Table H-2 provides a mapping from the security controls in ISO/IEC 27001 to the security controls in Special Publication 800-53. 115 Please review the introductory text at the beginning of Appendix H before employing the mappings in Table H-2.

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

ISO/IEC 27001 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.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, 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
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	

¹¹⁵ The use of the term XX-I controls in mapping Table H-2 refers to the set of security controls represented by the first control in each family in Appendix F, where XX is a placeholder for the two-letter family identifier.

and Organizations

	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.
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	
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
A.11.1.5 Working in secure areas	SC-42(3)*
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
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	

and Organizations

A12.3.1 Information backup A12.4.1 Event logging and monitoring A12.4.2 Protection of log information A12.4.3 Administrator and operator logs A12.4.3 Administrator and operator logs A12.4.3 Administrator and operator logs A12.4.4 Clock synchronization A12.5 Control of operational software A12.5.1 Installation of software on operational systems A12.6 Technical vulnerabilities A12.6.1 Management of technical vulnerabilities A12.6.1 Management of technical vulnerabilities A12.6.1 Information systems audit considerations A12.7 Information systems audit considerations A12.7.1 Information systems audit controls A13.1 Communications security A13.1 Network security management A13.1.1 Network controls A13.1.1 Network controls A13.1.2 Security of network services CA-3, SA-9 A13.1.3 Segregation in networks A13.2.1 Information transfer A13.2.1 Information transfer A13.2.2 Agreements on information transfer A13.2.3 Electronic messaging SC-8 A13.2.4 System acquisition, development and maintenance A14.1 Security requirements of information systems A14.1.1 Information security requirements analysis and specification A14.2 System change control procedures A14.2 System change control procedures A14.2 System changes to software packages A14.2 System changes to software packages A14.2.5 Secure development and support processes A14.2.6 Secure development environment A14.2.7 Outsourced development A14.2.8 System acquisition services transactions A14.3.1 Protection of test data A14.3.3 Terrocal procedure of application service packages A14.2.5 System security resting CA-2, SA-10, SA-11, SA-12, SA-15 A14.2.9 System accuptance testing A14.2.5 System security resting CA-2, SA-11 A14.3.1 Frotection of	ISO/IEC 27001 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 A 12.4.2 Protection of log information A 12.4.2 Protection of log information A 12.4.3 Administrator and operator logs A 12.4.4 Clock synchronization A 12.6.1 A 12.6.1 Control of operational software A 12.5.1 Installation of software on operational systems A 12.6.1 Installation of software on operational systems A 12.6.1 Management of technical vulnerabilities A 12.6.2 Restrictions on software installation A 12.7. Information systems audit considerations A 12.7. Information systems audit controls A 12.7. Information systems audit controls A 13.1.1 Network security A 13.1 Network security management A 13.1.1 Network controls A 13.1.2 Segregation in networks A 13.2.2 Agreements on information transfer A 13.2.1 Information transfer policies and procedures A 13.2.2 Information transfer policies and procedures A 13.2.3 Electronic messaging A 13.2.4 Contidentiality or nondisclosure agreements A 14.1.1 Information security requirements analysis and specification A 14.1.1 Protecting application services on public networks A 14.1.3 Protecting application services transactions A 14.1.3 Protecting application services transactions A 14.2.2 Security in development and maintenance A 14.2.3 Technical review of applications after operating platform changes A 14.2.5 Secure system engineering principles A 14.2.6 System change control procedures C M-3, SA-10, SA-10 A 14.2.8 System changes control procedures A 14.2.8 Ceuter development and support processes A 14.2.9 Technical review of applications after operating platform changes A 14.2.6 Secure development environment A 14.2.6 System changes control procedures A 14.2.7 Outsourced development A 14.2.8 System security testing A 14.2.8 System security testing A 14.2.9 System security testing A 14.2.8 System security testing A 14.2.9 Technical review of applications after operating A 14.2.8 System security testing A 14.2.9 System security testing A 14.2.9 System security testing A 14.3.1 Protection of test data A 14.2.8 System se	A.12.3 Backup	
A.12.4.1 Event logging A.12.4.2 Protection of log information A.12.4.3 Protection of log information A.12.4.3 Administrator and operator logs A.12.4.4 Clock synchronization A.12.5.1 Installation of software on operational systems A.12.5.1 Installation of software on operational systems A.12.6.2 Restrictions on software installation A.12.6.1 Management of technical vulnerabilities A.12.6.2 Restrictions on software installation A.12.7 Information systems audit considerations A.12.6.1 Management of technical vulnerabilities A.12.6.2 Restrictions on software installation A.12.7.1 Information systems audit considerations A.12.7.1 Information systems audit considerations A.12.7.1 Information systems audit considerations A.13.1.1 Network security A.13.1.1 Network security A.13.1.1 Network security management A.13.1.1 Information systems A.13.1.1 Information transfer A.13.2.1 Information transfer policies and procedures A.13.2.1 Information transfer policies and procedures A.13.2.2 Agreements on information transfer A.13.2.2 Agreements on information transfer A.13.2.2 Agreements on information transfer A.13.2.4 System acquisition, development and maintenance A.14.1 System acquisition, development and maintenance A.14.1.2 Security requirements of information systems A.14.1.3 Protecting application services on public networks A.14.1.3 Protecting application services on public networks A.14.2.2 System change control procedures C.M.3, SA-15, SA-17 A.14.2.2 System change control procedures C.M.3, SA-10, SA-10, SA-11, SA-12, SA-15 A.14.2.5 Secure system engineering principles A.14.2.6 Secure development and support A.14.2.6 Secure system engineering principles A.14.2.7 Outsourced development A.14.3.1 Terotection of test data A.15.1.1 Information security is supplier relationships A.15.1.1 Information security policy for supplier A.15.1.1 Information security policy for supplier		CP-9
A 12.4.2 Protection of log information A 12.4.3 Administrator and operator logs A 12.4.4 Clock synchronization A 12.6 Control of operational software A 12.5.1 installation of software on operational systems A 12.5.1 installation of software on operational systems A 12.6.1 Management of sechnical vulnerabilities A 12.6.2 Restrictions on software installation A 12.7 Information systems audit considerations A 12.7.1 Information systems audit considerations A 12.7.1 Information systems audit controls A 13.1 Network security A 13.1 Network security A 13.1.1 Network security management A 13.1.1 Network services A 13.2 Security of network services A 13.2.3 Information instere A 13.2.1 Information systems A 13.2.2 Agreements on information transfer A 13.2.2 Agreements on information transfer A 13.2.4 Confidentiality or nondisclosure agreements A 14.1 Security requirements of information systems A 14.1.1 Information security requirements analysis and specification A 14.1.2 Security in development and maintenance A 14.1.3 Security requirements on information systems A 14.1.4 Security requirements an origination services on public networks A 14.1.1 Poscurity requirements analysis and specification A 14.1.2 Security in development and support processes A 14.2.3 Security in development policy A 14.2.3 Control of the services on public networks A 14.2.3 Security in development and support processes A 14.2.4 Restrictions on changes to software packages A 14.2.5 Secure development environment A 14.2.6 Secure development environment A 14.2.		
A12.4.3 Administrator and operator logs A12.4.4 Clock synchronization A12.5 Control of operational software A12.5.1 Installation of software on operational systems A12.6.1 Installation of software on operational systems A12.6.1 Installation of software on operational systems A12.6.1 Management of technical vulnerabilities A12.6.2 Restrictions on software installation A12.7 Information systems audit considerations A12.7.1 Information systems audit considerations A12.7.1 Information systems audit considerations A13.1 Network security management A13.1.1 Network security management A13.1.1 Network controls A13.1.2 Security of network services A13.2.1 Information transfer A13.2.2 Information transfer A13.2.3 Information transfer A13.2.4 Information transfer policies and procedures A13.2.5 AC-4, AC-17, AC-18, AC-20, CA-3, PE-17, SC-7, SC-8, SC-10 A13.2.2 Agreements on information transfer A13.2.3 Electronic messaging A13.2.4 Security or nondisclosure agreements A14.3 System acquisition, development and maintenance A14.1 Security requirements of information systems A14.1.1 Information security requirements analysis and specification A14.1.2 Securing application services on public networks A14.2.3 System change control procedures A14.2.3 Technical review of applications after operating platform changes A14.2.4 Restrictions on changes to software packages A14.2.5 Secure development environment A14.2.6 Secure development environment A14.2.7 Outsourced development A14.2.8 System security testing A14.2.9 System security testing A14.3.1 Technical research and security in supplier relationships A15.1.1 Information security in supplier relationships A15.1.1 Information security in supplier relationships A15.1.1 Information security policy for supplier		
A 12.4 4 Clock synchronization A 12.5 Control of operational software A 12.5.1 Installation of software on operational systems A 12.6.1 Management of technical vulnerabilities A 12.6.1 Management of technical vulnerabilities A 12.6.2 Restrictions on software installation A 12.7 Information systems audit considerations A 12.7.1 Information systems audit considerations A 12.7.1 Information systems audit controls A 13.1 Operation of the security of the security A 13.1 Network security management A 13.1.1 Network security management A 13.1.2 Security of network services C 2.3, 3.4.3 Sergegation in networks A 2.4, 3.6.4, 3		
A 12.5 Control of operational software A 12.5.1 Installation of software on operational systems A 12.6. Technical vulnerability management A 12.6.1 Management of technical vulnerabilities A 12.6.2 Restrictions on software installation A 12.7 Information systems audit controls A 12.7.1 Information systems audit controls A 12.7.1 Information systems audit controls A 13.1 Network security A 13.1 Network security A 13.1.1 Network security management A 13.1.1 Network security management A 13.1.2 Security of network services A 13.2.1 Information transfer A 13.2.2 Agreements on information transfer A 13.2.3 Electronic messaging A 13.2.4 Segments on information transfer A 14.3.2 Security requirements of information systems A 14.1.1 Information security requirements analysis and specification A 14.1.2 Security in development and support processes A 14.2.2 Security in development policy A 14.2.2 Security in development and support processes A 14.2.3 Secure development policy A 14.2.4 Secure development policy A 14.2.5 Secure development engineering principles A 14.2.6 Secure development engineering principles A 14.2.7 Secure development engineering principles A 14.2.8 System security testing A 14.2.9 System engineering principles A 14.2.1 Secure development engineering principles A 14.2.2 System security testing A 14.2.3 Secure development of the security of the security in development A 14.2.4 Secure development policy A 14.2.5 Secure development policy A 14.2.6 Secure development engineering principles A 14.2.7 Secure development engineering principles A 14.2.8 System security testing A 14.2.9 System security testing A 14.2.9 System security testing A 14.3.1 Information security policy for supplier elationships A 15.1.1 Information security in supplier relationships A 15.1.1 Information security in supplier relationships A 15.1.1 Information security in supplier elationships A 15.1.1 Information security policy for supplier	·	AU-9, AU-12
A.12.5.1 Installation of software on operational systems A.12.6.1 Management of technical vulnerability management A.12.6.2 Restrictions on software installation A.12.6.2 Restrictions on software installation A.12.7.1 Information systems audit considerations A.12.7.1 Information systems audit controls A.12.7.1 Information security A.13.1 Network security management A.13.1.1 Network security management A.13.1.1 Network security management A.13.1.3 Segregation in networks A.13.1.3 Segregation in networks A.13.2 Information transfer A.13.2 Information transfer A.13.2.1 Information transfer policies and procedures A.13.2.2 Agreements on information transfer A.13.2.3 Electronic messaging A.14.3 Electronic messaging A.14.4 System acquisition, development and maintenance A.14.1 Security requirements of information systems A.14.1.1 Information services on public networks A.14.1.2 Security in development and support processes A.14.2.2 System change control procedures A.14.2.3 Electronical review of application services transactions A.14.2 Security in development and support processes A.14.2.3 Secure development policy A.14.2.3 Secure development policy A.14.2.4 Restrictions on changes to software packages A.14.2.5 Secure system engineering principles A.14.2.6 Secure development environment A.14.2.7 Secure development environment A.14.2.8 System security testing A.14.2.9 System security testing A.14.2.9 System security testing A.14.2.1 Security results and specification A.14.2.2 System change control procedures A.14.2.3 Secure development environment A.14.2.3 System security testing A.14.2.4 Restrictions on changes to software packages A.14.2.5 Secure development environment A.14.2.6 Secure development environment A.14.2.7 System acceptance testing A.14.2.8 System security testing A.14.2.9 System security testing A.14.2.1 Information security pilocy for supplier A.15.1 Information security in supplier relationships A.15.1.1 Information security pilocy for supplier		AU-8
A 12.6 Technical vulnerability management A 12.6.1 Management of technical vulnerabilities A 12.6.2 Restrictions on software installation A 12.7.1 Information systems audit controls A 12.7.1 Information systems audit controls A 13.1 Network security A 13.1 Network security management A 13.1.1 Network controls A 13.1.2 Security of network services A 13.1.3 Segregation in networks A 13.2.3 Information transfer A 13.2.1 Information transfer policies and procedures A 13.2.2 Agreements on information transfer A 13.2.3 Electronic messaging A 13.2.4 System acquisition, development and maintenance A 14.1 Security requirements of information systems A 14.1.1 Information security requirements analysis and specification A 14.1.2 Securing application services transactions A 14.2.1 Security in development and support processes A 14.2.2 System acquisition, development and support processes A 14.2.3 Technical review of applications after operating platform changes A 14.2.3 Technical review of applications after operating platform changes A 14.2.5 Secure development enting principles A 14.2.5 Secure system engineering principles A 14.2.5 System security testing A 14.2.5 System security testing A 14.2.5 System acceptance testing A 14.2.5 System acceptance testing A 14.2.5 System security testing A 14.2.5 System security testing A 14.2.6 Secure development and support B 14.2.7 System changes control procedures A 14.2.8 System security testing A 14.2.9 System acceptance testing A 14.2.9 System acceptance testing A 14.3.1 Information security in supplier relationships A 15.1.1 Information security in supplier relationships A 15.1.1 Information security in supplier relationships A 15.1.1 Information security policy for supplier		
A.12.6.1 Management of technical vulnerabilities A.12.6.2 Festrictions on software installation A.12.7 Information systems audit controls A.12.7.1 Information systems audit controls A.13.1.1 Network security A.13.1.1 Network security A.13.1.1 Network security A.13.1.1 Network security of network services A.13.1.2 Security of network services A.13.1.3 Segregation in networks A.13.2 Information transfer A.13.2.1 Information transfer policies and procedures A.13.2.2 Agreements on information transfer A.13.2.2 Agreements on information transfer A.13.2.3 Electronic messaging A.14.3 Security requirements of information systems A.14.1.1 Information security requirements analysis and specification A.14.1.2 Security prequirements on public networks A.14.1.3 Protecting application services on public networks A.14.2.3 Technical review of applications after operating platform changes A.14.2.3 Technical review of applications after operating platform changes A.14.2.4 Restrictions on changes to software packages A.14.2.5 Secure system engineering principles A.14.2.6 Secure development environment A.14.2.7 Unisourced development A.14.2.8 System acceptance testing A.14.2.8 System security testing A.14.2.9 System acceptance testing A.14.2.9 System acceptance testing A.14.3.1 Protection of test data A.14.3.1 Information security in supplier relationships A.15.1.1 Information security policy for supplier		CM-5, CM-7(4), CM-7(5), CM-11
A.12.6.2 Restrictions on software installation A.12.7 Information systems audit considerations A.12.7.1 Information systems audit controls A.13.1 Network security A.13.1 Network security management A.13.1.1 Network security management A.13.1.2 Security of network services CA-3, SA-9 A.13.1.2 Security of network services A.13.2 Information transfer A.13.2.1 Information transfer A.13.2.2 Agreements on information transfer A.13.2.2 Agreements on information transfer A.13.2.3 Electronic messaging A.13.2.4 Confidentiality or nondisclosure agreements A.14.3 System acquisition, development and maintenance A.14.1 Security requirements of information systems A.14.1.1 Information security requirements analysis and specification A.14.1.2 Security application services transactions A.14.2.3 Tectrolic application services transactions A.14.2.3 Technical review of applications after operating platform changes A.14.2.5 Secure development ending principles A.14.2.6 Secure development ending principles A.14.2.8 System security restrictions A.14.2.8 System security restring A.14.2.8 System security restring A.14.2.8 System security restring A.14.2.9 System security restring A.14.2.9 System security restring A.14.3.1 Frotection of test data A.14.3.1 Frotection of test data A.14.3.1 Information security in supplier relationships A.15.1.1 Information security policy for supplier	A.12.6 Technical vulnerability management	
A.12.7 Information systems audit considerations A.12.7.1 Information systems audit controls A.13. Communications security A.13.1 Network security management A.13.1.1 Network controls A.13.1.2 Security of network services A.13.2 Information transfer A.13.2 Information transfer policies and procedures A.13.2.1 Information transfer policies and procedures A.13.2.2 Agreements on information transfer A.13.2.3 Electronic messaging A.13.2.4 Confidentiality or nondisclosure agreements A.14.1.2 Security requirements of information systems A.14.1.1 Information security requirements analysis and specification A.14.1.2 Securing application services transactions A.14.2.3 Technical review of applications after operating platform changes A.14.2.4 Restrictions on changes to software packages A.14.2.5 Secure system engineering principles A.14.2.6 Secure development A.14.2.7 System security testing A.14.2.8 System security testing A.14.2.9 System security testing A.14.2.9 System security testing A.14.3.1 Protection of test data A.15.1 Information security in policy for supplier insciples A.15.1.1 Information security in policy for supplier SA-12.1 Information security in policy for supplier insciples A.15.1.1 Information security in policy for supplier SA-12.1 Information security in policy for supplier insciples A.15.1.1 Information security policy for supplier	A.12.6.1 Management of technical vulnerabilities	RA-3, RA-5, SI-2, SI-5
A.12.7.1 Information systems audit controls A.13 Communications security A.13.1. Network security management A.13.1.1 Network controls A.13.1.2 Security of network services A.13.1.3 Segregation in networks A.13.1.3 Segregation in networks A.13.2.1 Information transfer A.13.2.1 Information transfer policies and procedures A.13.2.2 Agreements on information transfer A.13.2.3 Electronic messaging A.13.2.4 Confidentiality or nondisclosure agreements A.14.3 System acquisition, development and maintenance A.14.1.1 Information security requirements analysis and specification A.14.1.2 Securing application services on public networks A.14.1.3 Protecting application services transactions A.14.2.1 Security in development and support processes A.14.2.2 System change control procedures A.14.2.3 Technical review of applications after operating platform changes A.14.2.4 Restrictions on changes to software packages A.14.2.5 Secure system engineering principles A.14.2.6 Secure development environment A.14.2.7 Outsourced development A.14.2.8 System acquisition A.14.2.9 System acquisition supplier relationships A.15.1.1 Information security regire acquirements and procedures A.14.2.1 Security in development A.14.2.2 System change control procedures A.14.2.3 Technical review of applications after operating principles A.14.2.4 Restrictions on changes to software packages A.14.2.5 Secure system engineering principles A.14.2.6 Secure development environment A.14.2.7 Outsourced development A.14.2.8 System security testing A.14.2.9 System acceptance testing A.14.3.1 Protection of test data A.15.1.1 Information security policy for supplier SA-15.1.1 Information security policy for supplier A.15.1.1 Information security policy for supplier	A.12.6.2 Restrictions on software installation	CM-11
A.13. Network security management A.13.1.1 Network scurity management A.13.1.2 Security of network services A.13.1.3 Segregation in networks A.13.1.3 Segregation in networks A.13.1.3 Information transfer A.13.2.1 Information transfer A.13.2.2 Agreements on information transfer A.13.2.3 Electronic messaging A.13.2.4 Confidentiality or nondisclosure agreements A.14.1 Security requirements of information systems A.14.1.1 Information security requirements analysis and specification A.14.1.2 Securing application services on public networks A.14.1.3 Protecting application services transactions A.14.2 Security in development and support processes A.14.2.1 Secure development policy A.14.2.2 System change control procedures A.14.2.3 Technical review of applications after operating platform changes A.14.2.4 Restrictions on changes to software packages A.14.2.5 Secure system engineering principles A.14.2.6 Secure development environment A.14.2.8 System acceptance testing A.14.2.9 System acceptance testing A.14.2.9 System acceptance testing A.14.2.9 System acceptance testing A.14.3.1 Protection of test data A.15.1.1 Information security policy for supplier SA-12.1 Information security in policy for supplier SA-12.1 Information security in supplier relationships A.15.1.1 Information security in supplier relationships A.15.1.1 Information security in supplier relationships	A.12.7 Information systems audit considerations	
A.13.1 Network security management A.13.1.1 Network controls A.13.1.2 Security of network services A.13.1.3 Segregation in networks A.13.1.3 Segregation in networks A.13.2 Information transfer A.13.2.1 Information transfer A.13.2.2 Information transfer A.13.2.2 Agreements on information transfer A.13.2.3 Electronic messaging A.13.2.4 Confidentiality or nondisclosure agreements A.14.3.2.4 Confidentiality or nondisclosure agreements A.14.1 Security requirements of information systems A.14.1.1 Information security requirements analysis and specification A.14.1.2 Securing application services on public networks A.14.1.3 Protecting application services transactions A.14.2.1 Security in development and support processes A.14.2.2 System change control procedures A.14.2.3 Technical review of applications after operating platform changes A.14.2.4 Restrictions on changes to software packages A.14.2.5 Secure system engineering principles A.14.2.6 Secure development environment A.14.2.7 Outsourced development A.14.3 Protection of test data A.14.3.1 Protection of test data A.14.3.1 Protection of test data A.14.3.1 Information security neutring supplier relationships A.15.1.1 Information security policy for supplier SA-12.1 Information security policy for supplier SA-12.1 Information security policy for supplier	A.12.7.1 Information systems audit controls	AU-5*
A.13.1.1 Network controls A.13.1.2 Security of network services A.13.1.3 Segregation in networks A.13.1.3 Segregation in networks A.13.2 Information transfer A.13.2.1 Information transfer A.13.2.1 Information transfer policies and procedures A.13.2.2 Agreements on information transfer A.13.2.2 Agreements on information transfer A.13.2.4 Confidentiality or nondisclosure agreements A.13.2.5 Electronic messaging S.C-8 A.13.2.6 Confidentiality or nondisclosure agreements A.14.1 System acquisition, development and maintenance A.14.1 Security requirements of information systems A.14.1.1 Information security requirements analysis and specification A.14.1.2 Securing application services on public networks A.14.1.3 Protecting application services transactions A.14.2.1 Security in development and support processes A.14.2.2 System change control procedures A.14.2.3 Technical review of applications after operating platform changes A.14.2.5 Secure development environment A.14.2.6 Secure development environment SA-3 A.14.2.7 Outsourced development A.14.2.8 System security testing A.14.2.9 System security testing A.14.2.1 Technical review of applications after operating platform changes A.14.2.2 Secure development environment SA-3 A.14.2.3 Test data A.14.2.1 Trotection of test data A.14.3.1 Protection of test data A.14.3.1 Protection of test data A.15.1.1 Information security policy for supplier SA-12	A.13 Communications security	
A.13.1.2 Security of network services A.13.1.3 Segregation in networks A.13.1.3 Information transfer A.13.2.1 Information transfer policies and procedures A.13.2.1 Information transfer policies and procedures A.13.2.2 Agreements on information transfer A.13.2.3 Electronic messaging A.13.2.4 Confidentiality or nondisclosure agreements A.14.2.5 Confidentiality or nondisclosure agreements A.14.1 Security requirements of information systems A.14.1.1 Information security requirements analysis and specification A.14.1.2 Security application services on public networks A.14.1.3 Protecting application services transactions A.14.2.1 Secure development and support processes A.14.2.2 System change control procedures A.14.2.3 Technical review of applications after operating platform changes A.14.2.4 Restrictions on changes to software packages A.14.2.5 Secure development environment A.14.2.6 Secure development A.14.2.7 Outsourced development A.14.2.8 System security testing A.14.2.9 System acceptance testing A.14.3 Test data A.14.3 Terotection of test data A.15.1.1 Information security in supplier relationships A.15.1.1 Information security policy for supplier A.15.1.1 Information security policies of AC-2, SA-12 A.15.1.1 Information security policy for supplier A.15.1.1 Information security policies of AC-2, SA-12 A.15.1.1 Information security policy for supplier	A.13.1 Network security management	
A.13.1.3 Segregation in networks A.13.2 Information transfer A.13.2.1 Information transfer policies and procedures A.13.2.2 Agreements on information transfer A.13.2.3 Electronic messaging A.13.2.4 Confidentiality or nondisclosure agreements A.14.1.1 Information security requirements of information systems A.14.1.1 Information security requirements analysis and specification A.14.1.2 Securing application services on public networks A.14.1.3 Protecting application services transactions A.14.1.1 Security in development and support processes A.14.2.1 Security in development and support processes A.14.2.2 System change control procedures A.14.2.3 Technical review of applications after operating platform changes A.14.2.4 Restrictions on changes to software packages A.14.2.5 Secure system engineering principles A.14.2.6 Secure development A.14.2.7 Outsourced development A.14.2.8 System security testing A.14.2.9 System acceptance testing A.14.3 Test data A.15.1.1 Information security solicy for supplier SA-15.1.1 Information security policy for supplier SA-12	A.13.1.1 Network controls	AC-3, AC-17, AC-18, AC-20, SC-7, SC-8, SC-10
A.13.2 Information transfer A.13.2.1 Information transfer policies and procedures A.13.2.2 Agreements on information transfer A.13.2.3 Electronic messaging A.13.2.4 Confidentiality or nondisclosure agreements A.14.1 System acquisition, development and maintenance A.14.1.1 Information security requirements analysis and specification A.14.1.2 Security requirements of information systems A.14.1.3 Protecting application services on public networks A.14.1.3 Protecting application services transactions A.14.1.4 Security in development and support processes A.14.2.1 Secure development policy A.14.2.2 System change control procedures A.14.2.3 Technical review of applications after operating platform changes A.14.2.4 Restrictions on changes to software packages A.14.2.5 Secure system engineering principles A.14.2.6 Secure development A.14.2.7 Outsourced development A.14.2.8 System security testing A.14.2.9 System acceptance testing A.14.3 Test data A.14.3 Protection of test data A.14.3 Information security in supplier relationships A.15.1.1 Information security policy for supplier SA-15.1.1 Information security policy for supplier	A.13.1.2 Security of network services	CA-3, SA-9
A.13.2.1 Information transfer policies and procedures A.3.2.2 Agreements on information transfer A.13.2.3 Electronic messaging A.13.2.4 Confidentiality or nondisclosure agreements A.14.2 System acquisition, development and maintenance A.14.1.1 Information security requirements of information systems A.14.1.2 Security requirements of information systems A.14.1.3 Protecting application services on public networks A.14.1.3 Protecting application services transactions A.14.2.1 Security in development and support processes A.14.2.2 System change control procedures A.14.2.3 Technical review of applications after operating platform changes A.14.2.4 Restrictions on changes to software packages A.14.2.5 Secure development environment A.14.2.6 Secure development A.14.2.7 Outsourced development A.14.2.9 System acceptance testing A.14.2.9 System acceptance testing A.14.3 Test data A.14.3 Trotection of test data A.15.1.1 Information security policy for supplier A.15.1.1 Information security policy for supplier SA-312	A.13.1.3 Segregation in networks	AC-4, SC-7
SC-8, SC-15 A.13.2.2 Agreements on information transfer A.13.2.3 Electronic messaging A.13.2.4 Confidentiality or nondisclosure agreements 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 A.14.1.2 Securing application services on public networks A.14.1.3 Protecting application services transactions A.14.1.3 Protecting application services transactions A.14.2 Security in development and support processes A.14.2.1 Secure development policy A.14.2.2 System change control procedures A.14.2.3 Technical review of applications after operating platform changes A.14.2.4 Restrictions on changes to software packages A.14.2.5 Secure system engineering principles A.14.2.6 Secure development A.14.2.7 Outsourced development A.14.2.8 System security testing A.14.2.9 System acceptance testing A.14.3 Test data A.14.3.1 Protection of test data A.15.1.1 Information security policy for supplier SA-12	A.13.2 Information transfer	
A.13.2.3 Electronic messaging A.13.2.4 Confidentiality or nondisclosure agreements 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 A.14.1.2 Securing application services on public networks A.14.1.3 Protecting application services transactions A.14.1.3 Protecting application services transactions A.14.2 Security in development and support processes A.14.2.1 Secure development policy A.14.2.2 System change control procedures A.14.2.3 Technical review of applications after operating platform changes A.14.2.4 Restrictions on changes to software packages A.14.2.5 Secure system engineering principles A.14.2.6 Secure development A.14.2.7 Outsourced development S.A-3, S.A-10, S.A-10, S.A-11, S.A-12, S.A-15 A.14.2.8 System acceptance testing A.14.2.9 System acceptance testing A.14.3 Test data A.14.3 Test data A.15.1.1 Information security in supplier relationships A.15.1.1 Information security policy for supplier	A.13.2.1 Information transfer policies and procedures	
A.13.2.4 Confidentiality or nondisclosure agreements 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 A.14.1.2 Securing application services on public networks A.14.1.3 Protecting application services transactions A.14.1.3 Protecting application services transactions A.14.2 Security in development and support processes A.14.2.1 Secure development policy A.14.2.2 System change control procedures A.14.2.3 Technical review of applications after operating platform changes A.14.2.4 Restrictions on changes to software packages A.14.2.5 Secure system engineering principles A.14.2.6 Secure development A.14.2.7 Outsourced development A.14.2.8 System security testing A.14.2.9 System acceptance testing A.14.2.9 System acceptance testing A.14.3 Test data A.14.3 Test data A.15.1.1 Information security in supplier relationships A.15.1.1 Information security policy for supplier SA-12	A.13.2.2 Agreements on information transfer	CA-3, PS-6, SA-9
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 A.14.1.2 Securing application services on public networks A.14.1.3 Protecting application services transactions A.14.1.3 Protecting application services transactions A.14.2 Security in development and support processes A.14.2.1 Secure development policy A.14.2.2 System change control procedures A.14.2.3 Technical review of applications after operating platform changes A.14.2.4 Restrictions on changes to software packages A.14.2.5 Secure system engineering principles A.14.2.6 Secure development A.14.2.7 Outsourced development A.14.2.8 System security testing A.14.2.9 System acceptance testing A.14.3 Test data A.14.3.1 Protection of test data A.15 Supplier Relationships A.15.1.1 Information security policy for supplier SA-12	A.13.2.3 Electronic messaging	SC-8
A.14.1 Security requirements of information systems A.14.1.1 Information security requirements analysis and specification A.14.1.2 Securing application services on public networks A.14.1.3 Protecting application services transactions A.14.2 Security in development and support processes A.14.2 Security in development and support processes A.14.2.1 Secure development policy A.14.2.2 System change control procedures A.14.2.3 Technical review of applications after operating platform changes A.14.2.4 Restrictions on changes to software packages A.14.2.5 Secure system engineering principles A.14.2.6 Secure development A.14.2.7 Outsourced development SA-3 A.14.2.8 System security testing A.14.2.9 System acceptance testing A.14.2.9 System acceptance testing A.14.3.1 Protection of test data A.14.3.1 Information security in supplier relationships A.15.1.1 Information security policy for supplier	A.13.2.4 Confidentiality or nondisclosure agreements	PS-6
A.14.1.1 Information security requirements analysis and specification A.14.1.2 Securing application services on public networks A.14.1.3 Protecting application services transactions A.14.2 Security in development and support processes A.14.2.1 Secure development policy A.14.2.2 System change control procedures A.14.2.3 Technical review of applications after operating platform changes A.14.2.4 Restrictions on changes to software packages A.14.2.5 Secure system engineering principles A.14.2.6 Secure development A.14.2.7 Outsourced development A.14.2.8 System security testing A.14.2.9 System acceptance testing A.14.3.1 Protection of test data A.14.3.1 Protection of test data A.15 Supplier Relationships A.15.1.1 Information security policy for supplier		
specification A.14.1.2 Securing application services on public networks A.14.1.3 Protecting application services transactions A.14.2 Security in development and support processes A.14.2.1 Secure development policy A.14.2.2 System change control procedures A.14.2.3 Technical review of applications after operating platform changes A.14.2.4 Restrictions on changes to software packages A.14.2.5 Secure system engineering principles A.14.2.6 Secure development A.14.2.7 Outsourced development A.14.2.8 System security testing A.14.2.9 System acceptance testing A.14.3 Test data A.14.3.1 Protection of test data A.15 Supplier Relationships A.15.1.1 Information security policy for supplier A.14.1 Security in Acceptance testing services on public networks A.14.2 Security application services transactions A.14.3.1 Acceptance testing A.14.3.1 Information security in supplier relationships A.15.1.1 Information security policy for supplier	A.14.1 Security requirements of information systems	
A.14.1.3 Protecting application services transactions A.14.2 Security in development and support processes A.14.2.1 Secure development policy A.14.2.2 System change control procedures A.14.2.3 Technical review of applications after operating platform changes A.14.2.4 Restrictions on changes to software packages A.14.2.5 Secure system engineering principles A.14.2.6 Secure development environment A.14.2.7 Outsourced development A.14.2.8 System security testing A.14.2.9 System acceptance testing A.14.3.1 Protection of test data A.14.3.1 Protection of test data A.15 Supplier Relationships A.15.1.1 Information security policy for supplier A.15.1.1 Information security policy for supplier		PL-2, PL-7, PL-8, SA-3, SA-4
A.14.2 Security in development and support processes A.14.2.1 Secure development policy A.14.2.2 System change control procedures A.14.2.3 Technical review of applications after operating platform changes A.14.2.4 Restrictions on changes to software packages A.14.2.5 Secure system engineering principles A.14.2.6 Secure development environment A.14.2.7 Outsourced development A.14.2.8 System security testing A.14.2.9 System acceptance testing A.14.3.1 Protection of test data A.14.3.1 Protection of test data A.15 Supplier Relationships A.15.1 Information security policy for supplier SA-32 SA-34 SA-15, SA-10 CM-3, CM-4, SI-2 CM-3, CM-4, S	A.14.1.2 Securing application services on public networks	AC-3, AC-4, AC-17, SC-8, SC-13
A.14.2.1 Secure development policy A.14.2.2 System change control procedures A.14.2.3 Technical review of applications after operating platform changes A.14.2.4 Restrictions on changes to software packages A.14.2.5 Secure system engineering principles A.14.2.6 Secure development environment A.14.2.7 Outsourced development A.14.2.8 System security testing A.14.2.9 System acceptance testing A.14.3.1 Protection of test data A.14.3.1 Protection of test data A.15 Supplier Relationships A.15.1 Information security policy for supplier SA-3, SA-15, SA-17 CM-3, CM-4, SI-2 SA-8 A.14.2.6 Secure development SA-4, SA-10 SA-4, SA-10 SA-11, SA-12, SA-15 A.14.2.9 System security testing SA-4, SA-10, SA-11, SA-12, SA-15 A.15 Supplier Relationships A.15.1 Information security in supplier relationships A.15.1.1 Information security policy for supplier	A.14.1.3 Protecting application services transactions	AC-3, AC-4, SC-7, SC-8, SC-13
A.14.2.1 Secure development policy A.14.2.2 System change control procedures A.14.2.3 Technical review of applications after operating platform changes A.14.2.4 Restrictions on changes to software packages A.14.2.5 Secure system engineering principles A.14.2.6 Secure development environment A.14.2.7 Outsourced development A.14.2.8 System security testing A.14.2.9 System acceptance testing A.14.3 Test data A.14.3 Test data A.14.3 Protection of test data A.15 Supplier Relationships A.15.1 Information security policy for supplier SA-3.12 SA-3.15, SA-17 CM-3, SA-10, SI-2 CM-3, SA-10 SA-8 SA-10 SA-4, SA-10 SA-4, SA-10, SA-11, SA-12, SA-15 SA-4, SA-11, SA-12, SA-15 SA-4, SA-12(7) A.14.2.9 System acceptance testing SA-4, SA-12(7) SA-15 Supplier Relationships A.15.1 Information security in supplier relationships A.15.1.1 Information security policy for supplier		
A.14.2.2 System change control procedures A.14.2.3 Technical review of applications after operating platform changes A.14.2.4 Restrictions on changes to software packages A.14.2.5 Secure system engineering principles A.14.2.6 Secure development environment A.14.2.7 Outsourced development A.14.2.8 System security testing A.14.2.9 System acceptance testing A.14.3 Test data A.14.3.1 Protection of test data A.15 Supplier Relationships A.15.1 Information security policy for supplier A.15.1.1 Information security policy for supplier	·	SA-3 SA-15 SA-17
A.14.2.3 Technical review of applications after operating platform changes A.14.2.4 Restrictions on changes to software packages A.14.2.5 Secure system engineering principles A.14.2.6 Secure development environment A.14.2.7 Outsourced development A.14.2.8 System security testing A.14.2.9 System acceptance testing A.14.3 Test data A.14.3.1 Protection of test data A.15 Supplier Relationships A.15.1 Information security policy for supplier A.15.1.1 Information security policy for supplier CM-3, CM-4, SI-2 SA-10 SA-4 SA-10, SA-11, SA-12, SA-15 CA-2, SA-11 SA-4, SA-12(7) A.14.3 Test data A.15.1 Information security in supplier relationships A.15.1.1 Information security policy for supplier		
A.14.2.4 Restrictions on changes to software packages A.14.2.5 Secure system engineering principles A.14.2.6 Secure development environment A.14.2.7 Outsourced development A.14.2.8 System security testing A.14.2.9 System acceptance testing A.14.3 Test data A.14.3.1 Protection of test data A.15 Supplier Relationships A.15.1 Information security policy for supplier A.15.1.1 Information security policy for supplier CM-3, SA-10 SA-8 SA-9 SA-10, SA-11, SA-12, SA-15 CA-2, SA-11 SA-4, SA-12(7) SA-15 SA-15 (9)* SA-15 Supplier Relationships A.15.1 Information security in supplier relationships A.15.1.1 Information security policy for supplier	A.14.2.3 Technical review of applications after operating	
A.14.2.5 Secure system engineering principles A.14.2.6 Secure development environment A.14.2.7 Outsourced development A.14.2.8 System security testing A.14.2.9 System acceptance testing A.14.3 Test data A.14.3.1 Protection of test data A.15 Supplier Relationships A.15.1 Information security in supplier relationships A.15.1.1 Information security policy for supplier SA-8 SA-8 SA-8 SA-9 SA-10, SA-11, SA-12, SA-15 SA-11 SA-4, SA-12(7) SA-4, SA-12(7) SA-15 Supplier Relationships A.15.1 Information security in supplier relationships A.15.1.1 Information security policy for supplier	•	CM 2 CA 10
A.14.2.6 Secure development environment A.14.2.7 Outsourced development A.14.2.8 System security testing A.14.2.9 System acceptance testing A.14.3 Test data A.14.3.1 Protection of test data A.15 Supplier Relationships A.15.1 Information security in supplier relationships A.15.1.1 Information security policy for supplier SA-3* SA-4, SA-10, SA-11, SA-12, SA-15 CA-2, SA-11 SA-4, SA-12(7) SA-15 SA-12(7) SA-15 Supplier Relationships A.15.1 Information security in supplier relationships SA-12		·
A.14.2.7 Outsourced development A.14.2.8 System security testing CA-2, SA-11 A.14.2.9 System acceptance testing A.14.3 Test data A.14.3.1 Protection of test data A.15 Supplier Relationships A.15.1 Information security in supplier relationships A.15.1.1 Information security policy for supplier SA-4, SA-12, SA-11 SA-4, SA-12(7) SA-15(9)*		
A.14.2.8 System security testing A.14.2.9 System acceptance testing A.14.3 Test data A.14.3.1 Protection of test data A.15 Supplier Relationships A.15.1 Information security in supplier relationships A.15.1.1 Information security policy for supplier SA-12		
A.14.2.9 System acceptance testing A.14.3 Test data A.14.3.1 Protection of test data A.15 Supplier Relationships A.15.1 Information security in supplier relationships A.15.1.1 Information security policy for supplier SA-12	*	
A.14.3 Test data A.14.3.1 Protection of test data A.15 Supplier Relationships A.15.1 Information security in supplier relationships A.15.1.1 Information security policy for supplier SA-12	, , ,	·
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 SA-12	, ,	SA-4, SA-12(1)
A.15 Supplier Relationships A.15.1 Information security in supplier relationships A.15.1.1 Information security policy for supplier SA-12		04.45(0)*
A.15.1 Information security in supplier relationships A.15.1.1 Information security policy for supplier SA-12		2A-13(9)"
A.15.1.1 Information security policy for supplier SA-12		
relationships	A.15.1.1 Information security policy for supplier	SA-12
A.15.1.2 Address security within supplier agreements SA-4, SA-12		SA-4. SA-12

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. A.15.1.3 Information and communication technology SA-12 supply chain A.15.2 Supplier service delivery management A.15.2.1 Monitoring and review of supplier services SA-9 SA-9 A.15.2.2 Managing changes to supplier services A.16 Information security incident management A.16.1 Managing of information security incidents and 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 AU-6, IR-4 security events IR-4 A.16.1.5 Response to information security incidents 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 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 All XX-1 controls contractual requirements A.18.1.2 Intellectual property rights 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

Note: The content of Table H-3, the mapping from the functional and assurance requirements in ISO/IEC 15408 (Common Criteria) to the security controls in Special Publication 800-53, is unaffected by the changes above.