

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

NIST SP 800-53 CONTROLS		ISO/IEC 27001 CONTROLS
AC-1	Access Control Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.3, A.8.1.1, A.10.1.1, A.10.8.1, A.11.1.1, A.11.2.1, A.11.2.2, A.11.4.1, A.11.7.1, A.11.7.2, A.15.1.1, A.15.2.1
AC-2	Account Management	A.8.3.3, A.11.2.1, A.11.2.2, A.11.2.4, A.11.5.6, A.15.2.1
AC-3	Access Enforcement	A.10.8.1, A.11.4.4, A.11.4.6, A.11.5.4, A.11.6.1, A.12.4.2
AC-4	Information Flow Enforcement	A.10.6.1, A.10.8.1, A.11.4.5, A.11.4.7, A.11.7.2, A.12.4.2, A.12.5.4
AC-5	Separation of Duties	A.6.1.3, A.8.1.1, A.10.1.3, A.11.1.1, A.11.4.1
AC-6	Least Privilege	A.6.1.3, A.8.1.1, A.11.1.1, A.11.2.2, A.11.4.1, A.11.4.4, A.11.4.6, A.11.5.4, A.11.6.1, A.12.4.3
AC-7	Unsuccessful Logon Attempts	A.11.5.1
AC-8	System Use Notification	A.6.2.2, A.8.1.1, A.11.5.1, A.15.1.5
AC-9	Previous Logon (Access) Notification	A.11.5.1
AC-10	Concurrent Session Control	A.11.5.1
AC-11	Session Lock	A.11.3.2, A.11.3.3, A.11.5.5
AC-12	<b>Withdrawn</b>	---
AC-13	<b>Withdrawn</b>	---
AC-14	Permitted Actions without Identification or Authentication	A.11.6.1
AC-15	<b>Withdrawn</b>	---
AC-16	Security Attributes	A.7.2.2
AC-17	Remote Access	A.10.6.1, A.10.8.1, A.11.1.1, A.11.4.1, A.11.4.2, A.11.4.4, A.11.4.6, A.11.4.7, A.11.7.1, A.11.7.2
AC-18	Wireless Access	A.10.6.1, A.10.8.1, A.11.1.1, A.11.4.1, A.11.4.2, A.11.4.4, A.11.4.6, A.11.4.7, A.11.7.1, A.11.7.2
AC-19	Access Control for Mobile Devices	A.10.4.1, A.11.1.1, A.11.4.3, A.11.7.1
AC-20	Use of External Information Systems	A.7.1.3, A.8.1.1, A.8.1.3, A.10.6.1, A.10.8.1, A.11.4.1, A.11.4.2
AC-21	Information Sharing	A.11.2.1, A.11.2.2
AC-22	Publicly Accessible Content	None
AC-23	Data Mining Protection	None
AC-24	Access Control Decisions	None
AC-25	Reference Monitor	None
AT-1	Security Awareness and Training Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.3, A.8.1.1, A.10.1.1, A.15.1.1, A.15.2.1
AT-2	Security Awareness Training	A.6.2.2, A.8.1.1, A.8.2.2, A.9.1.5, A.10.4.1
AT-3	Role-Based Security Training	A.8.1.1, A.8.2.2, A.9.1.5
AT-4	Security Training Records	None
AT-5	<b>Withdrawn</b>	---
AU-1	Audit and Accountability Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.3, A.8.1.1, A.10.1.1, A.10.10.2, A.15.1.1, A.15.2.1, A.15.3.1
AU-2	Audit Events	A.10.10.1, A.10.10.4, A.10.10.5, A.15.3.1
AU-3	Content of Audit Records	A.10.10.1
AU-4	Audit Storage Capacity	A.10.10.1, A.10.3.1
AU-5	Response to Audit Processing Failures	A.10.3.1, A.10.10.1
AU-6	Audit Review, Analysis, and Reporting	A.10.10.2, A.10.10.5, A.13.1.1, A.15.1.5
AU-7	Audit Reduction and Report Generation	A.10.10.2
AU-8	Time Stamps	A.10.10.1, A.10.10.6
AU-9	Protection of Audit Information	A.10.10.3, A.13.2.3, A.15.1.3, A.15.3.2
AU-10	Non-repudiation	A.10.9.1, A.12.2.3
AU-11	Audit Record Retention	A.10.10.1, A.10.10.2, A.15.1.3
AU-12	Audit Generation	A.10.10.1, A.10.10.4, A.10.10.5
AU-13	Monitoring for Information Disclosure	None
AU-14	Session Audit	None

NIST SP 800-53 CONTROLS		ISO/IEC 27001 CONTROLS
AU-15	Alternate Audit Capability	None
AU-16	Cross-Organizational Auditing	A.6.2.3
CA-1	Security Assessment and Authorization Policies and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.3 A.6.1.4, A.8.1.1, A.10.1.1, A.15.1.1, A.15.2.1
CA-2	Security Assessments	A.6.1.8, A.6.2.3, A.10.3.2, A.15.2.1, A.15.2.2
CA-3	System Interconnections	A.6.2.1, A.6.2.3, A.10.6.1, A.10.6.2, A.10.8.1, A.10.8.2, A.10.8.5, A.11.4.2
CA-4	<b>Withdrawn</b>	---
CA-5	Plan of Action and Milestones	None
CA-6	Security Authorization	A.6.1.4, A.10.3.2
CA-7	Continuous Monitoring	A.6.1.8, A.15.2.1, A.15.2.2
CA-8	Penetration Testing	None.
CA-9	Internal System Connections	None.
CM-1	Configuration Management Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.3, A.8.1.1, A.10.1.1, A.10.1.2, A.12.4.1, A.12.5.1, A.15.1.1, A.15.2.1
CM-2	Baseline Configuration	A.12.4.1, A.10.1.4
CM-3	Configuration Change Control	A.10.1.1, A.10.1.2, A.10.3.2, A.12.4.1, A.12.5.1, A.12.5.2, A.12.5.3
CM-4	Security Impact Analysis	A.10.1.2, A.10.3.2, A.12.4.1, A.12.5.2, A.12.5.3
CM-5	Access Restrictions for Change	A.10.1.2, A.11.1.1, A.11.6.1, A.12.4.1, A.12.4.3, A.12.5.3
CM-6	Configuration Settings	None
CM-7	Least Functionality	None
CM-8	Information System Component Inventory	A.7.1.1, A.7.1.2
CM-9	Configuration Management Plan	A.6.1.3, A.7.1.1, A.7.1.2, A.8.1.1, A.10.1.1, A.10.1.2, A.10.3.2, A.12.4.1, A.12.4.3, A.12.5.1, A.12.5.2, A.12.5.3
CM-10	Software Usage Restrictions	A.12.4.1, A.12.5.5, A.15.1.2
CM-11	User-Installed Software	A.12.4.1, A.12.5.5, A.15.1.5
CP-1	Contingency Planning Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.3, A.8.1.1, A.9.1.4, A.10.1.1, A.10.1.2, A.14.1.1, A.14.1.3, A.15.1.1, A.15.2.1
CP-2	Contingency Plan	A.6.1.2, A.9.1.4, A.10.3.1, A.14.1.1, A.14.1.2, A.14.1.3, A.14.1.4, A.14.1.5
CP-3	Contingency Training	A.8.2.2, A.9.1.4, A.14.1.3
CP-4	Contingency Plan Testing	A.6.1.2, A.9.1.4, A.14.1.1, A.14.1.3, A.14.1.4, A.14.1.5
CP-5	<b>Withdrawn</b>	---
CP-6	Alternate Storage Site	A.9.1.4, A.14.1.3
CP-7	Alternate Processing Site	A.9.1.4, A.14.1.3
CP-8	Telecommunications Services	A.9.1.4, A.10.6.1, A.14.1.3
CP-9	Information System Backup	A.9.1.4, A.10.5.1, A.14.1.3, A.15.1.3
CP-10	Information System Recovery and Reconstitution	A.9.1.4, A.14.1.3
CP-11	Alternate Communications Protocols	None
CP-12	Safe Mode	None
CP-13	Alternative Security Mechanisms	None
IA-1	Identification and Authentication Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.3, A.8.1.1, A.10.1.1, A.11.2.1, A.15.1.1, A.15.2.1
IA-2	Identification and Authentication (Organizational Users)	A.11.3.2, A.11.5.1, A.11.5.2, A.11.5.3
IA-3	Device Identification and Authentication	A.11.4.3
IA-4	Identifier Management	A.11.5.2
IA-5	Authenticator Management	A.11.2.1, A.11.2.3, A.11.3.1, A.11.5.2, A.11.5.3
IA-6	Authenticator Feedback	A.11.5.1
IA-7	Cryptographic Module Authentication	A.12.3.1, A.15.1.1, A.15.1.6, A.15.2.1
IA-8	Identification and Authentication (Non-Organizational Users)	A.10.9.1, A.11.4.2, A.11.5.1, A.11.5.2
IA-9	Service Identification and Authentication	None

NIST SP 800-53 CONTROLS		ISO/IEC 27001 CONTROLS
IA-10	Adaptive Identification and Authentication	None
IA-11	Re-authentication	None
IR-1	Incident Response Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.3, A.8.1.1, A.10.1.1, A.13.1.1, A.13.2.1, A.15.1.1, A.15.2.1
IR-2	Incident Response Training	A.8.2.2
IR-3	Incident Response Testing	None
IR-4	Incident Handling	A.6.1.2, A.13.2.2, A.13.2.3
IR-5	Incident Monitoring	None
IR-6	Incident Reporting	A.6.1.6, A.13.1.1
IR-7	Incident Response Assistance	None
IR-8	Incident Response Plan	None
IR-9	Information Spillage Response	A.12.5.4
IR-10	Integrated Information Security Cell	None
MA-1	System Maintenance Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.3, A.8.1.1, A.9.2.4, A.10.1.1, A.15.1.1, A.15.2.1
MA-2	Controlled Maintenance	A.9.2.4
MA-3	Maintenance Tools	A.9.2.4, A.11.4.4
MA-4	Nonlocal Maintenance	A.9.2.4, A.11.4.4
MA-5	Maintenance Personnel	A.9.2.4, A.12.4.3
MA-6	Timely Maintenance	A.9.2.4
MP-1	Media Protection Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.3, A.8.1.1, A.10.1.1, A.10.7.1, A.10.7.2, A.10.7.3, A.11.1.1, A.15.1.1, A.15.1.3, A.15.2.1
MP-2	Media Access	A.7.2.2, A.10.7.1, A.10.7.3
MP-3	Media Marking	A.7.2.2, A.10.7.1, A.10.7.3
MP-4	Media Storage	A.10.7.1, A.10.7.3, A.10.7.4, A.11.3.3, A.15.1.3
MP-5	Media Transport	A.9.2.5, A.9.2.7, A.10.7.1, A.10.7.3, A.10.8.3
MP-6	Media Sanitization	A.9.2.6, A.10.7.1, A.10.7.2, A.10.7.3
MP-7	Media Use	None
MP-8	Media Downgrading	None
PE-1	Physical and Environmental Protection Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.3, A.8.1.1, A.9.1.4, A.9.2.1, A.9.2.2, A.10.1.1, A.11.1.1, A.11.2.1, A.11.2.2, A.15.1.1, A.15.2.1
PE-2	Physical Access Authorizations	A.9.1.5, A.11.2.1, A.11.2.2, A.11.2.4
PE-3	Physical Access Control	A.9.1.1, A.9.1.2, A.9.1.3, A.9.1.5, A.9.1.6, A.11.3.2, A.11.4.4
PE-4	Access Control for Transmission Medium	A.9.1.3, A.9.1.5, A.9.2.3
PE-5	Access Control for Output Devices	A.9.1.2, A.9.1.3, A.10.6.1, A.11.3.2
PE-6	Monitoring Physical Access	A.9.1.2, A.9.1.5, A.10.10.2
PE-7	<b>Withdrawn</b>	---
PE-8	Visitor Access Records	A.9.1.5, A.10.10.2, A.15.2.1
PE-9	Power Equipment and Cabling	A.9.1.4, A.9.2.2, A.9.2.3
PE-10	Emergency Shutoff	A.9.1.4
PE-11	Emergency Power	A.9.1.4, A.9.2.2
PE-12	Emergency Lighting	A.9.2.2
PE-13	Fire Protection	A.9.1.4
PE-14	Temperature and Humidity Controls	A.9.2.2
PE-15	Water Damage Protection	A.9.1.4
PE-16	Delivery and Removal	A.9.1.6, A.9.2.7, A.10.7.1
PE-17	Alternate Work Site	A.9.2.5, A.11.7.2
PE-18	Location of Information System Components	A.9.2.1, A.11.3.2
PE-19	Information Leakage	A.12.5.4
PL-1	Security Planning Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.2, A.6.1.3, A.8.1.1, A.10.1.1, A.15.1.1, A.15.2.1
PL-2	System Security Plan	A.6.1.2, A.15.3.1
PL-3	<b>Withdrawn</b>	---

NIST SP 800-53 CONTROLS		ISO/IEC 27001 CONTROLS
PL-4	Rules of Behavior	A.6.1.5, A.6.2.2, A.7.1.3, A.8.1.1, A.8.1.3, A.8.2.1, A.9.1.5, A.10.8.1, A.11.7.1, A.11.7.2, A.12.4.1, A.13.1.2, A.15.1.5
PL-5	<b>Withdrawn</b>	---
PL-6	<b>Withdrawn</b>	---
PL-7	Security Concept of Operations	A.12.1.1
PL-8	Information Security Architecture	A.12.1.1
PL-9	Central Management	None
PS-1	Personnel Security Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.3, A.8.1.1, A.10.1.1, A.15.1.1, A.15.2.1
PS-2	Position Risk Designation	A.8.1.1
PS-3	Personnel Screening	A.8.1.2
PS-4	Personnel Termination	A.8.3.1, A.8.3.2, A.8.3.3
PS-5	Personnel Transfer	A.8.3.1, A.8.3.2, A.8.3.3
PS-6	Access Agreements	A.6.1.5, A.8.1.1, A.8.1.3, A.8.2.1, A.9.1.5, A.10.8.1, A.11.7.1, A.11.7.2, A.15.1.5
PS-7	Third-Party Personnel Security	A.6.2.3, A.8.1.1, A.8.2.1, A.8.1.3
PS-8	Personnel Sanctions	A.8.2.3, A.15.1.5
RA-1	Risk Assessment Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.3, A.8.1.1, A.10.1.1, A.14.1.2, A.15.1.1, A.15.2.1
RA-2	Security Categorization	A.7.2.1, A.14.1.2
RA-3	Risk Assessment	A.6.2.1, A.10.2.3, A.12.6.1, A.14.1.2
RA-4	<b>Withdrawn</b>	---
RA-5	Vulnerability Scanning	A.12.6.1, A.15.2.2
RA-6	Technical Surveillance Countermeasures Survey	None
SA-1	System and Services Acquisition Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.3, A.6.2.1, A.8.1.1, A.10.1.1, A.12.1.1, A.12.5.5, A.15.1.1, A.15.2.1
SA-2	Allocation of Resources	A.6.1.2, A.10.3.1
SA-3	System Development Life Cycle	A.12.1.1
SA-4	Acquisition Process	A.12.1.1, A.12.5.5
SA-5	Information System Documentation	A.10.7.4, A.15.1.3
SA-6	<b>Withdrawn</b>	---
SA-7	<b>Withdrawn</b>	---
SA-8	Security Engineering Principles	A.10.4.1, A.10.4.2, A.11.4.5, A.12.5.5
SA-9	External Information System Services	A.6.1.5, A.6.2.1, A.6.2.3, A.8.1.1, A.8.2.1, A.10.2.1, A.10.2.2, A.10.2.3, A.10.6.2, A.10.8.2, A.12.5.5
SA-10	Developer Configuration Management	A.10.2.3, A.12.4.3, A.12.5.1, A.12.5.5
SA-11	Developer Security Testing and Evaluation	A.10.3.2, A.12.5.5
SA-12	Supply Chain Protections	A.12.5.5
SA-13	Trustworthiness	A.12.5.5
SA-14	Criticality Analysis	None
SA-15	Development Process, Standards, and Tools	A.10.3.2, A.12.5.5
SA-16	Developer-Provided Training	None
SA-17	Developer Security Architecture and Design	A.10.3.2, A.12.5.5
SA-18	Tamper Resistance and Detection	None
SA-19	Component Authenticity	None
SA-20	Customized Development of Critical Components	None
SA-21	Developer Screening	None
SC-1	System and Communications Protection Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.3, A.8.1.1, A.10.1.1, A.15.1.1, A.15.2.1
SC-2	Application Partitioning	A.10.4.1, A.10.4.2
SC-3	Security Function Isolation	A.10.4.1, A.10.4.2, A.10.9.1, A.10.9.2

NIST SP 800-53 CONTROLS		ISO/IEC 27001 CONTROLS
SC-4	Information In Shared Resources	None
SC-5	Denial of Service Protection	A.10.3.1
SC-6	Resource Availability	None
SC-7	Boundary Protection	A.6.2.1, A.10.4.1, A.10.4.2, A.10.6.1, A.10.8.1, A.10.9.1, A.10.9.2, A.10.10.2, A.11.4.5, A.11.4.6, A.11.6.2
SC-8	Transmission Confidentiality and Integrity	A.10.4.2, A.10.6.1, A.10.6.2, A.10.9.1, A.10.9.2, A.12.2.3, A.12.3.1
SC-9	<b>Withdrawn</b>	---
SC-10	Network Disconnect	A.10.6.1, A.11.3.2, A.11.5.1, A.11.5.5
SC-11	Trusted Path	None
SC-12	Cryptographic Key Establishment and Management	A.12.3.2
SC-13	Cryptographic Protection	A.12.3.1, A.15.1.6
SC-14	<b>Withdrawn</b>	---
SC-15	Collaborative Computing Devices	None
SC-16	Transmission of Security Attributes	A.7.2.2, A.10.8.1
SC-17	Public Key Infrastructure Certificates	A.12.3.2
SC-18	Mobile Code	A.10.4.2
SC-19	Voice Over Internet Protocol	A.10.6.1
SC-20	Secure Name/Address Resolution Service (Authoritative Source)	A.10.6.1
SC-21	Secure Name/Address Resolution Service (Recursive or Caching Resolver)	A.10.6.1
SC-22	Architecture and Provisioning for Name/Address Resolution Service	A.10.6.1
SC-23	Session Authenticity	A.10.6.1, A.12.2.3
SC-24	Fail in Known State	None
SC-25	Thin Nodes	None
SC-26	Honeypots	None
SC-27	Platform-Independent Applications	None
SC-28	Protection of Information at Rest	None
SC-29	Heterogeneity	None
SC-30	Concealment and Misdirection	None
SC-31	Covert Channel Analysis	None
SC-32	Information System Partitioning	None
SC-33	<b>Withdrawn</b>	---
SC-34	Non-Modifiable Executable Programs	None
SC-35	Honeyclients	None
SC-36	Distributed Processing and Storage	None
SC-37	Out-of-Band Channels	None
SC-38	Operations Security	None
SC-39	Process Isolation	None
SC-40	Wireless Link Protection	None
SC-41	Port and I/O Device Access	A.10.4.1
SC-42	Sensor Data	None
SC-43	Usage Restrictions	None
SC-44	Detonation Chambers	None
SI-1	System and Information Integrity Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.3, A.8.1.1, A.10.1.1, A.15.1.1, A.15.2.1
SI-2	Flaw Remediation	A.10.10.5, A.12.5.2, A.12.6.1, A.13.1.2
SI-3	Malicious Code Protection	A.10.4.1
SI-4	Information System Monitoring	A.10.10.2, A.13.1.1, A.13.1.2
SI-5	Security Alerts, Advisories, and Directives	A.6.1.6, A.6.1.7, A.12.6.1, A.13.1.1, A.13.1.2
SI-6	Security Function Verification	None

NIST SP 800-53 CONTROLS		ISO/IEC 27001 CONTROLS
SI-7	Software, Firmware, and Information Integrity	A.10.4.1, A.12.2.2, A.12.2.3, A.12.2.4
SI-8	Spam Protection	None
SI-9	<b>Withdrawn</b>	---
SI-10	Information Input Validation	A.12.2.1, A.12.2.2
SI-11	Error Handling	None
SI-12	Information Handling and Retention	A.10.7.3, A.15.1.3, A.15.1.4, A.15.2.1
SI-13	Predictable Failure Prevention	None
SI-14	Non-Persistence	None
SI-15	Information Output Filtering	None
SI-16	Memory Protection	None
PM-1	Information Security Program Plan	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.3 A.8.1.1, A.15.1.1, A.15.2.1
PM-2	Senior Information Security Officer	A.6.1.1, A.6.1.2, A.6.1.3
PM-3	Information Security Resources	A.6.1.1
PM-4	Plan of Action and Milestones Process	None
PM-5	Information System Inventory	A.7.1.1, A.7.1.2
PM-6	Information Security Measures of Performance	None
PM-7	Enterprise Architecture	None
PM-8	Critical Infrastructure Plan	None
PM-9	Risk Management Strategy	A.6.1.1, A.6.2.1, A.14.1.2
PM-10	Security Authorization Process	A.6.1.4
PM-11	Mission/Business Process Definition	None
PM-12	Insider Threat Program	None
PM-13	Information Security Workforce	A.8.2.1
PM-14	Testing, Training, and Monitoring	A.8.2.1
PM-15	Contacts with Security Groups and Associations	A.6.1.7
PM-16	Threat Awareness Program	None.

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

ISO/IEC 27001 CONTROLS	NIST SP 800-53 CONTROLS
<b>A.5 Security Policy</b>	
A.5.1 Information security policy	
A.5.1.1 Information security policy document	XX-1 controls
A.5.1.2 Review of the information security policy	XX-1 controls
<b>A.6 Organization of information security</b>	
A.6.1 Internal	
A.6.1.1 Management commitment to information security	XX-1 controls, PM-2, PM-3, PM-9; SP 800-39, SP 800-37
A.6.1.2 Information security coordination	CP-2, CP-4, IR-4, PL-1, PL-2, PM-2, SA-2; SP 800-39, SP 800-37
A.6.1.3 Allocation of information security responsibilities	XX-1 controls, AC-5, AC-6, CM-9, PM-2; SP 800-39, SP 800-37
A.6.1.4 Authorization process for information processing facilities	CA-1, CA-6, PM-10; SP 800-37
A.6.1.5 Confidentiality agreements	PL-4, PS-6, SA-9
A.6.1.6 Contact with authorities	Multiple controls with contact reference (e.g., IR-6, SI-5); SP 800-39; SP 800-37
A.6.1.7 Contact with special interest groups	PM-15, SI-5
A.6.1.8 Independent review of information security	CA-2, CA-7; SP 800-39, SP 800-37
A.6.2 External Parties	
A.6.2.1 Identification of risks related to external parties	CA-3, PM-9, RA-3, SA-1, SA-9, SC-7
A.6.2.2 Addressing security when dealing with customers	AC-8 , AT-2, PL-4
A.6.2.3 Addressing security in third party agreements	AU-16, CA-2, CA-3, PS-7, SA-9
<b>A.7 Asset Management</b>	
A.7.1 Responsibility for assets	
A.7.1.1 Inventory of assets	CM-8, CM-9, PM-5
A.7.1.2 Ownership of assets	CM-8, CM-9, PM-5
A.7.1.3 Acceptable use of assets	AC-20, PL-4
A.7.2 Information Classification	
A.7.2.1 Classification Guidelines	RA-2
A.7.2.2 Information labeling and handling	AC-16, MP-2, MP-3, SC-16
<b>A.8 Human Resources Security</b>	
A.8.1 Prior to Employment	
A.8.1.1 Roles and Responsibilities	XX-1 controls, AC-5, AC-6, AC-8, AC-20, AT-2, AT-3, CM-9, PL-4, PS-2, PS-6, PS-7, SA-9
A.8.1.2 Screening	PS-3
A.8.1.3 Terms and conditions of employment	AC-20, PL-4, PS-6, PS-7
A.8.2 During employment	
A.8.2.1 Management responsibilities	PL-4, PM-13, PM-14, PS-6, PS-7, SA-9
A.8.2.2 Awareness, education, and training	AT-2, AT-3, IR-2
A.8.2.3 Disciplinary process	PS-8
A.8.3 Termination or change of employment	
A.8.3.1 Termination responsibilities	PS-4, PS-5
A.8.3.2 Return of assets	PS-4, PS-5
A.8.3.3 Removal of access rights	AC-2, PS-4, PS-5
<b>A.9 Physical and environmental security</b>	
A.9.1 Secure areas	
A.9.1.1 Physical security perimeter	PE-3
A.9.1.2 Physical entry controls	PE-3, PE-5, PE-6
A.9.1.3 Securing offices, rooms, facilities	PE-3, PE-4, PE-5
A.9.1.4 Protecting against external and environmental threats	CP Family; PE-1, PE-9, PE-10, PE-11, PE-13, PE-15
A.9.1.5 Working in secure areas	AT-2, AT-3 , PL-4, PS-6, PE-2, PE-3, PE-4, PE-6, PE-8
A.9.1.6 Public access, delivery and loading areas	PE-3 , PE-16

ISO/IEC 27001 CONTROLS	NIST SP 800-53 CONTROLS
A.9.2 Equipment security	
A.9.2.1 Equipment siting and protection	PE-1, PE-18
A.9.2.2 Supporting utilities	PE-1, PE-9, PE-11, PE-12, PE-14
A.9.2.3 Cabling security	PE-4, PE-9
A.9.2.4 Equipment maintenance	MA Family
A.9.2.5 Security of equipment off-premises	MP-5, PE-17
A.9.2.6 Secure disposal or reuse of equipment	MP-6
A.9.2.7 Removal of property	MP-5, PE-16
<b>A.10 Communications and operations management</b>	
A.10.1 Operational procedures and responsibilities	
A.10.1.1 Documented operating procedures	XX-1 controls, CM-9
A.10.1.2 Change management	CM-1, CM-3, CM-4, CM-5, CM-9
A.10.1.3 Segregation of duties	AC-5
A.10.1.4 Separation of development, test and operational facilities	CM-2
A.10.2 Third-party service delivery management	
A.10.2.1 Service delivery	SA-9
A.10.2.2 Monitoring and review of third-party services	SA-9
A.10.2.3 Managing changes to third-party services	RA-3, SA-9, SA-10
A.10.3 System planning and acceptance	
A.10.3.1 Capacity management	AU-4, AU-5, CP-2, SA-2, SC-5
A.10.3.2 System acceptance	CA-2, CA-6, CM-3, CM-4, CM-9, SA-11, SA-15, SA-17
A.10.4 Protection against malicious and mobile code	
A.10.4.1 Controls against malicious code	AC-19, AT-2, SA-8, SC-2, SC-3, SC-7, SC-42, SI-3, SI-7
A.10.4.2 Controls against mobile code	SA-8, SC-2, SC-3, SC-7, SC-8, SC-18
A.10.5 Backup	
A.10.5.1 Information backup	CP-9
A.10.6 Network security management	
A.10.6.1 Network controls	AC-4, AC-17, AC-18, AC-20, CA-3, CP-8, PE-5, SC-7, SC-8, SC-10, SC-19, SC-20, SC-21, SC-22, SC-23
A.10.6.2 Security of network services	CA-3, SA-9, SC-8
A.10.7 Media handling	
A.10.7.1 Management of removable media	MP Family, PE-16
A.10.7.2 Disposal of media	MP-6
A.10.7.3 Information handling procedures	MP Family, SI-12
A.10.7.4 Security of system documentation	MP-4, SA-5
A.10.8 Exchange of information	
A.10.8.1 Information exchange policies and procedures	AC-1, AC-3, AC-4, AC-17, AC-18, AC-20, CA-3, PL-4, PS-6, SC-7, SC-16
A.10.8.2 Exchange agreements	CA-3, SA-9
A.10.8.3 Physical media in transit	MP-5
A.10.8.4 Electronic messaging	Multiple controls; electronic messaging not addressed separately in SP 800-53
A.10.8.5 Business information systems	CA-1, CA-3
A.10.9 Electronic commerce services	
A.10.9.1 Electronic commerce	AU-10, IA-8, SC-7, SC-8, SC-3
A.10.9.2 Online transactions	SC-3, SC-7, SC-8
A.10.9.3 Publicly available information	
A.10.10 Monitoring	
A.10.10.1 Audit logging	AU-1, AU-2, AU-3, AU-4, AU-5, AU-8, AU-11, AU-12
A.10.10.2 Monitoring system use	AU-1, AU-6, AU-7, PE-6, PE-8, SC-7, SI-4
A.10.10.3 Protection of log information	AU-9



ISO/IEC 27001 CONTROLS	NIST SP 800-53 CONTROLS
A.10.10.4 Administrator and operator logs	AU-2, AU-12
A.10.10.5 Fault logging	AU-2, AU-6, AU-12, SI-2
A.10.10.6 Clock synchronization	AU-8
<b>A.11 Access Control</b>	
A.11.1 Business requirement for access control	
A.11.1.1 Access control policy	AC-1, AC-5, AC-6, AC-17, AC-18, AC-19, CM-5, MP-1
A.11.2 User access management	
A.11.2.1 User registration	AC-1, AC-2, AC-21, IA-5, PE-1, PE-2
A.11.2.2 Privilege management	AC-1, AC-2, AC-6, AC-21, PE-1, PE-2
A.11.2.3 User password management	IA-5
A.11.2.4 Review of user access rights	AC-2, PE-2
A.11.3 User responsibilities	
A.11.3.1 Password use	IA-2, IA-5
A.11.3.2 Unattended user equipment	AC-11, IA-2, PE-3, PE-5, PE-18, SC-10
A.11.3.3 Clear desk and clear screen policy	AC-11, MP-4
A.11.4 Network access control	
A.11.4.1 Policy on use of network services	AC-1, AC-5, AC-6, AC-17, AC-18, AC-20
A.11.4.2 User authentication for external connections	AC-17, AC-18, AC-20, CA-3, IA-2, IA-8
A.11.4.3 Equipment identification in networks	AC-19, IA-3
A.11.4.4 Remote diagnostic and configuration port protection	AC-3, AC-6, AC-17, AC-18, PE-3, MA-3, MA-4
A.11.4.5 Segregation in networks	AC-4, SA-8, SC-7
A.11.4.6 Network connection control	AC-3, AC-6, AC-17, AC-18, SC-7
A.11.4.7 Network routing control	AC-4, AC-17, AC-18
A.11.5 Operating system access control	
A.11.5.1 Secure log-on procedures	AC-7, AC-8, AC-9, AC-10, IA-2, IA-6, IA-8, SC-10
A.11.5.2 User identification and authentication	IA-2, IA-4, IA-5, IA-8
A.11.5.3 Password management system	IA-2, IA-5
A.11.5.4 Use of system utilities	AC-3, AC-6
A.11.5.5 Session time-out	AC-11, SC-10
A.11.5.6 Limitation of connection time	AC-2
A.11.6 Application and information access control	
A.11.6.1 Information access restriction	AC-3, AC-6, AC-14, CM-5
A.11.6.2 Sensitive system isolation	SC-7; SP 800-39
A.11.7 Mobile computing and teleworking	
A.11.7.1 Mobile computing and communications	AC-1, AC-17, AC-18, AC-19, PL-4, PS-6
A.11.7.2 Teleworking	AC-1, AC-4, AC-17, AC-18, PE-17, PL-4, PS-6
<b>A.12 Information systems acquisition, development and maintenance</b>	
A.12.1 Security requirements of information systems	
A.12.1.1 Security requirements analysis and specification	PL-7, PL-8, SA-1, SA-3, SA-4
A.12.2 Correct processing in applications	
A.12.2.1 Input data validation	SI-10
A.12.2.2 Control of internal processing	SI-7, SI-10
A.12.2.3 Message integrity	AU-10, SC-8, SC-23, SI-7
A.12.2.4 Output data validation	SI-7
A.12.3 Cryptographic controls	
A.12.3.1 Policy on the use of cryptographic controls	Multiple controls address cryptography (e.g., IA-7, SC-8, SC-12, SC-13)
A.12.3.2 Key management	SC-12, SC-17
A.12.4 Security of system files	
A.12.4.1 Control of operational software	CM-1, CM-2, CM-3, CM-4, CM-5, CM-9, CM-10, CM-11, PL-4

ISO/IEC 27001 CONTROLS	NIST SP 800-53 CONTROLS
A.12.4.2 Protection of system test data	Multiple controls; protection of test data not addressed separately in SP 800-53 (e.g., AC-3, AC-4)
A.12.4.3 Access control to program source code	AC-3, AC-6, CM-5, CM-9, MA-5, SA-10
A.12.5 Security in development and support processes	
A.12.5.1 Change control procedures	CM-1, CM-3, CM-9, SA-10
A.12.5.2 Technical review of applications after operating system changes	CM-3, CM-4, CM-9, SI-2
A.12.5.3 Restrictions on changes to software packages	CM-3, CM-4, CM-5, CM-9
A.12.5.4 Information leakage	AC-4, IR-9, PE-19
A.12.5.5 Outsourced software development	CM-10, CM-11, SA-1, SA-4, SA-8, SA-9, SA-11, SA-12, SA-13, SA-15, SA-17
A.12.6 Technical Vulnerability Management	
A.12.6.1 Control of technical vulnerabilities	RA-3, RA-5, SI-2, SI-5
<b>A.13 Information security incident management</b>	
A.13.1 Reporting information security events and weaknesses	
A.13.1.1 Reporting information security events	AU-6, IR-1, IR-6, SI-4, SI-5
A.13.1.2 Reporting security weaknesses	PL-4, SI-2, SI-4, SI-5
A.13.2 Management of information security incidents and improvements	
A.13.2.1 Responsibilities and procedures	IR-1
A.13.2.2 Learning from information security incidents	IR-4
A.13.2.3 Collection of evidence	AU-7, AU-9, IR-4
<b>A.14 Business continuity management</b>	
A.14.1 Information security aspects of business continuity management	
A.14.1.1 Including information security in the business continuity management process	CP-1, CP-2, CP-4
A.14.1.2 Business continuity and risk assessment	CP-2, PM-9, RA Family
A.14.1.3 Developing and implementing continuity plans including information security	CP Family
A.14.1.4 Business continuity planning framework	CP-2, CP-4
A.14.1.5 Testing, maintaining and reassessing business continuity plans	CP-2, CP-4
<b>A.15 Compliance</b>	
A.15.1 Compliance with legal requirements	
A.15.1.1 Identification of applicable legislation	XX-1 controls, IA-7
A.15.1.2 Intellectual property rights (IPR)	CM-10
A.15.1.3 Protection of organizational records	AU-9, AU-11, CP-9, MP-1, MP-4, SA-5, SI-12
A.15.1.4 Data protection and privacy of personal information	Appendix J; SI-12
A.15.1.5 Prevention of misuse of information processing facilities	AC-8, AU-6, CM-11, PL-4, PS-6, PS-8
A.15.1.6 Regulation of cryptographic controls	IA-7, SC-13
A.15.2 Compliance with security policies and standards, and technical compliance	
A.15.2.1 Compliance with security policies and standards	XX-1 controls, AC-2, CA-2, CA-7, IA-7, PE-8, SI-12
A.15.2.2 Technical compliance checking	CA-2, CA-7, RA-5
A.15.3 Information systems audit considerations	
A.15.3.1 Information systems audit controls	AU-1, AU-2
A.15.3.2 Protection of information systems audit tools	AU-9

**TABLE H-3: MAPPING ISO/IEC 15408 TO NIST SP 800-53**

ISO/IEC 15408 REQUIREMENTS		NIST SP 800-53 CONTROLS	
<i>Functional Requirements</i>			
FAU_ARP.1	<b>Security Audit Automatic Response</b> Security Alarms	AU-5	<b>Response to Audit Processing Failures</b>
		AU-5 (1)	<b>Response to Audit Processing Failures</b> <i>Audit Storage Capacity</i>
		AU-5 (2)	<b>Response to Audit Processing Failures</b> <i>Real-Time Alerts</i>
		AU-5 (3)	<b>Response to Audit Processing Failures</b> <i>Configurable Traffic Volume Thresholds</i>
		AU-5 (4)	<b>Response to Audit Processing Failures</b> <i>Shutdown on Failure</i>
		PE-6 (2)	<b>Monitoring Physical Access</b> <i>Automated Intrusion Recognition / Responses</i>
		SI-3	<b>Malicious Code Protection</b>
		SI-3 (8)	<b>Malicious Code Protection</b> <i>Detect Unauthorized Commands</i>
		SI-4 (5)	<b>Information System Monitoring</b> <i>System-Generated Alerts</i>
		SI-4 (7)	<b>Information Systems Monitoring</b> <i>Automated Response to Suspicious Events</i>
		SI-4 (22)	<b>Information Systems Monitoring</b> <i>Unauthorized Network Services</i>
		SI-7 (2)	<b>Software, Firmware, and Information Integrity</b> <i>Automated Notifications of Integrity Violations</i>
		SI-7 (5)	<b>Software, Firmware, and Information Integrity</b> <i>Automated Response to Integrity Violations</i>
		SI-7 (8)	<b>Software, Firmware, and Information Integrity</b> <i>Auditing Capability for Significant Events</i>
FAU_GEN.1	<b>Security Audit Data Generation</b> Audit Data Generation	AU-2	<b>Audit Events</b>
		AU-3	<b>Content of Audit Records</b>
		AU-3 (1)	<b>Content of Audit Records</b> <i>Additional Audit Information</i>
		AU-12	<b>Audit Generation</b>
FAU_GEN.2	<b>Security Audit Data Generation</b> User Identity Association	AU-3	<b>Content of Audit Records</b>
FAU_SAA.1	<b>Security Audit Analysis</b> Potential Violation Analysis	SI-4	<b>Information System Monitoring</b>
FAU_SAA.2	<b>Security Audit Analysis</b> Profile-Based Anomaly Detection	AC-2 (12)	<b>Account Management</b> <i>Account Monitoring / Atypical Usage</i>
		SI-4	<b>Information System Monitoring</b>
FAU_SAA.3	<b>Security Audit Analysis</b> Simple Attack Heuristics	SI-3 (7)	<b>Malicious Code Protection</b> <i>Non Signature-Based Protection</i>
		SI-4	<b>Information System Monitoring</b>
FAU_SAA.4	<b>Security Audit Analysis</b> Complex Attack Heuristics	SI-3 (7)	<b>Malicious Code Protection</b> <i>Non Signature-Based Protection</i>
		SI-4	<b>Information System Monitoring</b>