Definitions & References

Control Satisfaction Matrix

Framework Standard	Category	Controls Satisfied	800-53r4 Controls	ISO/SEC 27001	Audit Controls
NIST 800-171	None	None	None	None	None

Major Document History

Date	Comment	Who
8/12/2019	Added Template Fields and FIPS 199, Format Updates	Tharp
8/13/2019	Added NIST 800-53r4 to ISO/IEC Matrix	Tharp

Policy Page Template

Control Satisfaction Matrix

Framework Standard	Category	Controls Satisfied	800-53r4 Controls	ISO/SEC 27001	Audit Controls
NIST 800-171	Can Name	Controls Covered	NIST Sections	ISO Topics	A-lign Topics

Major Document History

Date	Comment	Who
1/1/2000	Change Notes	Change Author

Purpose and Scope====

Background====

Policies====

n.nn===

Response Plan

Plan # Name====

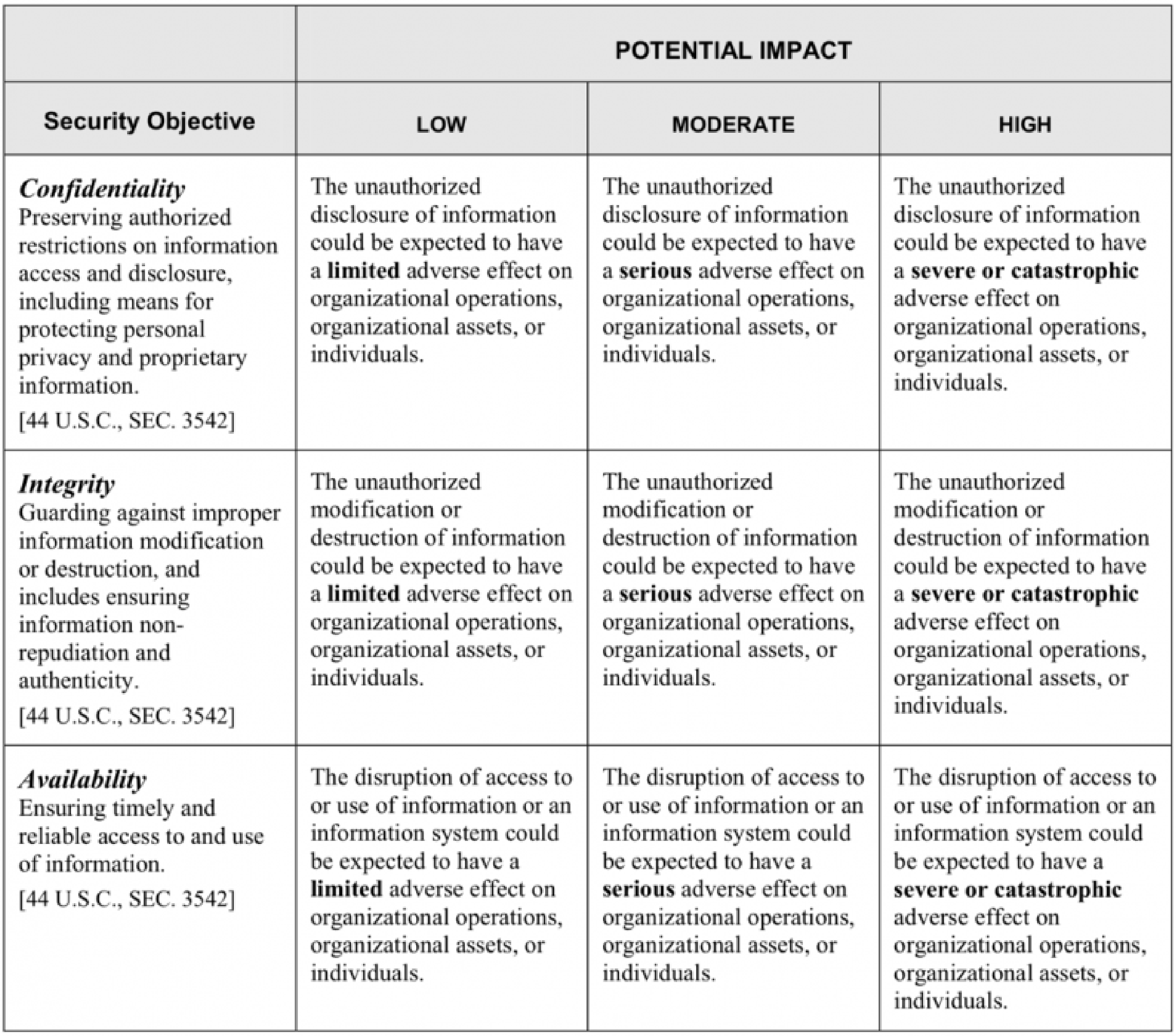
A===

B===

Term	Definition
Policy	Policies are the statements of the specific framework being referenced
Plans	Are DLZP Group's implementation documentation to achieve the corresponding policy

Definitions

FIPS 199



	POTENTIAL IMPACT		
Security Objective	**LOW**	**MODERATE**	**HIGH**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

POTENTIAL IMPACT DEFINITIONS FOR SECURITY OBJECTIVES

800-53r4 to ISO/IEC Map

NIST SP 800-53 CONTROLS	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	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 (Access) Notification	A.9.4.2
AC-10	Concurrent Session Control	None
AC-11	Session 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 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.11.2.6; A.13.2.1
AC-20	Use of External Information 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	Security Awareness and Training Policy and Procedures	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	Security Awareness Training	A.7.2.2; A.12.2.1
AT-3	Role-Based Security Training	A.7.2.2*
AT-4	Security Training Records	None
AT-5	Withdrawn	—

NIST SP 800-53 CONTROLS	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-1	Audit and Accountability Policy and Procedures	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	Audit Events	None
AU-3	Content of Audit Records	A.12.4.1*
AU-4	Audit Storage Capacity	A.12.1.3
AU-5	Response to Audit Processing Failures	None
AU-6	Audit Review; Analysis; and Reporting	A.12.4.1; A.16.1.2; A.16.1.4
AU-7	Audit Reduction and Report Generation	None
AU-8	Time Stamps	A.12.4.4
AU-9	Protection of Audit Information	A.12.4.2; A.12.4.3; A.18.1.3
AU-10	Non-repudiation	None
AU-11	Audit Record Retention	A.12.4.1; A.16.1.7
AU-12	Audit 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	Alternate Audit Capability	None
AU-16	Cross-Organizational Auditing	None
CA-1	Security Assessment and Authorization Policies and Procedures	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	Security Assessments	A.14.2.8; A.18.2.2; A.18.2.3
CA-3	System Interconnections	A.13.1.2; A.13.2.1; A.13.2.2
CA-4	Withdrawn	—
CA-5	Plan of Action and Milestones	None
CA-6	Security Authorization	None
CA-7	Continuous Monitoring	None
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.12.1.1; A.18.1.1; A.18.2.2
CM-2	Baseline Configuration	None
CM-3	Configuration Change Control	A.12.1.2; A.14.2.2; A.14.2.3; A.14.2.4
CM-4	Security Impact Analysis	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	Information 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

NIST SP 800-53 CONTROLS	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. ”
CP-1	Contingency Planning Policy and Procedures	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	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	Information System Backup	A.12.3.1; A.17.1.2; A.18.1.3
CP-10	Information 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	A.5.1.1; A.5.1.2; A.6.1.1; A.12.1.1; A.18.1.1; A.18.2.2
IA-2	Identification and Authentication (Organizational Users)	A.9.2.1
IA-3	Device Identification and Authentication	None
IA-4	Identifier Management	A.9.2.1
IA-5	Authenticator Management	A.9.2.1; A.9.2.4; A.9.3.1; A.9.4.3
IA-6	Authenticator 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
IR-1	Incident Response Policy and Procedures	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	A.16.1.1
IR-9	Information Spillage Response	None
IR-10	Integrated Information Security Analysis Team	None
MA-1	System Maintenance Policy and Procedures	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	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. ”
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
MP-1	Media Protection Policy and Procedures	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	A.5.1.1; A.5.1.2; A.6.1.1; A.12.1.1; A.18.1.1; A.18.2.2
PE-2	Physical Access Authorizations	A.11.1.2*
PE-3	Physical Access Control	A.11.1.1; A.11.1.2; A.11.1.3
PE-4	Access Control for Transmission Medium	A.11.1.2; A.11.2.3
PE-5	Access Control for Output Devices	A.11.1.2; A.11.1.3
PE-6	Monitoring Physical Access	None
PE-7	Withdrawn	—
PE-8	Visitor Access Records	None
PE-9	Power Equipment and Cabling	A.11.1.4; A.11.2.1; A.11.2.2; A.11.2.3
PE-10	Emergency Shutoff	A.11.2.2*
PE-11	Emergency Power	A.11.2.2
PE-12	Emergency Lighting	A.11.2.2*
PE-13	Fire Protection	A.11.1.4; A.11.2.1
PE-14	Temperature and Humidity 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 Information 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*
PL-1	Security Planning Policy and Procedures	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 Plan	A.14.1.1
PL-3	Withdrawn	—

NIST SP 800-53 CONTROLS	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. ”
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	Security Concept of Operations	A.14.1.1*
PL-8	Information Security Architecture	A.14.1.1*
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.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	Third-Party Personnel Security	A.6.1.1*; A.7.2.1*
PS-8	Personnel Sanctions	A.7.2.3
RA-1	Risk Assessment Policy and Procedures	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	A.12.6.1*
RA-4	Withdrawn	—
RA-5	Vulnerability Scanning	A.12.6.1*
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.12.1.1; A.18.1.1; A.18.2.2
SA-2	Allocation of Resources	None
SA-3	System Development Life Cycle	A.6.1.1; A.6.1.5; A.14.1.1; A.14.2.1; A.14.2.6
SA-4	Acquisition Process	A.14.1.1; A.14.2.7; A.14.2.9; A.15.1.2
SA-5	Information System Documentation	A.12.1.1*
SA-6	Withdrawn	—
SA-7	Withdrawn	—
SA-8	Security Engineering Principles	A.14.2.5
SA-9	External Information 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 Security Testing and Evaluation	A.14.2.7; A.14.2.8
SA-12	Supply Chain Protections	A.14.2.7; A.15.1.1; A.15.1.2; A.15.1.3
SA-13	Trustworthiness	None
SA-14	Criticality Analysis	None

NIST SP 800-53 CONTROLS	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-15	Development Process; Standards; and Tools	A.6.1.5; A.14.2.1;
SA-16	Developer-Provided Training	None
SA-17	Developer Security Architecture and Design	A.14.2.1; A.14.2.5
SA-18	Tamper Resistance and Detection	None
SA-19	Component Authenticity	None
SA-20	Customized Development of Critical Components	None
SA-21	Developer Screening	A.7.1.1
SA-22	Unsupported System Components	None
SC-1	System and Communications Protection Policy and Procedures	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	Application Partitioning	None
SC-3	Security Function Isolation	None
SC-4	Information In Shared 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	A.13.2.1*
SC-16	Transmission of Security Attributes	None
SC-17	Public Key Infrastructure Certificates	A.10.1.2
SC-18	Mobile Code	None
SC-19	Voice Over Internet Protocol	None
SC-20	Secure Name/Address Resolution Service (Authoritative Source)	None
SC-21	Secure Name/Address Resolution Service (Recursive or Caching Resolver)	None
SC-22	Architecture and Provisioning for Name/Address Resolution Service	None
SC-23	Session Authenticity	None
SC-24	Fail in Known State	None
SC-25	Thin Nodes	None
SC-26	Honeypots	None
SC-27	Platform-Independent Applications	None

NIST SP 800-53 CONTROLS	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-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	Information System Partitioning	None
SC-33	Withdrawn	—
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	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	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.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	Information System Monitoring	None
SI-5	Security Alerts; Advisories; and Directives	A.6.1.4*
SI-6	Security 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 Handling 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
PM-1	Information Security Program Plan	A.5.1.1; A.5.1.2; A.6.1.1; A.18.1.1; A.18.2.2
PM-2	Senior Information Security Officer	A.6.1.1*
PM-3	Information Security Resources	None
PM-4	Plan of Action and Milestones Process	None

NIST SP 800-53 CONTROLS	**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-5	Information System Inventory	None
PM-6	Information Security Measures of Performance	None
PM-7	Enterprise Architecture	None
PM-8	Critical Infrastructure Plan	None
PM-9	Risk Management Strategy	None
PM-10	Security Authorization Process	A.6.1.1*
PM-11	Mission/Business Process Definition	None
PM-12	Insider Threat Program	None
PM-13	Information Security Workforce	A.7.2.2*
PM-14	Testing; Training; and Monitoring	None
PM-15	Contacts with Security Groups and Associations	A.6.1.4
PM-16	Threat Awareness Program	None