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

The mapping tables in this appendix provide organizations with a *general* indication of security control coverage with respect to ISO/IEC 27001, *Information technology–Security techniques–Information security management systems–Requirements.*[1] 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 information 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 27001:2013 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 business continuity management 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 A.6.1.1, Information Security Roles and Responsibilities, in ISO/IEC 27001 states that "all information security responsibilities shall be defined and allocated" while security control PM-10, Security Authorization Process, in Special Publication 800-53 that is mapped to A.6.1.1, has three distinct parts. Part b. of PM-10 requires designation of "individuals to fulfill specific roles and responsibilities…" If A.6.1.1 is mapped to PM-10 without any additional information, organizations might assume that if A.6.1.1 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 the left column of the

[1] ISO/IEC 27001 was published in October 2013 by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

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.

And finally, the security controls from ISO/IEC 27002 were not considered in the mapping analysis since the 27002 standard is informative rather than normative.

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
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

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.*
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*
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

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.*
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
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

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-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
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
PM-20	Dissemination of Privacy Program Information	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-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
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

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.*
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
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

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-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
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

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

Table 2 provides a mapping from the security requirements and controls in ISO/IEC 27001 to the security controls in Special Publication 800-53.[2] 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	
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

[2] 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.

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.*
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
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	

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.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	
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

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.12.4 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
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	
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	

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.15.2.1 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)
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