, 2020, https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final.
[11] Overview of the NIST Cybersecurity Framework, 2018, https://1path2020b.websitetotalcare.com/blog/overviewof-thenist-cybersecurity-framework.
[12] PCI DSS Quick Reference Guide, Understanding the Payment Card Industry Data Security Standard, ver. 3.2.1, 2018, https://www.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf
[13] CIS Controls v8, Center for Internet Security, 2021, https://www.cisecurity.org/controls/v8/.
[14] CIS Controls v8 Mapping to NIST SP 800-53 Rev 5, Center for Internet Security, 2021.
[15] HITRUST CSF Framework, HITRUST Alliance, 2021, https://hitrustalliance.net/product-tool/hitrust-csf/
[16] HIPAA; Pub. L. 104-191, 110 Stat. 1936, enacted August 21, 1996
[17] Cloud Controls Matrix, Cloud Security Alliance, 2021, https://cloudsecurityalliance.org/artifacts/cloud-controls-matrix-v4/
[18] Regulation (EU) 2016/679 of the European Parliament and of the Council on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 2018, pp. 1–88.
[19] ISO/IEC 27701:2019, Security Techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for Privacy Information Management — Requirements and Guidelines, 2019, https://www.iso.org/standard/71670.html
[20] Trust Services Criteria Issued by the AICPA Assurance Services Executive Committee, 2017, https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/trust-services-criteria.pdf
[21] COBIT 5, A Framework for the Governance and Management of Enterprise IT, 2012.
[22] D. Sulistyowati, F. Handayani, Y. Suryanto, Comparative Analysis and Design of Cybersecurity Maturity Assessment Methodology Using NIST CSF COBIT ISO/IEC 27002 and PCI DSS, International Journal on Informatics Visualization, vol. 4, no. 4, 2020, pp. 225–230.
[23] M. Siponen, R. Willison, Information Security Management Standards: Problems and Solutions, J. Information & Management, vol. 46, 2009, pp. 267–270.
[24] S. Yevseiev, et al. Synergy of Building Cybersecurity Systems: Monograph, PC Technology Center, 2021.
[25] Computer Security Resource Center - SP 800-53 Rev. 5. https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final
[26] V. Susukailo, I. Opirsky, O. Yaremko, Methodology of ISMS Establishment Against Modern Cybersecurity Threats, in Future Intent-Based Networking. Lecture Notes in Electrical Engineering, vol. 831, 2022. doi: 10.1007/978-3-030-92435-5_15.
[27] ISO Official website—ISO/IEC 27001 Information security management, https://www.iso.org/isoiec-27001-information-security.html
[28] Best Practice ISO 27001 Required Documentation. https://www.riskmanagementstudio.com/best-practice-iso-27001-required-documentation/
[29] NIST SP 800-53, Revision 5 Control Mappings to ISO/IEC 27001 URL: https://csrc.nist.gov/CSRC/media/Publications/sp/800-53/rev-5/final/documents/sp800-53r5-to-iso-27001-mapping.docx