

## NIST SP 800-53, Revision 5 Control Mappings to ISO/IEC 27001

July 2023

The mapping tables in this appendix provide organizations with a *general* indication of security control coverage with respect to ISO/IEC 27001, *Information security, cybersecurity and privacy protection—Information security management systems—Requirements*.<sup>1</sup> ISO/IEC 27001 may be applied to all types of organizations and specifies requirements for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving a documented information security management system (ISMS) within the context of business risks. [NIST Special Publication 800-39](#) includes guidance on managing risk at the organizational level, mission/business process level, and system level, is consistent with ISO/IEC 27001, and provides additional implementation detail for the federal government and its contractors.

The mapping of SP 800-53 Revision 5 controls to ISO/IEC 27001:2022 requirements and controls reflects whether the implementation of a security control from Special Publication 800-53 satisfies the intent of the mapped security requirement or control from ISO/IEC 27001 and conversely, whether the implementation of a security requirement or security control from ISO/IEC 27001 satisfies the intent of the mapped control from Special Publication 800-53. To successfully meet the mapping criteria, the implementation of the mapped controls should result in an equivalent information security posture. However, organizations should not assume security requirement and control equivalency based solely on the mapping tables herein since there is always some degree of subjectivity in the mapping analysis because the mappings are not always one-to-one and may not be completely equivalent. Organization-specific implementations may also play a role in control equivalency. The following examples illustrate some of the mapping issues:

- **Example 1:** Special Publication 800-53 contingency planning and ISO/IEC 27001 ICT<sup>2</sup> readiness for business continuity were deemed to have similar, but not the same, functionality.
- **Example 2:** Similar topics addressed in the two security control sets may have a different context, perspective, or scope. Special Publication 800-53 addresses information flow control broadly in terms of approved authorizations for controlling access between source and destination objects, whereas ISO/IEC 27001 addresses information flow more narrowly as it applies to interconnected network domains.
- **Example 3:** Security control 5.2, Information security roles and responsibilities, in ISO/IEC 27001 Annex A states that “Information security roles and responsibilities shall be defined and allocated according to the organization needs” while security control PM-10, Authorization Process, in Special Publication 800-53 that is mapped to 5.2, has three distinct parts. Part b. of PM-10 requires designation of “individuals to fulfill specific roles and responsibilities...” If 5.2 is mapped to PM-10 without any additional information, organizations might assume that if 5.2 is implemented (i.e., all responsibilities are defined and allocated), then the intent of PM-10 is also fully satisfied. However, this may not be the case since the parts a. and c. of PM-10 may not have been addressed. To resolve and clarify the security control mappings, when a security requirement or control in the right column of Tables 1 and 2 does not fully satisfy the intent of the security requirement or control in

---

1 The third edition of ISO/IEC 27001 was published in October 2022 by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

2 Information and Communication Technology (ICT).

the left column of the tables, the control or controls (i.e., the entire set of controls listed) in the right column is designated with an asterisk (\*).

- **Example 4:** Privacy controls were integrated into the SP 800-53, Revision 5, control set to address privacy requirements for the processing of personally identifiable information (PII) and thus are included in the mapping table; however, ISO/IEC 27001 does not specifically address privacy beyond the inherent benefits provided by maintaining the security of PII. Users of this mapping table may assume that the ISO/IEC 27001 controls do not satisfy privacy requirements with respect to PII processing.

In a few cases, an ISO/IEC 27001 security requirement or control could only be directly mapped to a Special Publication 800-53 control *enhancement*. In such cases, the relevant enhancement is specified in Table 2 indicating that the corresponding ISO/IEC 27001 requirement or control satisfies only the intent of the specified enhancement and does not address the associated base control from Special Publication 800-53 or any other enhancements under that base control. Where no enhancement is specified, the ISO/IEC 27001 requirement or control is relevant only to the Special Publication 800-53 base control.

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. Note: although the prefix “A.” was removed from Annex A in 27001:2022, the prefix was maintained in Tables 1 and 2 below to distinguish between requirements and controls (controls from Annex A).

TABLE 1: MAPPING NIST SP 800-53, REVISION 5 TO ISO/IEC 27001:2022

NIST SP 800-53, REVISION 5 CONTROLS		ISO/IEC 27001:2022 REQUIREMENTS AND CONTROLS <i>Note: An asterisk (*) indicates that the ISO/IEC control <b>does not fully satisfy</b> the intent of the NIST control.</i>
AC-1	Access Control Policy and Procedures	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1, A.5.2, A.5.4, A.5.15, A.5.31, A.5.36, A.5.37
AC-2	Account Management	A.5.16, A.5.18, A.8.2
AC-3	Access Enforcement	A.5.15, A.5.33*, A.8.3, A.8.4*, A.8.18, A.8.20, A.8.26
AC-4	Information Flow Enforcement	A.5.14, A.8.22, A.8.23
AC-5	Separation of Duties	A.5.3
AC-6	Least Privilege	A.5.15*, A.8.2, A.8.18
AC-7	Unsuccessful Logon Attempts	A.8.5*
AC-8	System Use Notification	A.8.5*
AC-9	Previous Logon Notification	A.8.5*
AC-10	Concurrent Session Control	None
AC-11	Device Lock	A.7.7, A.8.1
AC-12	Session Termination	None
AC-13	<b>Withdrawn</b>	---
AC-14	Permitted Actions without Identification or Authentication	None
AC-15	<b>Withdrawn</b>	---
AC-16	Security and Privacy Attributes	None
AC-17	Remote Access	A.5.14, A.6.7, A.8.1,
AC-18	Wireless Access	A.5.14, A.8.1, A.8.20
AC-19	Access Control for Mobile Devices	A.5.14, A.7.9, A.8.1
AC-20	Use of External Systems	A.5.14, A.7.9, A.8.20
AC-21	Information Sharing	None
AC-22	Publicly Accessible Content	None
AC-23	Data Mining Protection	None
AC-24	Access Control Decisions	A.8.3*
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, A.5.2, A.5.4, A.5.31, A.5.36, A.5.37
AT-2	Literacy Training and Awareness	7.3, A.6.3, A.8.7*
AT-3	Role-Based Training	A.6.3*
AT-4	Training Records	None
AT-5	<b>Withdrawn</b>	---
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, A.5.2, A.5.4, A.5.31, A.5.36, A.5.37
AU-2	Event Logging	A.8.15
AU-3	Content of Audit Records	A.8.15*
AU-4	Audit Log Storage Capacity	A.8.6
AU-5	Response to Audit Logging Process Failures	None
AU-6	Audit Record Review, Analysis, and Reporting	A.5.25, A.6.8, A.8.15

NIST SP 800-53, REVISION 5 CONTROLS		ISO/IEC 27001:2022 REQUIREMENTS AND CONTROLS <i>Note: An asterisk (*) indicates that the ISO/IEC control <b>does not fully satisfy</b> the intent of the NIST control.</i>
AU-7	Audit Record Reduction and Report Generation	None
AU-8	Time Stamps	A.8.17
AU-9	Protection of Audit Information	A.5.33, A.8.15
AU-10	Non-repudiation	None
AU-11	Audit Record Retention	A.5.28, A.8.15
AU-12	Audit Record Generation	A.8.15
AU-13	Monitoring for Information Disclosure	A.8.12, A.8.16*
AU-14	Session Audit	A.8.15*
AU-15	<b>Withdrawn</b>	---
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, 9.2.2*, 9.3.1*, A.5.1, A.5.2, A.5.4, A.5.31, A.5.36, A.5.37
CA-2	Control Assessments	9.2.1*, 9.2.2*, A.5.30*, A.5.36, A.8.29
CA-3	Information Exchange	A.5.14, A.8.21
CA-4	<b>Withdrawn</b>	---
CA-5	Plan of Action and Milestones	8.3, 9.3.3*, 10.2*
CA-6	Authorization	9.3.1*, 9.3.3*
CA-7	Continuous Monitoring	9.1, 9.3.2*, 9.3.3*, A.5.36*
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, A.5.2, A.5.4, A.5.31, A.5.36, A.5.37, A.8.9
CM-2	Baseline Configuration	A.8.9
CM-3	Configuration Change Control	8.1, 9.3.3*, A.8.9, A.8.32
CM-4	Impact Analyses	A.8.9
CM-5	Access Restrictions for Change	A.8.2, A.8.4, A.8.9, A.8.19, A.8.31, A.8.32
CM-6	Configuration Settings	A.8.9
CM-7	Least Functionality	A.8.19*
CM-8	System Component Inventory	A.5.9, A.8.9
CM-9	Configuration Management Plan	A.5.2*, A.8.9
CM-10	Software Usage Restrictions	A.5.32*
CM-11	User-Installed Software	A.8.19*
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, A.5.2, A.5.4, A.5.31, A.5.36, A.5.37
CP-2	Contingency Plan	7.5.1, 7.5.2, 7.5.3, A.5.2, A.5.29, A.8.14
CP-3	Contingency Training	A.6.3*
CP-4	Contingency Plan Testing	A.5.29, A.5.30*
CP-5	<b>Withdrawn</b>	---
CP-6	Alternate Storage Site	A.5.29*, A.7.5*, A.8.14*
CP-7	Alternate Processing Site	A.5.29*, A.7.5*, A.8.14*
CP-8	Telecommunications Services	A.5.29*, A.7.11
CP-9	System Backup	A.5.29*, A.5.33*, A.8.13
CP-10	System Recovery and Reconstitution	A.5.29*
CP-11	Alternate Communications Protocols	A.5.29*
CP-12	Safe Mode	None
CP-13	Alternative Security Mechanisms	A.5.29*

NIST SP 800-53, REVISION 5 CONTROLS		ISO/IEC 27001:2022 REQUIREMENTS AND CONTROLS <i>Note: An asterisk (*) indicates that the ISO/IEC control <b>does not fully satisfy</b> the intent of the NIST control.</i>
IA-1	Identification and Authentication Policy and Procedures	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1, A.5.2, A.5.4, A.5.31, A.5.36, A.5.37
IA-2	Identification and Authentication (Organizational Users)	A.5.16
IA-3	Device Identification and Authentication	None
IA-4	Identifier Management	A.5.16
IA-5	Authenticator Management	A.5.16, A.5.17
IA-6	Authentication Feedback	A.8.5*
IA-7	Cryptographic Module Authentication	None
IA-8	Identification and Authentication (Non-Organizational Users)	A.5.16
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, A.5.2, A.5.4, A.5.31, A.5.36, A.5.37
IR-2	Incident Response Training	A.6.3*
IR-3	Incident Response Testing	None
IR-4	Incident Handling	A.5.25, A.5.26, A.5.27
IR-5	Incident Monitoring	None
IR-6	Incident Reporting	A.5.5*, A.6.8
IR-7	Incident Response Assistance	None
IR-8	Incident Response Plan	7.5.1, 7.5.2, 7.5.3, A.5.24
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, A.5.2, A.5.4, A.5.37, A.18.1.1, A.18.2.2
MA-2	Controlled Maintenance	A.7.10*, A.7.13*, A.8.10*
MA-3	Maintenance Tools	None
MA-4	Nonlocal Maintenance	None
MA-5	Maintenance Personnel	None
MA-6	Timely Maintenance	A.7.13
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, A.5.2, A.5.4, A.5.31, A.5.36, A.5.37
MP-2	Media Access	A.5.10*, A.7.7*, A.7.10*
MP-3	Media Marking	A.5.13
MP-4	Media Storage	A.5.10*, A.7.7*, A.7.10, A.8.10*
MP-5	Media Transport	A.5.10*, A.7.9, A.7.10
MP-6	Media Sanitization	A.5.10, A.7.10*, A.7.14, A.8.10
MP-7	Media Use	A.5.10, A.7.10
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, A.5.2, A.5.4, A.5.31, A.5.36, A.5.37
PE-2	Physical Access Authorizations	A.7.2*
PE-3	Physical Access Control	A.7.1, A.7.2, A.7.3, A.7.4
PE-4	Access Control for Transmission Medium	A.7.2, A.7.12
PE-5	Access Control for Output Devices	A.7.2, A.7.3, A.7.7
PE-6	Monitoring Physical Access	A.7.4, A.8.16*

NIST SP 800-53, REVISION 5 CONTROLS		ISO/IEC 27001:2022 REQUIREMENTS AND CONTROLS <i>Note: An asterisk (*) indicates that the ISO/IEC control <b>does not fully satisfy</b> the intent of the NIST control.</i>
PE-7	<b>Withdrawn</b>	---
PE-8	Visitor Access Records	None
PE-9	Power Equipment and Cabling	A.7.5, A.7.8, A.7.11, A.7.12
PE-10	Emergency Shutoff	A.7.11*
PE-11	Emergency Power	A.7.11
PE-12	Emergency Lighting	A.7.11*
PE-13	Fire Protection	A.7.5, A.7.8
PE-14	Environmental Controls	A.7.5, A.7.8, A.7.11
PE-15	Water Damage Protection	A.7.5, A.7.8, A.7.11
PE-16	Delivery and Removal	A.5.10*, A.7.2*, A.7.10*
PE-17	Alternate Work Site	A.5.14*, A.6.7, A.7.9
PE-18	Location of System Components	A.5.10*, A.7.5, A.7.8
PE-19	Information Leakage	A.7.5*, A.7.8*, A.8.12
PE-20	Asset Monitoring and Tracking	A.5.10*
PE-21	Electromagnetic Pulse Protection	None
PE-22	Component Marking	A.5.13
PE-23	Facility Location	A.7.5, A.7.8
PL-1	Planning Policy and Procedures	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1, A.5.2, A.5.4, A.5.31, A.5.36, A.5.37
PL-2	System Security and Privacy Plans	7.5.1, 7.5.2, 7.5.3, 10.2, A.5.8*
PL-3	<b>Withdrawn</b>	---
PL-4	Rules of Behavior	A.5.4, A.5.10, A.6.2*
PL-5	<b>Withdrawn</b>	---
PL-6	<b>Withdrawn</b>	---
PL-7	Concept of Operations	8.1, A.5.8*
PL-8	Security and Privacy Architectures	A.5.8*
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, 9.3.1*, 10.1, A.5.1, A.5.2, A.5.4, A.5.31, A.5.36
PM-2	Information Security Program Leadership Role	5.1, 5.3, A.5.2
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, 9.3.2*, 10.2
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, 10.1
PM-10	Authorization Process	A.5.2*
PM-11	Mission and Business Process Definition	4.1
PM-12	Insider Threat Program	None
PM-13	Security and Privacy Workforce	7.2, A.6.3*
PM-14	Testing, Training, and Monitoring	6.2*
PM-15	Security and Privacy Groups and Associations	7.4, A.5.6
PM-16	Threat Awareness Program	A.5.7
PM-17	Protecting Controlled Unclassified Information on External Systems	None
PM-18	Privacy Program Plan	A.5.4

NIST SP 800-53, REVISION 5 CONTROLS		ISO/IEC 27001:2022 REQUIREMENTS AND CONTROLS <i>Note: An asterisk (*) indicates that the ISO/IEC control <b>does not fully satisfy</b> the intent of the NIST control.</i>
PM-19	Privacy Program Leadership Role	None
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, 9.3.1*, A.5.2
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, 9.2.2*, 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, A.5.2, A.5.4, A.5.31, A.5.36, A.5.37
PS-2	Position Risk Designation	None
PS-3	Personnel Screening	A.6.1
PS-4	Personnel Termination	A.5.11, A.6.5
PS-5	Personnel Transfer	A.5.11, A.6.5
PS-6	Access Agreements	A.5.4*, A.6.2, A.6.6*
PS-7	External Personnel Security	A.5.2, A.5.4*
PS-8	Personnel Sanctions	7.3, A.6.4
PS-9	Position Descriptions	A.5.2
PT-1	Personally Identifiable Information Processing and Transparency Policy and Procedures	A.5.4
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, A.5.2, A.5.4, A.5.31, A.5.36, A.5.37
RA-2	Security Categorization	A.5.12*
RA-3	Risk Assessment	6.1.2, 8.2, 9.3.2*, A.8.8*
RA-4	<b>Withdrawn</b>	---
RA-5	Vulnerability Monitoring and Scanning	A.8.8*
RA-6	Technical Surveillance Countermeasures Survey	None
RA-7	Risk Response	6.1.3, 8.3, 10.2
RA-8	Privacy Impact Assessments	None
RA-9	Criticality Analysis	A.5.22*
RA-10	Threat Hunting	A.5.7*

NIST SP 800-53, REVISION 5 CONTROLS		ISO/IEC 27001:2022 REQUIREMENTS AND CONTROLS <i>Note: An asterisk (*) indicates that the ISO/IEC control <b>does not fully satisfy</b> the intent of the NIST control.</i>
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, A.5.2, A.5.4, A.5.23, A.5.31, A.5.36, A.5.37
SA-2	Allocation of Resources	None
SA-3	System Development Life Cycle	A.5.2*, A.5.8, A.8.25, A.8.31*
SA-4	Acquisition Process	8.1, A.5.8, A.5.20, A.5.23, A.8.29, A.8.30
SA-5	System Documentation	7.5.1, 7.5.2, 7.5.3, A.5.37*
SA-6	<b>Withdrawn</b>	---
SA-7	<b>Withdrawn</b>	---
SA-8	Security Engineering Principles	A.8.27, A.8.28*
SA-9	External System Services	A.5.2*, A.5.4*, A.5.8*, A.5.14*, A.5.22, A.5.23, A.8.21
SA-10	Developer Configuration Management	A.8.9, A.8.28*, A.8.30*, A.8.32
SA-11	Developer Testing and Evaluation	A.8.29, A.8.30*
SA-12	<b>Withdrawn</b>	---
SA-13	<b>Withdrawn</b>	---
SA-14	<b>Withdrawn</b>	---
SA-15	Development Process, Standards, and Tools	A.5.8*, A.8.25
SA-16	Developer-Provided Training	None
SA-17	Developer Security and Privacy Architecture and Design	A.8.25, A.8.27
SA-18	<b>Withdrawn</b>	---
SA-19	<b>Withdrawn</b>	---
SA-20	Customized Development of Critical Components	None
SA-21	Developer Screening	A.6.1
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, A.5.2, A.5.4, A.5.31, A.5.36, A.5.37
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.5.14*, A.8.16*, A.8.20*, A.8.22*, A.8.23*, A.8.26*
SC-8	Transmission Confidentiality and Integrity	A.5.10*, A.5.14, A.8.20*, A.8.26*
SC-9	<b>Withdrawn</b>	---
SC-10	Network Disconnect	A.8.20
SC-11	Trusted Path	None
SC-12	Cryptographic Key Establishment and Management	A.8.24
SC-13	Cryptographic Protection	A.8.24, A.8.26, A.5.31
SC-14	<b>Withdrawn</b>	---
SC-15	Collaborative Computing Devices and Applications	A.5.14*
SC-16	Transmission of Security and Privacy Attributes	None
SC-17	Public Key Infrastructure Certificates	A.8.24
SC-18	Mobile Code	None
SC-19	<b>Withdrawn</b>	None
SC-20	Secure Name/Address Resolution Service (Authoritative Source)	None
SC-21	Secure Name/Address Resolution Service (Recursive or Caching Resolver)	None

NIST SP 800-53, REVISION 5 CONTROLS		ISO/IEC 27001:2022 REQUIREMENTS AND CONTROLS <i>Note: An asterisk (*) indicates that the ISO/IEC control <b>does not fully satisfy</b> the intent of the NIST control.</i>
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.5.10*
SC-29	Heterogeneity	None
SC-30	Concealment and Misdirection	None
SC-31	Covert Channel Analysis	None
SC-32	System Partitioning	None
SC-33	<b>Withdrawn</b>	---
SC-34	Non-Modifiable Executable Programs	None
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.8.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	None
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, A.5.2, A.5.4, A.5.31, A.5.36, A.5.37
SI-2	Flaw Remediation	A.6.8*, A.8.8, A.8.32*
SI-3	Malicious Code Protection	A.8.7
SI-4	System Monitoring	A.8.16*
SI-5	Security Alerts, Advisories, and Directives	A.5.6*
SI-6	Security and Privacy Function Verification	None
SI-7	Software, Firmware, and Information Integrity	None
SI-8	Spam Protection	None
SI-9	<b>Withdrawn</b>	---
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

NIST SP 800-53, REVISION 5 CONTROLS		ISO/IEC 27001:2022 REQUIREMENTS AND CONTROLS <i>Note: An asterisk (*) indicates that the ISO/IEC control <b>does not fully satisfy</b> the intent of the NIST control.</i>
SI-16	Memory Protection	None
SI-17	Fail-Safe Procedures	None
SI-18	Personally Identifiable Information Quality Operations	None
SI-19	De-identification	None
SI-20	Tainting	A.8.12
SI-21	Information Refresh	A.8.10
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, A.5.2, A.5.4, A.5.19, A.5.31, A.5.36, A.5.37
SR-2	Supply Chain Risk Management Plan	A.5.19, A.5.20*, A.5.21*, A.8.30*
SR-3	Supply Chain Controls and Processes	A.5.20, A.5.21*
SR-4	Provenance	A.5.21*, A.8.30*
SR-5	Acquisition Strategies, Tools, and Methods	A.5.20, A.5.21, A.5.23
SR-6	Supplier Assessments and Reviews	A.5.22
SR-7	Supply Chain Operations Security	A.5.22*
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

Table 2 provides a mapping from the security requirements and controls in ISO/IEC 27001 to the security controls in Special Publication 800-53 including mappings of ISO/IEC 27001 requirements and controls to control enhancements.<sup>3</sup> Please review the introductory text provided above before employing the mappings in Table 2.

TABLE 2: MAPPING ISO/IEC 27001:2022 TO NIST SP 800-53, REVISION 5

ISO/IEC 27001:2022 REQUIREMENTS AND CONTROLS	NIST SP 800-53, REVISION 5 CONTROLS
	Note: An asterisk (*) indicates that the ISO/IEC control does not fully satisfy the intent of the NIST control.
ISO/IEC 27001 Requirements	
<b>4. Context of the Organization</b>	
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
<b>5. Leadership</b>	
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
<b>6. Planning</b>	
<b>6.1 Actions to address risks and opportunities</b>	
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 to achieve them	PM-1, PM-3, PM-4, PM-6, PM-9, PM-14, PM-28, PM-30, PM-31
<b>7. Support</b>	
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
<b>7.5 Documented information</b>	
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
<b>8. Operation</b>	
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
<b>9. Performance evaluation</b>	
9.1 Monitoring, measurement, analysis and evaluation	CA-1, CA-7, PM-6, PM-31
9.2 Internal audit	
9.2.1 General	CA-2*, CA-7*
9.2.2 Internal audit programme	CA-1*, CA-2*, CA-2(1)*, CA-7(1)*, PM-31*

<sup>3</sup> 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.

<b>ISO/IEC 27001:2022 REQUIREMENTS AND CONTROLS</b>		<b>NIST SP 800-53, REVISION 5 CONTROLS</b> <i>Note: An asterisk (*) indicates that the ISO/IEC control does not fully satisfy the intent of the NIST control.</i>
9.3 Management review		
9.3.1 General		CA-1*, CA-6*, PM-1*, PM-29
9.3.2 Management review inputs		CA-7*, CA-7(3)*, CA-7(4)*, PM-4*, RA-3*
9.3.3 Management review results		CA-5*, CA-6*, CA-7*, CM-3*
<b>10. Improvement</b>		
10.1 Continual improvement		PM-1, PM-9, PM-30, PM-31
10.2 Nonconformity and corrective action		CA-5, PL-2, PM-4, PM-31, RA-7
<b>ISO/IEC 27001 Controls</b>		
<b>5 Organizational controls</b>		
5.1 Policies for information security		
5.2 Information security roles and responsibilities		
5.3 Segregation of duties		
5.4 Management responsibilities		
5.5 Contact with authorities		
5.6 Contact with special interest groups		
5.7 Threat intelligence		
5.8 Information security in project management		
5.9 Inventory of information and other associated assets		
5.10 Acceptable use of information and other associated assets		
5.11 Return of assets		
5.12 Classification of information		
5.13 Labelling of information		
5.14 Information transfer		
5.15 Access control		
5.16 Identity management		
5.17 Authentication information		
5.18 Access rights		
5.19 Information security in supplier relationships		
5.20 Addressing information security within supplier agreements		
5.21 Managing information security in the information and communication technology (ICT) supply chain		
5.22 Monitoring, review and change management of supplier services		
5.23 Information security for use of cloud services		
5.24 Information security incident management planning and preparation		
5.25 Assessment and decision on information security events		
5.26 Response to information security events		
5.27 Learning from information security incidents		
5.28 Collection of evidence		
5.29 Information security during disruption		
5.30 ICT readiness for business continuity		
5.31 Legal, statutory, regulatory and contractual requirements		
5.32 Intellectual property rights		
5.33 Protection of records		

<b>ISO/IEC 27001:2022 REQUIREMENTS AND CONTROLS</b>	<b>NIST SP 800-53, REVISION 5 CONTROLS</b> <i>Note: An asterisk (*) indicates that the ISO/IEC control does not fully satisfy the intent of the NIST control.</i>
5.34 Privacy and protection of personal identifiable information (PII)	PM-18, PT-1, PT-3, PT-7, CA-9*, CA-3*, PL-2*, PL-8*
5.35 Independent review of information security	CA-2(1)
5.36 Compliance with policies, rules and standards for information security	All XX-1 controls, CA-2
5.37 Documented operating procedures	All XX-1 controls, SA-5
<b>6 People controls</b>	
6.1 Screening	PS-3, SA-21
6.2 Terms and conditions of employment	PL-4, PS-6
6.3 Information security awareness, education, and training	AT-2, AT-3, CP-3, IR-2, PM-13
6.4 Disciplinary process	PS-8
6.5 Responsibilities after termination or change of employment	PS-4, PS-5
6.6 Confidentiality or non-disclosure agreements	PS-6
6.7 Remote working	None
6.8 Information security event reporting	AU-6, IR-6, SI-2
<b>7 Physical Controls</b>	
7.1 Physical security perimeters	PE-3*
7.2 Physical entry	PE-2, PE-3, PE-4, PE-5, PE-16
7.3 Securing offices, rooms and facilities	PE-3, PE-5
7.4 Physical security monitoring	AU-6(6)*, PE-3, PE-3(3), PE-6, PE-6(1), PE-6(4)*
7.5 Protecting against physical and environmental threats	CP-6, CP-7, PE-9, PE-13, PE-14, PE-15, PE-18, PE-19, PE-23
7.6 Working in secure areas	SC-42*
7.7 Clear desk and clear screen	AC-11, MP-2, MP-4
7.8 Equipment siting and protection	PE-9, PE-13, PE-14, PE-15, PE-18, PE-19, PE-23
7.9 Security of assets off-premises	AC-19, AC-20, MP-5, PE-17
7.10 Storage media	MA-2, MP-2, MP-4, MP-5, MP-6, MP-7, PE-16
7.11 Supporting utilities	CP-8, PE-9, PE-10, PE-11, PE-12, PE-14, PE-15
7.12 Cabling security	PE-4, PE-9
7.13 Equipment maintenance	MA-2, MA-6
7.14 Secure disposal or re-use of equipment	MP-6
<b>8 Technological controls</b>	
8.1 User end point devices	AC-11
8.2 Privileged access rights	AC-2, AC-3, AC-6, CM-5
8.3 Information access restriction	AC-3, AC-24
8.4 Access to source code	AC-3*, AC-3(11), CM-5
8.5 Secure authentication	AC-7, AC-8, AC-9, IA-6
8.6 Capacity management	AU-4, CP-2(2), SC-5(2)*
8.7 Protection against malware	AT-2, SI-3
8.8 Management of technical vulnerabilities	RA-3, RA-5, SI-2, SI-5
8.9 Configuration management	CM-1, CM-2, CM-2(3)*, CM-3, CM-3(7), CM-3(8), CM-4, CM-5, CM-6, CM-8, CM-9, CM-9(1)*, SA-10
8.10 Information deletion	AC-4(25)*, AC-7(2)*, MA-2, MA-3(3)*, MA-4(3)*, MP-4, MP-6, MP-6(1)*, SI-21
8.11 Data masking	AC-4(23), SI-19(4)
8.12 Data leakage prevention	AU-13, PE-3(2)*, PE-19, SC-7(10)*, SI-20
8.13 Information backup	CP-9
8.14 Redundancy of information processing facilities	CP-2, CP-6, CP-7
8.15 Logging	AU-3, AU-6, AU-9, AU-11, AU-12, AU-14

<b>ISO/IEC 27001:2022 REQUIREMENTS AND CONTROLS</b>		<b>NIST SP 800-53, REVISION 5 CONTROLS</b>
		<i>Note: An asterisk (*) indicates that the ISO/IEC control does not fully satisfy the intent of the NIST control.</i>
8.16 Monitoring activities		AC-2(12), AC-17(1), AU-13*, IR-4(13)*, MA-4(1)*, PE-6*, PE-6(3)*, SI-4, SI-4(4)*, SI-4(13)*, SI-4(16)*
8.17 Clock synchronization		AU-8
8.18 Use of privileged utility programs		AC-3, AC-6
8.19 Installation of software on operational systems		CM-5, CM-7(4)*, CM-7(5)*, CM-11*
8.20 Networks security		AC-3, AC-18, AC-20, SC-7, SC-8, SC-10
8.21 Security of network services		CA-3, SA-9
8.22 Segregation of networks		AC-4, SC-7
8.23 Web filtering		AC-4, SC-7, SC-7(8)
8.24 Use of cryptography		SC-12, SC-13, SC-17
8.25 Secure development life cycle		SA-3, SA-15, SA-17
8.26 Application security requirements		AC-3, SC-8*, SC-13
8.27 Secure system architecture and engineering principles		SA-8
8.28 Secure coding		SA-4(3)*, SA-8, SA-11(1)*, SA-15(5)*, SI-10
8.29 Security testing in development and acceptance		CA-2, SA-4, SA-11, SR-5(2)*
8.30 Outsourced development		SA-4, SA-10, SA-11, SA-15, SR-2, SR-4
8.31 Separation of development, test and production environments		CM-4(1), CM-5*, SA-3*
8.32 Change management		CM-3, CM-5, SA-10, SI-2
8.33 Test information		SA-3(2)*
8.34 Protection of information systems during audit testing		AU-5*