	Security Control Family	Control Name	NIST 800-53 Control #	Low (Control and Control Enhancements)	MODERATE (Control and Control Enhancements)	Security Program Area (Function Area -> Functional Sub-Area)	NIST 800-53 Rev. 4 Control (Control and Control Enhancements) Detailed breakdown of required controls	Vendor's Response (Please Address all the controls and control enhancements in DETAIL. Controls and Enhancements identified in Column H)	Overall Control(s) Implementation Status (Reference on Comments Page) Please select from Drop down (Lower right corner)	Where does the Control(s) originate from? Please select from Drop down (Lower right corner)	Supporting Documentation (Policies and procedures must be explicitly referenced (title and date or version) so that it is clear which document is being referred to. Section numbers or similar mechanisms should allow the reviewer to easily find the	Vendor's Compensating Controls (If Control Can't Be Met - What is the alternative security controls employed by organization)	Vendor Non-Compliance (If you can't meet this control at all please explain why) (Please See Risk Statement for examples of Non-Compliance language Column R)	General Assessment Questions	Detailed Control Testing Procedure(s)	Risk Statement Examples	SOA Policy Number 1	SOA SubSection 1	SOA Policy Number 2	SOA SubSection 2	SOA Policy Number 3	SOA SubSection 3	SOA Policy Number 4	SOA SubSection 4			Arizona Breach Notification A.R.S. § 44-7501	Arizona Computer Tampering A.R.S. § 13-2316	COBIT Reference (Control Objective)
R0001	ACCESS CONTROL	ACCESS CONTROL POLICY AND PROCEDURES	AC-1	Required	Required	Protect -> Access Control	The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the access control policy and associated access controls; and b. Reviews and updates the current: 1. Access control policy [at least every 3 years]; and 2. Access control procedures [at least annually].	[redacted]							Have a documented access control policy standard that provides guidance regarding rules for granting access and is communicated to administrators and data / application owners for controlling access to information systems? The policy or standard reviewed and if not, updated on a scheduled basis?	Obtain access control policy and procedures; other relevant documents or records and ascertain if (1) the organization develops and documents access control policy and procedures; (2) the organization disseminates access control policy and procedures to appropriate elements within the organization; (3) responsible parties within the organization periodically review access control policy and procedures; and (4) the organization updates access control policy and procedures when organizational review indicates updates are required.	Access provided is not consistent with job function as Access Control Policy is not documented, communicated, and underpinned.	8120	6.2	8270	6.2	8280	6.1 - 6.7.1	8310	6.1 - 6.10	8320	6.1 - 6.18				COBIT v5 - High Level Control Objective APO13; DSS02; DSS05]Controls have been defined to ensure system security by defining IT security policies, procedures and standards, and monitoring, detecting, reporting security vulnerabilities and incidents.
R0002	ACCESS CONTROL	ACCOUNT MANAGEMENT	AC-2	Required	Required (1,2,3,4,5,7,9,10,12)	Protect -> Access Control	The organization: a. Identifies and selects the following types of information system accounts to support organizational missions/business functions: [Assignment: organization-defined information system account types]; b. Assigns account managers for information system accounts; c. Establishes conditions for group and role membership; d. Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account; e. Requires approvals by [Assignment: organization-defined personnel or roles] for requests to create information system accounts; f. Creates, enables, modifies, disables, and removes information system accounts in accordance with [Assignment: organization-defined procedures or conditions]; g. Monitors the use of information system accounts; h. Notifies account managers: 1. When accounts are no longer required; 2. When users are terminated or transferred; and 3. When individual information system usage or need-to-know changes; i. Authorizes access to the information system based on: 1. A valid access authorization; 2. Intended system usage; and 3. Other attributes as required by the organization or associated missions/business functions; j. Reviews accounts for compliance with account management requirements [At least annually]; and k. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.	[redacted]							There processes in place to ensure access added to users (e.g., the role provided to a for an application, or privileged access added to an IT administrator, etc.) aligns business requirements and/or access rights? For an example could be documented email from asset/business owner, timely list of access from transferred or ended employees, etc.).	Obtain access control policy and procedures; other relevant documents or records and ascertain if (1) the organization develops and documents access control policy and procedures; (2) the organization disseminates access control policy and procedures to appropriate elements within the organization; (3) responsible parties within the organization periodically review access control policy and procedures; and (4) the organization updates access control policy and procedures when organizational review indicates updates are required. Obtain access control policy; procedures addressing account management; security plan; list of active system accounts along with the name of the individual associated with each account; lists of recently transferred, separated, or terminated employees; list of recently disabled information system accounts along with the name of the individual associated with each account; system-generated records with user IDs and last login date; other relevant documents or records and ascertain if (1) the organization manages information system accounts, including authorizing, establishing, activating, modifying, reviewing, disabling, and removing accounts; (2) the organization defines in the security plan, explicitly or by reference, the frequency of information system account reviews and the frequency is at least annually; (3) the organization reviews information system accounts in accordance with organization-defined frequency; and (4) the organization initiates required actions on information system accounts based on the review. (5) determine if the organization employs automated mechanisms to support information system account management functions. (6) the organization defines in the security plan, explicitly or by reference, a time period for each type of account after which the information system terminates temporary and emergency accounts; and (7) the information system automatically terminates temporary and emergency accounts after organization-defined time period for each type of account. (8) the organization defines in the security plan, explicitly or by reference, a time period after which the information system disables inactive accounts; and (9) the information system automatically disables inactive accounts after organization-defined time period. (10) the organization employs automated mechanisms to audit account creation, modification, disabling, and termination actions; and (11) the organization employs automated mechanisms to notify, as required, appropriate individuals.	Unauthorized access is gained to information systems.	8310	6.1	8310	6.3-6.10							A.R.S 13-2316 (A)	COBIT v5 - High Level Control Objective APO13; DSS02; DSS05]Controls have been defined to ensure system security by defining IT security policies, procedures and standards, and monitoring, detecting, reporting security vulnerabilities and incidents.
R0003	ACCESS CONTROL	ACCESS ENFORCEMENT	AC-3	Required	Required	Protect -> Access Control	The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.	[redacted]							Information systems (applications, operating systems, network devices, databases, etc.) enforce approved authorizations for logical access employed per approved policy to provide protection from unauthorized access by malicious users, software or systems?	Obtain access control policy; procedures addressing access enforcement; information system configuration settings and associated documentation; list of assigned authorizations (user privileges); information system audit records; other relevant documents or records and ascertain if (1) the information system enforces assigned authorizations for controlling access to the system in accordance with applicable policy; and (2) user privileges on the information system are consistent with the documented user authorizations.	Misconfigured access controls provide unauthorized access to information held in application systems.	8320	6.1	8410	6.3								COBIT v5 - High Level Control Objective APO13; DSS02; DSS05]Controls have been defined to ensure system security by defining IT security policies, procedures and standards, and monitoring, detecting, reporting security vulnerabilities and incidents.
R0004	ACCESS CONTROL	INFORMATION FLOW ENFORCEMENT	AC-4		Required (21)	Protect -> Access Control	The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies]. Control Enhancements: (21) INFORMATION FLOW ENFORCEMENT	PHYSICAL / LOGICAL SEPARATION OF INFORMATION FLOWS The information system separates information flows logically or physically using [Assignment: organization-defined mechanisms and/or techniques] to accomplish [Assignment: organization defined required separations by types of information].	[redacted]							Is the institution or department have rules and supporting processes in place to "authorize" and regulate connections to and from applicable information systems, and are supporting processes can include security considerations when interfaces are created to and from the information system; defining administrative type access that can be to interface accounts, etc.); restrict and control the allocation and use of administrative access to information resources; (For examples may include approvals needed and administrative type access; monitoring administrative access need and usage; etc.)	Obtain access control policy; procedures addressing information flow enforcement; information system design documentation; information system configuration settings and associated documentation; information system baseline configuration; list of information flow authorizations; information system audit records; other relevant documents or records and ascertain if the information system enforces assigned authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy.	Users gain access to information that is beyond their appropriate level of privilege.	8320	6.3											COBIT v5 - High Level Control Objective APO13; DSS02; DSS05]Controls have been defined to ensure system security by defining IT security policies, procedures and standards, and monitoring, detecting, reporting security vulnerabilities and incidents.
R0005	ACCESS CONTROL	SEPARATION OF DUTIES	AC-5		Required	Protect -> Account Management	The organization: a. Separates [Assignment: organization-defined duties of individuals]; b. Documents separation of duties of individuals; and c. Defines information system access authorizations to support separation of duties.	[redacted]							Is the institution or department identified, documented and implemented roles (or roles) as necessary to prevent abuse or fraud if so, has such separation of duties been implemented through assigned information system access authorizations? (e. Fraud could occur when: administrator ability to clear system logs; developers update access to production systems; person roles where individual with access accounts payable has access to cash accounts, etc.)	Obtain access control policy; procedures addressing divisions of responsibility and separation of duties; information system configuration settings and associated documentation; list of divisions of responsibility and separation of duties; information system audit records; other relevant documents or records and ascertain if (1) the organization establishes appropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals; and (2) the information system enforces separation of duties through assigned access authorizations.	The lack of user segregation of duties may result in unauthorized or unintentional modification or misuse of the organization's information assets.	8310	6.3.4											COBIT v5 - High Level Control Objective APO13; DSS02; DSS05]Controls have been defined to ensure system security by defining IT security policies, procedures and standards, and monitoring, detecting, reporting security vulnerabilities and incidents. APO12]Controls have been established for defining the IT processes, organization and relationships to be responsive to business strategy and simply with governance requirements.
R0006	ACCESS CONTROL	LEAST PRIVILEGE	AC-6		Required (1,2,5,9,10)	Protect - Account Management	The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. Control Enhancement: (1) LEAST PRIVILEGE | AUTHORIZE ACCESS TO SECURITY FUNCTIONS The organization explicitly authorizes access to [Assignment: organization-defined security functions (deployed in hardware, software, and firmware) and security-relevant information]; (2) LEAST PRIVILEGE | NON-PRIVILEGED ACCESS FOR NONSECURITY FUNCTIONS The organization requires that users of information system accounts, or roles, with access to [all security functions] use non-privileged accounts or roles, when accessing non-security functions. (5) LEAST PRIVILEGE | PRIVILEGED ACCOUNTS The organization restricts privileged accounts on the information system to [Assignment: organization-defined personnel or roles]; (9) LEAST PRIVILEGE | AUDITING USE OF PRIVILEGED FUNCTIONS The information system audits the execution of privileged functions. (10) LEAST PRIVILEGE | PROHIBIT NON-PRIVILEGED USERS FROM EXECUTING PRIVILEGED FUNCTIONS The information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.	[redacted]							Is the institution or department established implemented procedures to restrict system access to only authorized personnel based on "need to know and to other information needs based on business function requirements? [Note the organization may be central access to facilities, information systems or applications, software programs for testing and revision.]	Obtain access control policy; procedures addressing least privilege; list of assigned access authorizations (user privileges); information system configuration settings and associated documentation; information system audit records; other relevant documents or records and ascertain if (1) the organization assigns the most restrictive set of rights/privileges or accesses needed by users for the performance of specified tasks; and (2) the information system enforces the most restrictive set of rights/privileges or accesses needed by users.	Information in applications is accessed by users and support personnel outside of defined business requirements.	8310	6.3.3, 6.4-6.8	8320	6.4-6.8	8410	6.4					A.R.S 13-2316 (A)	COBIT v5 - High Level Control Objective APO13; DSS02; DSS05]Controls have been defined to ensure system security by defining IT security policies, procedures and standards, and monitoring, detecting, reporting security vulnerabilities and incidents.
R0007	ACCESS CONTROL	UNSUCCESSFUL LOGON ATTEMPTS	AC-7	Required	Required	Protect -> System Configuration Hardening & Patch Management	The information system: a. Enforces a limit of [Assignment: organization-defined number] consecutive invalid logon attempts by a user during a [not more than three] and [Fifteen Minutes] b. Automatically [Selection: locks the account/node for an [locks the account/node for thirty minutes], locks the account/node until released by an administrator, delays next logon prompt according to [Assignment: organization-defined delay algorithm]] when the maximum number of unsuccessful attempts is exceeded.	[redacted]							The institution or department implemented procedures and controls to lock accounts after a defined number of unsuccessful logon attempts?	Obtain access control policy; procedures addressing unsuccessful logon attempts; security plan; information system configuration settings and associated documentation; information system audit records; other relevant documents or records and ascertain if (1) the organization defines in the security plan, explicitly or by reference, the maximum number of consecutive invalid access attempts to the information system by a user and the time period in which the consecutive invalid access attempts occur; (2) the information system enforces the organization-defined limit of consecutive invalid access attempts by a user during the organization-defined time period; (3) the organization defines in the security plan, explicitly or by reference, the time period for lock out mode or delay period; (4) the organization selects either a lock out mode for the organization-defined time period or delays next login prompt for the organization-defined delay period for information system responses to consecutive invalid access attempts; (5) the information system enforces the organization-selected lock out mode or delayed login prompt.	Unauthorized access is gained to operating systems.	8320	6.9										A.R.S 13-2316 (A)	COBIT v5 - High Level Control Objective APO13; DSS05]Controls have been defined to ensure system security by defining IT security policies, procedures and standards, and monitoring, detecting, reporting security vulnerabilities and incidents.
R0008	ACCESS CONTROL	SYSTEM USE NOTIFICATION	AC-8	Required	Required	Protect -> Identification & Authentication	The information system: a. Displays to users [Assignment: organization-defined system use notification message or banner] before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that: 1. Users are accessing a State of Arizona information system; 2. Information system usage may be monitored, recorded, and subject to audit; 3. Unauthorized use of the information system is prohibited and subject to criminal and civil penalties; and 4. Use of the information system indicates consent to monitoring and recording; b. Retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the information system; and c. For publicly accessible systems: 1. Displays system use information [Assignment: organization-defined conditions], before granting further access; 2. Displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and 3. Includes a description of the authorized uses of the system.	[redacted]							Is institutional or departmental information system display an approved system use notification message or banner before granting access to the information system?	Obtain access control policy; privacy and security policies; procedures addressing system use notification; information system configuration settings and associated documentation; information system audit records; other relevant documents or records and ascertain if (1) the information system displays a system use notification message before granting system access informing potential users: - that the user is accessing a State of Arizona information system; - that system usage may be monitored, recorded, and subject to audit; - that unauthorized use of the system is prohibited and subject to criminal and civil penalties; and - that use of the system indicates consent to monitoring and recording; (2) the system use notification message provides appropriate privacy and security notices (based on associated privacy and security policies or summaries); (3) the information system retains the information system use notification message before its use; and (4) the system use notification message remains on the screen until the user takes explicit actions to log on to the information system.	Unauthorized users log on to information systems.	8320	6.1											COBIT v5 - High Level Control Objective APO13; DSS02; DSS05]Controls have been defined to ensure system security by defining IT security policies, procedures and standards, and monitoring, detecting, reporting security vulnerabilities and incidents.
R0009	ACCESS CONTROL	CONCURRENT SESSION LOCK	AC-10		Required	Protect>Information & Authentication	Control: The information system: a. Prevents further access to the system by initiating a session lock after [three (3) sessions for privileged access and two (2) sessions for non-privileged access] of inactivity or upon receiving a request from a user; and b. Retains the session lock until the user reestablishes access using established identification and authentication procedures.	[redacted]							Does the information system enforce a session lock after a determined amount of time and until the users reestablishes access using established credentials.	Obtain access control policy; procedures addressing session lock; information system design documentation; information system configuration settings and associated documentation; security plan; other relevant documents or records and ascertain if (1) the organization defines in the security plan, explicitly or by reference, the time period of user inactivity after which the information system initiates a session lock; (2) the information system initiates a session lock after the organization-defined time period of inactivity; (3) the information system provides the capability for users to directly initiate session lock mechanisms; and (4) the information system maintains the session lock until the user reestablishes access using appropriate identification and authentication procedures.	Does not enforce a session lock													COBIT v5 - High Level Control Objective APO13; DSS02; DSS05]Controls have been defined to ensure system security by defining IT security policies, procedures and standards, and monitoring, detecting, reporting security vulnerabilities and incidents.
R0010	ACCESS CONTROL	SESSION LOCK	AC-11		Required (1)	Protect -> Account Management	The information system: a. Prevents further access to the system by initiating a session lock after [Assignment: organization-defined time period] of inactivity or upon receiving a request from a user; and b. Retains the session lock until the user reestablishes access using established identification and authentication procedures. Control Enhancement: (1) SESSION LOCK | PATTERN-HIDING DISPLAYS The information system conceals, via the session lock, information previously visible on the display with a publicly viewable image.	[redacted]							Does the information system enforce automatic session time-out after a pre-determined (reasonable period of inactivity (e.g. 30 minutes)? Upon log-off or system time-out, does the session lock the session in such a manner that unauthorized user cannot logon (e.g., in case of a web application, using an old session instance)?	Obtain access control policy; procedures addressing session lock; information system design documentation; information system configuration settings and associated documentation; security plan; other relevant documents or records and ascertain if (1) the organization defines in the security plan, explicitly or by reference, the time period of user inactivity after which the information system initiates a session lock; (2) the information system initiates a session lock after the organization-defined time period of inactivity; (3) the information system provides the capability for users to directly initiate session lock mechanisms; and (4) the information system maintains the session lock until the user reestablishes access using appropriate identification and authentication procedures.	Unauthorized users access operating systems by physically or logically accessing valid inactive and/or unattended sessions.	8320	6.11											COBIT v5 - High Level Control Objective APO13; DSS02; DSS05]Controls have been defined to ensure system security by defining IT security policies, procedures and standards, and monitoring, detecting, reporting security vulnerabilities and incidents.
R0011	ACCESS CONTROL	SESSION TERMINATION	AC-12		Required	Protect -> Account Management	The information system automatically terminates a user session after [Assignment: organization-defined conditions or trigger events requiring session disconnect].	[redacted]							Is the institution or department have documented processes and operational procedures for terminating user session after a defined period of inactivity?	Obtain documents relating to security safeguards and ascertain if the information system automatically terminates a user session when trigger events or conditions are met (such as organization-defined periods of user inactivity, targeted responses to certain types of incidents, time-of-day restrictions on information system use).	Inadequate session limit mechanisms may expose sensitive information or operating systems to unauthorized access.													COBIT v5 - High Level Control Objective APO13; DSS02; DSS05]Controls have been defined to ensure system security by defining IT security policies, procedures and standards, and monitoring, detecting, reporting security vulnerabilities and incidents.
R0012	ACCESS CONTROL	PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION	AC-14		Required	Protect -> Identification & Authentication	The organization: a. Identifies [Assignment: organization-defined user actions] that can be performed on the information system without identification or authentication consistent with organizational missions/business functions; and b. Documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification or authentication.	[redacted]							Are procedures in place for obtaining necessary access information during an emergency but identification and authentication only to a extent necessary to accomplish mission/business objectives?	Obtain access control policy; procedures addressing permitted actions without identification and authentication; information system configuration settings and associated documentation; security plan; other relevant documents or records and ascertain if the organization identifies and documents specific user actions that can be performed on the information system without identification or authentication.	During an emergency access to information will not be available or will be disclosed to unauthorized parties.	8320	6.12											COBIT v5 - High Level Control Objective APO13; DSS02; DSS05]Controls have been defined to ensure system security by defining IT security policies, procedures and standards, and monitoring, detecting, reporting security vulnerabilities and incidents.

	Security Control Family	Control Name	NIST 800-53 Control #	Low (Control and Control Enhancements)	MODERATE (Control and Control Enhancements)	Security Program Area (Function Area or Functional Sub-Area)	NIST 800-53 Rev. 4 Control (Control and Control Enhancements) Detailed breakdown of required controls	Vendor's Response (Please Address all the controls and control enhancements in DETAIL. Controls and Enhancements identified in Column H)	Overall Control(s) Implementation Status (Reference on Comments Page) Please select from Drop down (Lower right corner)	Where does the Control(s) originate from? Please select from Drop down (Lower right corner)	Supporting Documentation (Policies and procedures must be explicitly referenced (title and date or version) so that it is clear which document is being referred to. Section numbers or similar mechanisms should allow the reviewer to easily find the	Vendor's Compensating Controls (If Control Can't Be Met - What is the alternative security controls employed by organization)	Vendor Non-Compliance (If you can't meet this control at all please explain why) (Please See Risk Statement for examples of Non-Compliance language Column R)	General Assessment Questions	Detailed Control Testing Precaution(s)	Risk Statement Examples	SOA Policy Number 1	SOA SubSection 1	SOA Policy Number 2	SOA SubSection 2	SOA Policy Number 3	SOA SubSection 3	SOA Policy Number 4	SOA SubSection 4			Arizona Breach Notification A.R.S. § 44-7501	Arizona Computer Tampering A.R.S. § 13-2316	COBIT Reference (Control Objective)
R0813	ACCESS CONTROL	REMOTE ACCESS	AC-17	Required	Required (1,2,3,4,9)	Protect -> Portable & Remote Computing	The organization: a. Establishes and documents usage restrictions, configuration/connection requirements and implementation guidance for each type of remote access allowed; and b. Authorizes remote access to the information system prior to allowing such connections. Control Enhancement: (1) REMOTE ACCESS	AUTOMATED MONITORING / CONTROL The information system monitors and controls remote access methods. (2) REMOTE ACCESS	CONFIDENTIALITY / INTEGRITY USING ENCRYPTIO The information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions. (3) REMOTE ACCESS	MANAGED ACCESS CONTROL POINTS The information system routes all remote accesses through [Assignment: organization-defined number] managed network access control points. (4) REMOTE ACCESS	PRIVILEGED COMMANDS / ACCESS The organization: (a) Authorizes the execution of privileged commands and access to security-relevant information via remote access only for [Assignment: organization-defined needs]; and (b) Documents the rationale for such access in the security plan for the information system. (9) REMOTE ACCESS	DISCONNECT / DISABLE ACCESS The organization provides the capability to expeditiously disconnect or disable remote access to the information system within [no greater than 15 minutes].		

	Security Control Family	Control Name	NIST 800-53 Control #	Low (Control and Control Enhancements)	MODERATE (Control and Control Enhancements)	Security Program Area (Function Area – Functional Sub-Area)	NIST 800-53 Rev. 4 Control (Control and Control Enhancements) Detailed breakdown of required controls	Vendor's Response (Please Address all the controls and control enhancements in DETAIL Controls and Enhancements identified in Column H)	Overall Control(s) Implementation Status (Reference on Comments Page) Please select from Drop down (Lower right corner)	Where does the Control(s) originate from? Please select from Drop down (Lower right corner)	Supporting Documentation (Policies and procedures must be explicitly referenced (title and date or version) so that it is clear which document is being referred to. Section numbers or similar mechanisms should allow the reviewer to easily find the reference)	Vendor's Compensating Controls (If Control Can't Be Met - What is the alternative security controls employed by organization)	Vendor Non-Compliance (If you can't meet this control at all please explain why) (Please See Risk Statement for examples of Non-Compliance language Column R)	General Assessment Questions	Detailed Control Testing Procedure(s)	Risk Statement Examples	SOA Policy Number 1	SOA SubSection 1	SOA Policy Number 2	SOA SubSection 2	SOA Policy Number 3	SOA SubSection 3	SOA Policy Number 4	SOA SubSection 4			Arizona Breach Notification A.R.S. § 44-7501	Arizona Computer Tampering A.R.S. § 13-2316	COBIT Reference (Control Objective)
R0026	AUDIT AND ACCOUNTABILITY	AUDIT STORAGE CAPACITY	AU-4	Required	Required	Protect -> Audit Logging and Security Event Management & Media	The organization allocates audit record storage capacity in accordance with [Assignment: organization-defined audit record storage requirements].	[redacted]						es the institution or department monitor e storage capacity of its logging servers to event data over-writing?	Obtain audit and accountability policy; procedures addressing audit storage capacity; information system design documentation; organization-defined audit record storage capacity for information system components that store audit records; list of organization-defined auditable events; information system configuration settings and associated documentation; information system audit records; other relevant documents or records and ascertain if : 1)the organization allocates sufficient audit record storage capacity; and 2)the organization configures auditing to reduce the likelihood of audit record storage capacity being exceeded.	Logging facilities and log information is compromised and tampered with due to inadequate data protection mechanisms.												CobiT v5 - High Level Control Objective AP013: DSS02, DSS05 Controls have been defined to ensure system security by defining IT security policies, procedures and standards, and monitoring, detecting, reporting security vulnerabilities and incidents.
R0027	AUDIT AND ACCOUNTABILITY	RESPONSE TO AUDIT PROCESSING FAILURES	AU-5	Required	Required	Protect -> Audit Logging and Security Event Management & Media	The information system: a. Alerts [Assignment: organization-defined personnel or roles] in the event of an audit processing failure; and b. Takes the following additional actions: [low-impact: overwrite oldest audit records; moderate-impact: shut down].	[redacted]						es the institution or department log all user ess to confidential data (e.g., card holder ata, PII) and enable audit trails to equately log each user's activities	Obtain audit and accountability policy; procedures addressing response to audit processing failures; information system design documentation; security plan; information system configuration settings and associated documentation; list of personnel to be notified in case of an audit processing failure; information system audit records; other relevant documents or records. And ascertain if 1)the organization defines in the security plan, explicitly or by reference, actions to be taken in the event of an audit processing failure; 2)the organization defines in the security plan, explicitly or by reference, personnel to be notified in case of an audit processing failure; and 3)the information system alerts appropriate organizational officials and takes any additional organization-defined actions in the event of an audit failure, to include audit storage capacity being reached or exceeded.	Unauthorized system activities are undetected because of inconsistent audit log monitoring.	8330	6.2.3											CobiT v5 - High Level Control Objective AP013: DSS05Controls have been defined to ensure system security by defining IT security policies, procedures and standards, and monitoring, detecting, reporting security vulnerabilities and incidents.
R0028	AUDIT AND ACCOUNTABILITY	AUDIT REVIEW, ANALYSIS, AND REPORTING	AU-6	Required	Required (1,3)	Protect -> Audit Logging and Security Event Management & Media	The organization: a. Reviews and analyzes information system audit records [Assignment: organization-defined frequency] for indications of [Parameter: [at least weekly]]; and b. Reports findings to [Assignment: organization-defined personnel or roles]. Control Enhancement: (1) AUDIT REVIEW, ANALYSIS, AND REPORTING	PROCESS INTEGRATION The organization employs automated mechanisms to integrate audit review, analysis, an reporting processes to support organizational processes for investigation and response t suspicious activities. (3) AUDIT REVIEW, ANALYSIS, AND REPORTING	CORRELATE AUDIT REPOSITORIES The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness.	[redacted]						e information system audit records reviewed d analyzed on a daily basis for indications of appropriate or unusual activity, findings ported to designated organizational officials, d corrective action plans implemented for entified issues? g., logs from different system correlated in der to effectively detect potential security ues; specific use cases for alerts been fined in order to identify critical security ents; and organizational personnel that st and are responsible for responding to erts; such process is tied to the incident-ponse process]	Obtain audit and accountability policy; procedures addressing audit monitoring, analysis, and reporting; threat information documentation from law enforcement, intelligence community, or other sources; information system configuration settings and associated documentation; information system audit records; reports of audit findings; records of actions taken in response to reviews/analyses of audit records; other relevant documents or records and ascertain if : 1)the organization regularly reviews/analyzes audit records for indications of inappropriate or unusual activity; 2)the organization investigates suspicious activity or suspected violations; 3)the organization reports findings of inappropriate/unusual activities, suspicious behavior, or suspected violations to appropriate officials; and 4)the organization takes necessary actions in response to the reviews/analyses of audit records	Audit findings are not effectively communicated or resolved by management.	8330	6.5											CobiT v5 - High Level Control Objective ME02.01-02 Controls have been defined to monitoring and evaluating internal controls.
R0029	AUDIT AND ACCOUNTABILITY	AUDIT REDUCTION AND REPORT GENERATION	AU-7		Required (1)	Respond -> Cyber-Security Incident Response	The information system provides an audit reduction and report generation capability tha a. Supports on-demand audit review, analysis, and reporting requirements and after-the fact investigations of security incidents; and b. Does not alter the original content or time ordering of audit records. Control Enhancement: (1) AUDIT REDUCTION AND REPORT GENERATION	AUTOMATIC PROCESSING The information system provides the capability to process audit records for events of interest based on [Assignment: organization-defined audit fields within audit records].	[redacted]						es the department have security incident management policies and supporting oceduresin place that includes: requirements for proper tuning of logs and erts so as to focus on higher risk events; proper log retention policies; and proper handling and access controls to ntain integrity of logs and other data that upport forensics and investigations have documented use cases that guide the sponders on how to manage incidents: ported or identified [e.g., classification and ne steps] clearly indicate who needs to be notified, by hen, and in what manner?	Obtain audit and accountability policy; procedures addressing audit reduction and report generation; information system design documentation; audit reduction, review, and reporting tools; and associated documentation ;other relevant documents or records and ascertain if: (1) the information system provides audit reduction and report generation tools that support after-the-fact investigations of security incidents without altering original audit records; (2)the information system provides the capability to automatically process audit records for events of interest based upon selectable, event criteria.	Information security events are not reported.	8330	6.6											CobiT v5 - High Level Control Objective DSS is derived from COBIT as it does not cover Service Desk Process.] Controls have been defined for management of the service desk and incidents.
R0030	AUDIT AND ACCOUNTABILITY	TIME STAMPS	AU-8	Required	Required (1)	Protect -> Audit Logging and Security Event Management & Media	The information system: a. Uses internal system clocks to generate time stamps for audit records; and b. Records time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) and meets [Assignment: organization-define granularity of time measurement]. Control Enhancement: (1) TIME STAMPS | SYNCHRONIZATION WITH AUTHORITATIVE TIME SOURCE The information system: (a) Compares the internal information system clocks [http://tf.nist.gov/tf-cgi/servers.cgi] (b) Synchronizes the internal system clocks to the authoritative time source when the tim difference is greater than [At least hourly].	[redacted]						the information system configured to use ternal system clocks to generate time stamps audit records? [Note: The ability to curately monitor timestamps from logs could fect the incident response process.]	Obtain audit and accountability policy; procedures addressing time stamp generation; information system design documentation; information system configuration settings and associated documentation; information system audit records; security plan; other relevant documents or records and ascertain if : (1) the information system provides time stamps in audit records. (2)the organization defines in the security plan, explicitly or by reference, the frequency of internal clock synchronization for the information system; and (3)the organization synchronizes internal information system clocks periodically in accordance with organization-defined frequency.	The lack of operational control to synchronize system clocks with an authoritative time source may hinder the ability to accurately monitor timestamps from logs which could affect the incident response process.	8330	6.7											CobiT v5 - High Level Control Objective AP013: DSS05Controls have been defined to ensure system security by defining IT security policies, procedures and standards, and monitoring, detecting, reporting security vulnerabilities and incidents.
R0031	AUDIT AND ACCOUNTABILITY	PROTECTION OF AUDIT INFORMATION	AU-9	Required	Required (2,4)	Protect -> Audit Logging and Security Event Management & Media	The information system protects audit information and audit tools from unauthorized access, modification, and deletion. Control Enhancement: (2) PROTECTION OF AUDIT INFORMATION | AUDIT BACKUP ON SEPARATE PHYSICAL SYSTEMS / COMPONENTS The information system backs up audit records [At least weekly] onto physically different system or system component than the system or component being audited. (4) PROTECTION OF AUDIT INFORMATION | ACCESS BY SUBSET OF PRIVILEGED USERS The organization authorizes access to management of audit functionality to only [Assignment: organization-defined subset of users.].	[redacted]						access to log data directories adequately ntrolled?	Obtain audit and accountability policy; procedures addressing protection of audit information; access control policy and procedures; information system design documentation; information system configuration settings and associated documentation; information system audit records; audit tools; other relevant documents or records and ascertain if :the information system protects audit information and audit tools from unauthorized access, modification, and deletion.	Failure to restrict access to logging facilities and log information may result in unauthorized access, log information tampering and loss of user activity evidence.	8330	6.8											CobiT v5 - High Level Control Objective AP013: DSS05Controls have been defined to ensure system security by defining IT security policies, procedures and standards, and monitoring, detecting, reporting security vulnerabilities and incidents.
R0032	AUDIT AND ACCOUNTABILITY	AUDIT RECORD RETENTION	AU-11	Required	Required	Protect -> Data Loss Prevention	The organization retains audit records for [at least ninety days] to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.	[redacted]						e audit records retained to provide support for after-the-fact investigations of security cidents in accordance with regulatory uirements and institutional records ention requirements?	Obtain audit and accountability policy; procedures addressing audit record retention; organization-defined retention period for audit records; information system audit records; other relevant documents or records and ascertain if : (1)the organization defines the retention period for audit records generated by the information system; and (2)the organization retains information system audit records for the organization-defined time period to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.	Laws and regulations are violated due to data not being retained for the required duration of time or inappropriate data being stored.	8330	6.9											CobiT v5 - High Level Control Objective ME03: Controls have been defined to ensure regulatory compliance by identifying all applicable laws and regulations and the corresponding level of IT compliance and optimizing IT processes to reduce the risk of non-compliance.
R0033	AUDIT AND ACCOUNTABILITY	AUDIT GENERATION	AU-12	Required	Required	Protect -> Audit Logging and Security Event Management & Media	The information system: a. Provides audit record generation capability for the auditable events defined in AU-2 a. at [all information system and network components where audit capability is deployed/available]; b. Allows [Assignment: organization-defined personnel or roles] to select which auditable events are to be audited by specific components of the information system; and c. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3.	[redacted]						es the institution or department have a cumented logging standard that defines the ents requirements for logging (e.g., fields log, type of events, log processes, uirements, retention requirements, etc.)?	Obtain audit and accountability policy; procedures addressing audit record generation; security plan; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records and ascertain if : (1) the organization defines the information system components that provide audit record generation capability for the list of auditable events defined in AU-2; (2) the information system provides audit record generation capability, at organization-defined information system components, for the list of auditable events defined in AU-2; (3) the information system allows designated organizational personnel to select which auditable events are to be audited by specific components of the system; and (4) the information system generates audit records for the list of audited events defined in AU-2 with the content as defined in AU-3.	Failure to plan and execute IT audit activities may result in potential compromise of critical business processes and sensitive data to go undetected.	8330	6.1											CobiT v5 - High Level Control Objective ME02.01-02 Controls have been defined to monitoring and evaluating internal controls.
R0034	SECURITY ASSESSMENT AND AUTHORIZATION	SECURITY ASSESSMENT AND AUTHORIZATION POLICY AND PROCEDURES	CA-1	Required	Required	Identify -> Security Assessment and Authorization / Technology Risk Assessments	The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A security assessment and authorization policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization controls; and b. Reviews and updates the current: 1. Security assessment and authorization policy [At least every 3 years]; and 2. Security assessment and authorization procedures [At least annually].	[redacted]						es the institution or department *published a ntry or other directives related to* ssment and authorization and communicated to faculty, staff, business, IT, d other users about expectations and their e concerning information security?	Obtain security assessment and certification and accreditation policies and procedures; other relevant documents or records and ascertain if : (1)the organization develops and documents security assessment and certification and accreditation policies and procedures. (2)the organization disseminates security assessment and certification and accreditation policies and procedures to appropriate elements within the organization. (3)responsible parties within the organization periodically review policy and procedures. (4)the organization updates security assessment and authorization and accreditation policies and procedures when organizational review indicates updates are required. (5)the security assessment and certification and accreditation policies address purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance. (6)the security assessment and certification and accreditation policies are consistent with the organization's mission and business functions and with applicable laws, directives, policies, regulations, standards, and guidance. (7)the security assessment and certification and accreditation procedures address all areas identified in the security assessment and certification and accreditation policies and address achieving policy-compliant implementations of all associated security assessment and certification and accreditation controls.	Management does not set a clear policy direction in line with business objectives and demonstrate support for, and commitment to, information security.	8120	6.2											CobiT v5 - High Level Control Objective ME03: AP001 Controls have been defined to ensure effective management aims and direction through providing accurate, understandable and approved policies, procedures, guidelines and other documentation to stakeholders, embedded in an IT control framework.
R0035	SECURITY ASSESSMENT AND AUTHORIZATION	SECURITY ASSESSMENTS	CA-2	Required (1)	Required (1,2,3)	Identify -> Security Assessment and Authorization / Technology Risk Assessments	The organization: a. Develops a security assessment plan that describes the scope of the assessment including: 1. Security controls and control enhancements under assessment; 2. Assessment procedures to be used to determine security control effectiveness; and 3. Assessment environment, assessment team, and assessment roles and responsibilities b. Assesses the security controls in the information system and its environment of operation[at least annually] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements; c. Produces a security assessment report that documents the results of the assessment; and d. Provides the results of the security control assessment to [individuals or roles to include AODA;NIST]. Control Enhancement: **(1) SECURITY ASSESSMENTS | INDEPENDENT ASSESSORS** **The organization employs assessors or assessment teams with [Assignment: organization defined level of independence] to conduct security control assessments.** (2) SECURITY ASSESSMENTS | SPECIALIZED ASSESSMENTS The organization includes as part of security control assessments, [at least annually], [Selection: announced; unannounced]; [Selection (one or more): in-depth monitoring; vulnerability scanning; malicious user testing; insider threat assessment; performance/load testing; [Assignment: organization-defined other forms of security assessment]]. (3) SECURITY ASSESSMENTS | EXTERNAL ORGANIZATIONS [Assignment: organization-defined information system] performed by [Assignment:	[redacted]						es the institution or department have a fined information security program that ludes: developing a plan and executing periodic ssessments of security control effectiveness; identifying objective and qualified assessors; d reporting results of such assessment(s) to e appropriate stakeholders?	Obtain security assessment policy; procedures addressing security assessments; security plan; security assessment plan; security assessment report; assessment evidence; security authorization package (including security plan; security assessment report, plan of action and milestones, authorization statement); other relevant documents or records and ascertain if : (1)the organization defines in the security plan, explicitly or by reference, the frequency of security control assessments and the frequency is at least annually (2)the organization conducts an assessment of the security controls in the information system at an organization-defined frequency. (3)the organization employs an independent assessor or assessment team to conduct an assessment of the security controls in the information system.	Independent reviews of information security are not regularly performed to ensure the continuing suitability, adequacy, and effectiveness of the organization's information security program.	8120	6.5.1											CobiT v5 - High Level Control Objective ME02.01-02 Controls have been defined to monitoring and evaluating internal controls.
R0036	SECURITY ASSESSMENT AND AUTHORIZATION	SYSTEM INTERCONNECTIONS	CA-3	Required	Required (3,5)	Identify -> Security Assessment and Authorization / Technology Risk Assessments & Identify -> External Vendors and Third Party Providers Identify -> Privacy & Confidentiality	The organization: a. Authorizes connections from the information system to other information systems through the use of Interconnection Security Agreements; b. Documents, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated; and c. Reviews and updates Interconnection Security Agreements [3 Years / Annually and as input from State of Arizona]. Control Enhancement: (3) SYSTEM INTERCONNECTIONS | UNCLASSIFIED NON-NATIONAL SECURITY SYSTEM CONNECTIONS The organization prohibits the direct connection of an [Assignment: organization-defined unclassified, non-national security system] to an external network without the use of [Assignment: organization-defined boundary protection device]. (5) SYSTEM INTERCONNECTIONS | RESTRICTIONS ON EXTERNAL SYSTEM CONNECTIONS The organization employs [Selection: allow-all, deny-by-exception; deny-all, permit-by-exception] policy for allowing [Assignment: organization-defined information systems] to connect to external information systems.	[redacted]						es the institution or department have uirements defined and perform monitoring those requirements for systems that connect other systems outside of its immediate ntrol?	Obtain access control policy; procedures addressing information system connections; NIST Special Publication 800-47; system and communications protection policy; personnel security policy; information system connection agreements; security plan; information system design documentation; information system configuration management and control documentation; security assessment report; plan of action and milestones; other relevant documents or records and ascertain if : (1)the organization identifies all connections to external information systems [i.e., information systems outside of the accreditation boundary]. (2)the organization authorizes all connections from the information system to external information systems through the use of system connection agreements. (3)the organization monitors/controls the system interconnections on an ongoing basis.	Security breaches occur due to risks related to external parties not being identified and controlled.	8120	6.5.4											CobiT v5 - High Level Control Objective AP010: Controls have been defined for managing third-party services by establishing relationships and bilateral responsibilities with qualified third-party service providers and monitoring the service delivery to verify and ensure adherence to agreements.
R0037	SECURITY ASSESSMENT AND AUTHORIZATION	PLAN OF ACTION AND MILESTONES	CA-5	Required	Required	Detect -> Vulnerability Assessment	The organization: a. Develops a plan of action and milestones for the information system to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and b. Updates existing plan of action and milestones [At least monthly] based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.	[redacted]						s there a defined process for recording, signing ownership, and remediating issues ntified in security assessments such as dits, vulnerability assessments, risk sessments, and penetration tests?	Obtain certification and accreditation policy; procedures addressing plan of action and milestones; security plan; security assessment plan; security assessment report; assessment evidence; plan of action and milestones; other relevant documents or records and ascertain if : (1)the organization develops a plan of action and milestones for the information system. (2)the organization documents the planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system. (3)the organization defines in the security plan, explicitly or by reference, the frequency of plan of action and milestone updates. (4)the organization updates the plan of action and milestones at an organization-defined frequency.	Identified risks are not accepted, mitigated or responded to with actionable plans and decisions.	8120	6.5.5											CobiT v5 - High Level Control Objective EDM03, AP012, AP013Controls have been defined to assess and manage IT risks.
R0038	SECURITY ASSESSMENT AND AUTHORIZATION	SECURITY AUTHORIZATION	CA-6	Required	Required	Identify -> Control Oversight and Safeguard Assurance & Protect -> Change Management	The organization: a. Assigns a senior-level executive or manager as the authorizing official for the information system; b. Ensures that the authorizing official authorizes the information system for processing before commencing operations; and c. Updates the security authorization [at least every three years or when a significant change occurs].	[redacted]						Does the institution or department follow a fined process for approving new information ems for production use based upon ovals from appropriate stakeholders, luding information security (e.g., approval from ISO)? For existing systems, does the department ure appropriate approvals from relevant eholders, including information security g., approval from ISO) when major changes e made to information systems and/or ated processes?	Obtain certification and accreditation policy; procedures addressing security accreditation; NIST Special Publication 800-37; security accreditation package (including security plan; security assessment report; plan of action and milestones; authorization statement); other relevant documents or records and ascertain if : (1)the organization defines in the security plan, explicitly or by reference, the frequency of authorization updates (not to exceed three years). (2)the organization authorizes (i.e., accredits) the information system for processing before operations and updates the authorization at an organization-defined frequency or when there is a significant change to the information system. (3)a senior organizational official signs and approves the security accreditation; and (4)the security accreditation process employed by the organization is consistent with NIST Special Publications 800-37.	Responsibility for the IT program has not been defined.	8120	6.5.6											CobiT v5 - High Level Control Objective AP013, DSS05Controls have been defined to ensure system security by defining IT security policies, procedures and standards, and monitoring, detecting, reporting security vulnerabilities and incidents.

	Security Control Family	Control Name	NIST 800-53 Control #	Low (Control and Control Enhancements)	MODERATE (Control and Control Enhancements)	Security Program Area (Function Area or Functional Sub-Area)	NIST 800-53 Rev. 4 Control (Control and Control Enhancements) Detailed breakdown of required controls	Vendor's Response (Please Address all the controls and control enhancements in DETAIL. Controls and Enhancements identified in Column H)	Overall Control(s) Implementation Status (Reference on Comments Page) Please select from Drop down (Lower right corner)	Where does the Control(s) originate from? Please select from Drop down (Lower right corner)	Supporting Documentation (Policies and procedures must be explicitly referenced (title and date or version) so that it is clear which document is being referred to. Section numbers or similar mechanisms should allow the reviewer to easily find the reference.)	Vendor's Compensating Controls (If Control Can't Be Met - What is the alternative security controls employed by organization)	Vendor Non-Compliance (If you can't meet this control at all please explain why) (Please See Risk Statement for examples of Non-Compliance language Column R)	General Assessment Questions	Detailed Control Testing Procedure(s)	Risk Statement Examples	SOA Policy Number 1	SOA SubSection 1	SOA Policy Number 2	SOA SubSection 2	SOA Policy Number 3	SOA SubSection 3	SOA Policy Number 4	SOA SubSection 4			Arizona Breach Notification A.R.S. § 44-7501	Arizona Computer Tampering A.R.S. § 13-2316	COBIT Reference (Control Objective)
R0039	SECURITY ASSESSMENT AND AUTHORIZATION	CONTINUOUS MONITORING	CA-7		Required	Required (1)	Identify-> Control Oversight and Safeguard Assurance & Security Compliance and Regulatory Requirements Management	The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes: a. Establishment of [Assignment: organization-defined metrics] to be monitored; b. Establishment of [Assignment: organization-defined frequencies] for monitoring an [Assignment: organization-defined frequencies] for assessments supporting such monitoring; c. Ongoing security control assessments in accordance with the organizational contin monitoring strategy; d. Ongoing security status monitoring of organization-defined metrics in accordance the organizational continuous monitoring strategy; [To meet State of Arizona's requirements:] e. Correlation and analysis of security-related information generated by assessments monitoring; f. Response actions to address results of the analysis of security-related information; g. Reporting the security status of organization and the information system to [Assignment: organization-defined personnel or roles] [Assignment: organization-def frequency]. Control Enhancement: (1) CONTINUOUS MONITORING	INDEPENDENT ASSESSMENT The organization employs assessors or assessment teams with [Assignment: organiz defined level of independence] to monitor the security controls in the information sy on an ongoing basis.																						
R0040	SECURITY ASSESSMENT AND AUTHORIZATION	PENETRATION TESTING	CA-8			Required (1)	Identify-> Control Oversight and Safeguard Assurance & Security Compliance and Regulatory Requirements Management	The organization conducts penetration testing [At least annually] on [Assignment: organization-defined information systems or system components]. (1) PENETRATION TESTING	INDEPENDENT PENETRATION AGENT OR TEAM The organization employs an independent penetration agent or penetration team to perform penetration testing on the information system or system components.					Does the institution or department conduct penetration testing on defined information systems or system components. Does your institution or department employs an independent penetration agent or penetration team to perform penetration testing on the information system or system components.	Obtain certification and accreditation policy; procedures addressing Information Security Testing and Assessment ; NIST Special Publications 800-115	Do not conduct penetration testing or employ independent penetration testing													
R0041	SECURITY ASSESSMENT AND AUTHORIZATION	INTERNAL SYSTEM CONNECTIONS	CA-9		Required	Required	Information Security Operations & Media & Identify -> Security Assessment and Authorization / Technology Risk Assessments	The organization: a. Authorizes internal connections of [Assignment: organization-defined information system components or classes of components] to the information system; and b. Documents, for each internal connection, the interface characteristics, security requirements, and the nature of the information communicated.						Does the institution or department have processes to authorize internal connections between organization-defined information system components? (Note: example of internal system connections include, system connections with mobile devices, notebook/desktop computers, printers, copiers, facsimile machines, scanners, sensors, and servers)	Obtain procedures addressing internal connections between organization-defined information system components (such as system connections with mobile devices, notebook/desktop computers, printers, copiers, facsimile machines, scanners, sensors, and servers) and ascertain if: (1) the internal connections are authorized; (2) the documentation contains interface characteristics, security requirements and the nature of information communicated.	Failure to establish formal authorization processes for restricting user access to internal system connections may result in unauthorized or unsecure connections to the network exposing sensitive or critical business applications.													{CobiT v5 - High Level Control Objective APO13, DSS05}Controls have been defined to ensure system security by defining IT security policies, procedures and standards, and monitoring, detecting, reporting security vulnerabilities and incidents.
R0042	CONFIGURATION MANAGEMENT	CONFIGURATION MANAGEMENT POLICY AND PROCEDURES	CM-1		Required	Required	Protect -> Secure Configuration Management & Change Management	The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entiti and compliance; and 2. Procedures to facilitate the implementation of the configuration management poli and associated configuration management controls; and b. Reviews and updates the current: 1. Configuration management policy [at least every 3 years]; and 2. Configuration management procedures [at least every annually];							Does the institution or department have documented policies, standards, and procedures in place to establish, communicate, and monitor minimum information security configurations for all information system types connecting institutional networks?	Obtain configuration management policy and procedures; other relevant documents or records; and ascertain if: (1)the organization develops and documents configuration management policy and procedures. (2)the organization disseminates configuration management policy and procedures to appropriate elements within the organization. (3)responsible parties within the organization periodically review configuration management policy and procedures. (4)the organization updates configuration management policy and procedures when organizational review indicates updates are required. (5)the configuration management policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance; (6)the configuration management policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and (7)the configuration management procedures address all areas identified in the configuration management policy and address achieving policy-compliant implementations of all associated configuration management controls.	The change management process in place does not adequately protect the environment from disruptive changes in production.													{CobiT v5 - High Level Control Objective BAI06}Controls have been defined to manage changes to information systems in order to minimize the likelihood of disruption, unauthorized alterations and errors.
R0043	CONFIGURATION MANAGEMENT	BASELINE CONFIGURATION	CM-2		Required	Required (1,2,3,7)	Protect -> Secure Configuration Management & Change Management Identify -> Critical Information Asset Inventory	The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system. Control Enhancement: (1) BASELINE CONFIGURATION	REVIEWS AND UPDATES The organization reviews and updates the baseline configuration of the information system: (a) [at least annually]; (b) When required due [to include when directed by Authorizing Official]; and (c) As an integral part of information system component installations and upgrades. (2) BASELINE CONFIGURATION	AUTOMATION SUPPORT FOR ACCURACY / CURRENCY The organization employs automated mechanisms to maintain an up-to-date, compl accurate, and readily available baseline configuration of the information system. (3)BASELINE CONFIGURATION	AUTOMATION SUPPORT FOR ACCURACY / CURRENCY The organization employs automated mechanisms to maintain an up-to-date, compl accurate, and readily available baseline configuration of the information system. (7) BASELINE CONFIGURATION	RETENTION OF PREVIOUS CONFIGURATIONS The organization retains [Assignment: organization-defined previous versions of base configurations of the information system] to support rollback. (9) BASELINE CONFIGURATION	CONFIGURE SYSTEMS, COMPONENTS, OR DEVICES FO HIGH-RISK AREAS The organization: (a) Issues [Assignment: organization-defined information systems, system component devices] with [Assignment: organization-defined configurations] to individuals travel locations that the organization deems to be of significant risk; and					Does the institution or department established and communicated minimum baseline security configuration standards for information systems accessing institutional networks? If yes, are the baseline security standards based on some recognized or industry guidance (e.g., vendor documentation, CIS,Center for Internet Security), NIST, etc.?	Obtain configuration management policy; procedures addressing the baseline configuration of the information system; configuration management plan; Federal Enterprise Architecture documentation; information system design documentation; information system architecture and configuration documentation; historical copies of baseline configurations; list of software programs not authorized to execute on the information system; other relevant documents or records and ascertain if: (1)the organization develops and documents a baseline configuration of the information system that is consistent with the Federal Enterprise Architecture, shows relationships among information system components, and provides a well-defined and documented specification to which the information system is built. (2)the organization maintains the baseline configuration. (3)the organization documents deviations from the baseline configuration, in support of mission needs/objectives. (4) the organization develops and maintains a list of software programs not authorized to execute on the information system.	Changes to systems and applications are executed inconsistently in the production environment due to ill-defined procedures.													{CobiT v5 - High Level Control Objective BAI06}Controls have been defined to manage changes to information systems in order to minimize the likelihood of disruption, unauthorized alterations and errors.
R0044	CONFIGURATION MANAGEMENT	CONFIGURATION CHANGE CONTROL	CM-3		Required	Required	Protect -> Secure Configuration Management & Change Management	The organization: a. Determines the types of changes to the information system that are configuration-controlled; b. Reviews proposed configuration-controlled changes to the information system and approves or disapproves such changes with explicit consideration for security impact analyses; c. Documents configuration change decisions associated with the information system; d. Implements approved configuration-controlled changes to the information system e. Retains records of configuration-controlled changes to the information system for [Assignment: organization-defined time period]; f. Audits and reviews activities associated with configuration-controlled changes to th information system; and g. Coordinates and provides oversight for configuration change control activities thro [Assignment: organization-defined configuration change control element (e.g., commi board)] that convenes [Selection (one or more): [Assignment: organization-defined frequency]; [Assignment: organization-defined configuration change conditions]]. Control Enhancement: (2) CONFIGURATION CHANGE CONTROL	TEST / VALIDATE / DOCUMENT CHANGES The organization tests, validates, and documents changes to the information system before implementing the changes on the operational system.								Are changes to baseline security configuration standards managed, tested, and approved by a formally defined change management function that includes representation from appropriate stakeholders?	Obtain configuration management policy; procedures addressing information system configuration change control; configuration management plan; information system design documentation; information system architecture and configuration documentation; change control records; information system audit records; other relevant documents or records and ascertain if : (1)the organization employs automated mechanisms to document proposed changes to the information system; (2)the organization employs automated mechanisms to notify appropriate approval authorities; (3)the organization employs automated mechanisms to highlight approvals that have not been received in a timely manner; (4)the organization employs automated mechanisms to inhibit change until necessary approvals are received; and (5)the organization employs automated mechanisms to document completed changes to the information system. (6)If the organization tests, validates, and documents changes to the information system before implementing the changes on the operational system	Changes to the production environment that are inadequately tested disrupt production environment. Management does not approve changes to the operating environment prior to implementation into production.													{CobiT v5 - High Level Control Objective BAI06}Controls have been defined to manage changes to information systems in order to minimize the likelihood of disruption, unauthorized alterations and errors.
R0045	CONFIGURATION MANAGEMENT	SECURITY IMPACT ANALYSIS	CM-4		Required	Required	Protect -> Secure Configuration Management & Change Management	The organization analyses changes to the information system to determine potential security impacts prior to change implementation.							Are changes to information systems (including those related to procedures, processes, system and service parameters) logged, assessed and authorized prior to implementation and verified to ensure they meet the following implementation (including impact from an information security perspective)?	Obtain configuration management policy; procedures addressing the monitoring of configuration changes to the information system; information system architecture and configuration documentation; change control records; information system audit records; other relevant documents or records and ascertain if : (1)the organization monitors changes to the information system by verifying that the organization-defined types of changes to the information system have gone through change approval process, conducts security impact analyses to assess the effects of the system changes; -after the system is changed (including upgrades and modifications), checks the security features to confirm that the features are still functioning properly; and -audits activities associated with configuration changes to the information system.	Effects from changes to systems or applications are undetected in the production environment.													{CobiT v5 - High Level Control Objective BAI06}Controls have been defined to manage changes to information systems in order to minimize the likelihood of disruption, unauthorized alterations and errors.
R0046	CONFIGURATION MANAGEMENT	ACCESS RESTRICTIONS FOR CHANGE	CM-5			Required (1,3,5)	Protect -> Secure Configuration Management & Change Management Identify - Critical Information Asset Inventory	The organization defines, documents, approves, and enforces physical and logical acc restrictions associated with changes to the information system. Control Enhancements: (1) ACCESS RESTRICTIONS FOR CHANGE	AUTOMATED ACCESS ENFORCEMENT / AUDI The information system enforces access restrictions and supports auditing of the enforcement actions. Supplemental Guidance: Related controls: AU-2, AU-12, AU-6, AU-9, CM-3, CM-6. (3) ACCESS RESTRICTIONS FOR CHANGE	SIGNED COMPONENTS The information system prevents the installation of [Assignment: organization-define software and firmware components] without verification that the component has been digitall signed using a certificate that is recognized and approved by the organization. (5) ACCESS RESTRICTIONS FOR CHANGE	LIMIT PRODUCTION / OPERATIONAL PRIVILES The organization: (a) Limits privileges to change information system components and system-related information within a production or operational environment; and (b) Reviews and revealuates privileges [Assignment: organization-defined frequency]																							{CobiT v5 - High Level Control Objective BAI06}Controls have been defined to manage changes to information systems in order to minimize the likelihood of disruption, unauthorized alterations and errors.
R0047	CONFIGURATION MANAGEMENT	CONFIGURATION SETTINGS	CM-6		Required	Required (1)	Protect -> Secure Configuration Management & Change Management Identify -> Critical Information Asset Inventory	The organization: a. Establishes and documents configuration settings for information technology prod employed within the information system using [State of Arizona Configuration Base (SACB)] that reflect the most restrictive mode consistent with operational requirme b. Implements the configuration settings; c. Identifies, documents, and approves any deviations from established configuration settings for [Assignment: organization-defined information system components] base [Assignment: organization-defined operational requirements]; and d. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures. Control Enhancements: (1) CONFIGURATION SETTINGS	AUTOMATED CENTRAL MANAGEMENT / APPLICATION VERIFICATION The organization employs automated mechanisms to centrally manage, apply, and ve configuration settings for [service provider defined configuration settings]. (2) CONFIGURATION SETTINGS	RESPOND TO UNAUTHORIZED CHANGES The organization employs [service provider defined security safeguards] to respond t unauthorized changes to [Assignment: organization-defined configuration settings].								Does the institution or department have processes in place to monitor and control changes to the baseline configuration settings for information systems in accordance with organizational policies and procedures?	Obtain configuration management policy; procedures addressing configuration settings for the information system; information system configuration settings and associated documentation; NIST Special Publication 800-70; other relevant documents or records and ascertain if: (1)the organization establishes mandatory configuration settings for information technology products employed within the information system; (2)the organization configures the security settings of information technology products to the most restrictive mode consistent with operational requirements. (3)the organization documents the configuration settings. (4)the organization enforces the configuration settings in all components of the information system.	Changes to the production environment are not operating as expected disrupt the production environment.													{CobiT v5 - High Level Control Objective BAI06}Controls have been defined to manage changes to information systems in order to minimize the likelihood of disruption, unauthorized alterations and errors.
R0048	CONFIGURATION MANAGEMENT	LEAST FUNCTIONALITY	CM-7		Required	Required (1,2,5)	Protect -> Secure Configuration Management & Change Management Protect -> Network Access and Perimeter Controls	The organization: a. Configures the information system to provide only essential capabilities; and b. Prohibits or restricts the use of the following functions, ports, protocols, and/or services: [Assignment: organization-defined prohibited or restricted functions, ports, protocols, and/or services]. Control Enhancement: (1) LEAST FUNCTIONALITY	PERIODIC REVIEW The organization: (a) Reviews the information system [Assignment: organization-defined frequency] to identify unnecessary and/or non-secure functions, ports, protocols, and services; and (b) Disables [Assignment: organization-defined functions, ports, protocols, and servic within the information system deemed to be unnecessary and/or non-secure]. (2) LEAST FUNCTIONALITY	PREVENT PROGRAM EXECUTION The information system prevents program execution in accordance with [Selection (o more): [Assignment: organization-defined policies regarding software program usage restrictions]; rules authorizing the terms and conditions of software program usage]. (5) LEAST FUNCTIONALITY	AUTHORIZED SOFTWARE / WHITELISTING The organization: (a) Identifies [Assignment: organization-defined software programs authorized to exe on the information system]; (b) Employs a deny-all, permit-by-exception policy to allow the execution of authoriz programs programs on the information system; and (c) Reviews and updates the list of authorized software programs [Assignment: organization-defined									Does the institution or department's documented policies and procedures include a rationale for providing only essential functionality and restrict the use of functionality, ports, protocols, and/or services based on risk?	Obtain configuration management policy; procedures addressing least functionality in the information system; security plan; information system configuration settings and associated documentation and ascertain if: (1)the organization defines in the security plan, explicitly or by reference, prohibited or restricted functions, ports, protocols, and services for the information system. (2)the organization configures the information system to provide only essential capabilities. (3)the organization configures the information system to specifically prohibit and/or restrict the use of organization-defined functions, ports, protocols, and/or services. (4)the organization defines in the security plan, explicitly or by reference, the frequency of the information system reviews to identify and eliminate unnecessary functions, ports, protocols, and services; and (5)the organization reviews the information system to identify and eliminate unnecessary functions, ports, protocols, and/or services in accordance with organization-defined frequency.	Configuration standards do not exist for systems being implemented.													{CobiT v5 - High Level Control Objective BAI10, BAI10, DSS05}Controls have been defined to manage the configuration of IT hardware and software.

	Security Control Family	Control Name	NIST 800-53 Control #	Low (Control and Control Enhancements)	MODERATE (Control and Control Enhancements)	Security Program Area (Function Area -> Functional Sub-Area)	NIST 800-53 Rev. 4 Control (Control and Control Enhancements) Detailed breakdown of required controls	Vendor's Response (Please Address all the controls and control enhancements in DETAIL Controls and Enhancements identified in Column H)	Overall Control(s) Implementation Status (Reference on Comments Page) Please select from Drop down (Lower right corner)	Where does the Control(s) originate from? Please select from Drop down (Lower right corner)	Supporting Documentation (Policies and procedures must be explicitly referenced (title and date or version) so that it is clear which document is being referred to. Section numbers or similar mechanisms should allow the reviewer to easily find the reference.)	Vendor's Compensating Controls (If Control Can't Be Met - What is the alternative security controls employed by organization)	Vendor Non-Compliance (If you can't meet this control at all please explain why) (Please See Risk Statement for examples of Non-Compliance language Column R)	General Assessment Questions	Detailed Control Testing Procedure(s)	Risk Statement Examples	SOA Policy Number 1	SOA SubSection 1	SOA Policy Number 2	SOA SubSection 2	SOA Policy Number 3	SOA SubSection 3	SOA Policy Number 4	SOA SubSection 4			Arizona Breach Notification A.R.S. § 44-7501	Arizona Computer Tampering A.R.S. § 13-2316	COBIT Reference (Control Objective)
R0049	CONFIGURATION MANAGEMENT	INFORMATION SYSTEM COMPONENT INVENTORY	CM-8	Required	Required (1,3,5)	Identify -> Data Classification Identify -> Critical Information Asset Inventory	The organization: a. Develops and documents an inventory of information system components that: 1. Accurately reflects the current information system; 2. Includes all components within the authorization boundary of the information syst 3. Is at the level of granularity deemed necessary for tracking and reporting; and 4. Includes [Assignment: organization-defined information deemed necessary to achie effective information system component accountability]; and b. Reviews and updates the information system component inventory [At least month Control Enhancement: (1) INFORMATION SYSTEM COMPONENT INVENTORY	UPDATES DURING INSTALLATION REMOVALS The organization updates the inventory of information system components as an inte part of component installations, removals, and information system updates. (3) INFORMATION SYSTEM COMPONENT INVENTORY | AUTOMATED UNAUTHORIZED COMPONENT DETECTION The organization: (a) Employs automated mechanisms [Continuously, using automated mechanisms wit maximum five-minute delay in detection.] to detect the presence of unauthorized hardware, software, and firmware components within the information system; and (b) Takes the following actions when unauthorized components are detected: [Selection (one or more): disables network access by such components; isolates the components notifies [Assignment: organization-defined personnel or roles]]; (5) INFORMATION SYSTEM COMPONENT INVENTORY | NO DUPLICATE ACCOUNTING OF COMPONENTS The organization verifies that all components within the authorization boundary of th information system are not duplicated in other information system inventories.					Does the institution or department assign owner and custodian to all information and IT systems, and is there an approved document which describes and distinguishes the roles and responsibilities of an owner, custodian, and user? 2) Is there a current and accurate inventory of systems, that provides details such as associated owners, location, security requirements, data classification, etc., for the department?	Obtain configuration management policy; procedures addressing information system component inventory information system inventory records; security plan; component installation records; other relevant documents or records and ascertain if : (1)the organization develops and documents an inventory of the components of the information system: (a)it is at the level of granularity deemed appropriate by the organization for the components included in the inventory that are subject to tracking and reporting. (b)it includes any information determined to be necessary by the organization to achieve effective property accountability; (c)it is consistent with the accreditation boundary of the system. (2)the organization maintains the inventory of the components of the information system to reflect the current status of the system: (3)the organization updates the inventory of information system components as an integral part of component installations.	Information and assets associated with information processing facilities are not owned by a designated part of the organization.	8220	6.1.7				

	Security Control Family	Control Name	NIST 800-53 Control #	Low (Control and Control Enhancements)	MODERATE (Control and Control Enhancements)	Security Program Area (Function Area -> Functional Sub-Area)	NIST 800-53 Rev. 4 Control (Control and Control Enhancements) Detailed breakdown of required controls	Vendor's Response (Please Address all the controls and control enhancements in DETAIL. Controls and Enhancements identified in Column H)	Overall Control(s) Implementation Status (Reference on Comments Page) Please select from Drop down (Lower right corner)	Where does the Control(s) originate from? Please select from Drop down (Lower right corner)	Supporting Documentation (Policies and procedures must be explicitly referenced (title and date or version) so that it is clear which document is being referred to. Section numbers or similar mechanisms should allow the reviewer to easily find the	Vendor's Compensating Controls (If Control Can't Be Met - What is the alternative security controls employed by organization)	Vendor Non-Compliance (If you can't meet this control at all please explain why) (Please See Risk Statement for examples of Non-Compliance language Column R)	General Assessment Questions	Detailed Control Testing Procedure(s)	Risk Statement Examples	SOA Policy Number 1	SOA SubSection 1	SOA Policy Number 2	SOA SubSection 2	SOA Policy Number 3	SOA SubSection 3	SOA Policy Number 4	SOA SubSection 4				Arizona Breach Notification A.R.S. § 44-7501	Arizona Computer Tampering A.R.S. § 13-2316	COBIT Reference (Control Objective)
R0060	CONTINGENCY PLANNING	INFORMATION SYSTEM BACKUP	CP-9		**Required**	**Required (1,3)**	Protect -> Contingency Planning	The organization: a. Conducts backups of user-level information contained in the information system [daily incremental; weekly full]; b. Conducts backups of system-level information contained in the information system [daily incremental; weekly full]; c. Conducts backups of information system documentation including security-related documentation [daily incremental; weekly full]; and d. Protects the confidentiality, integrity, and availability of backup information at storage locations. Control Enhancement: (1) INFORMATION SYSTEM BACKUP | TESTING FOR RELIABILITY / INTEGRITY The organization tests backup information [at least annually] to verify media reliability and information integrity. (3) INFORMATION SYSTEM BACKUP | SEPARATE STORAGE FOR CRITICAL INFORMATION The organization stores backup copies of [Assignment: organization-defined critical information system software and other security-related information] in a separate facility or in a fire-rated container that is not collocated with the operational system.			

	Security Control Family	Control Name	NIST 800-53 Control #	Low (Control and Control Enhancements)	MODERATE (Control and Control Enhancements)	Security Program Area (Function Area -> Functional Sub-Area)	NIST 800-53 Rev. 4 Control (Control and Control Enhancements) Detailed breakdown of required controls	Vendor's Response (Please Address all the controls and control enhancements in DETAIL. Controls and Enhancements identified in Column H)	Overall Control(s) Implementation Status (Reference on Comments Page) Please select from Drop down (Lower right corner)	Where does the Control(s) originate from? Please select from Drop down (Lower right corner)	Supporting Documentation (Policies and procedures must be explicitly referenced (title and date or version) so that it is clear which document is being referred to. Section numbers or similar mechanisms should allow the reviewer to easily find the reference.)	Vendor's Compensating Controls (If Control Can't Be Met - What is the alternative security controls employed by organization)	Vendor Non-Compliance (If you can't meet this control at all please explain why) (Please See Risk Statement for examples of Non-Compliance language Column R)	General Assessment Questions	Detailed Control Testing Procedure(s)	Risk Statement Examples	SOA Policy Number 1	SOA SubSection 1	SOA Policy Number 2	SOA SubSection 2	SOA Policy Number 3	SOA SubSection 3	SOA Policy Number 4	SOA SubSection 4			Arizona Breach Notification A.R.S. § 44-7501	Arizona Computer Tampering A.R.S. § 13-2316	COBIT Reference (Control Objective)
R0074	INCIDENT RESPONSE	INCIDENT MONITORING	IR-5	Required	Required	Protect -> Data Loss Prevention Respond -> Cyber-Security Incident Response	The organization tracks and documents information system security incidents.							es the institution or department have a rocess in place to document details of each ncident to support forensics and trend nalysis? [e.g., maintaining records about each ncident, status of the incident, and other ertinent information necessary for forensics, rc.]	Obtain incident response policy; procedures addressing incident monitoring; information system design documentation; information system configuration settings and associated documentation; automated mechanisms supporting incident monitoring; other relevant documents or records and ascertain if the organization employs automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information.	Rules for evidence handling are not followed by when evidence is collected, retained, or presented.	8240	6.5										[Cobit5 v5 - High Level Control Objective Deleted—ITIL 3 does not refer to Service Desk as a process.]Controls have been defined for management of the service desk and incidents.
R0075	INCIDENT RESPONSE	INCIDENT REPORTING	IR-6	Required	Required (1)	Respond -> Cyber-Security Incident Response	The organization: a. Requires personnel to report suspected security incidents to the organizational incident response capability within [Assignment: organization-defined time period]; and b. Reports security incident information to [Assignment: organization-defined authorities]. Control Enhancement: (1) INCIDENT REPORTING | AUTOMATED REPORTING The organization employs automated mechanisms to assist in the reporting of security incidents.								es the institution or department have olicies and effective communications in place hat require and inform employees, contractors nd third-party users of information systems nd services that they must promptly report ny observed or suspected security weaknesses n systems or services, or any suspected or ctual breach of institutional data, in digital or aper format) to their supervisors, Information Security Officer, and/or institution's compliance ntitive?	Obtain incident response policy; procedures addressing incident reporting; NIST Special Publication 800-61; automated mechanisms supporting incident reporting; incident reporting records and documentation; other relevant documents or records and ascertain if : (1)the organization promptly reports incident information to appropriate authorities. (2)Incident reporting is consistent with NIST Special Publication 800-61; (3)weaknesses and vulnerabilities in the information system are reported to appropriate organizational officials in a timely manner to prevent security incidents;	Security events and weaknesses are not detected and corrected due to lack of users reporting the events or weaknesses.	8240	6.6										[Cobit5 v5 - High Level Control Objective Deleted—ITIL 3 does not refer to Service Desk as a process.]Controls have been defined for management of the service desk and incidents.
R0076	INCIDENT RESPONSE	INCIDENT RESPONSE ASSISTANCE	IR-7	Required	Required (1,2)	Respond -> Cyber-Security Incident Response	The organization provides an incident response support resource, integral to the organizational incident response capability that offers advice and assistance to users of the information system for the handling and reporting of security incidents. Control Enhancement: (1) INCIDENT RESPONSE ASSISTANCE | AUTOMATION SUPPORT FOR AVAILABILITY OF INFORMATION / SUPPORT The organization employs automated mechanisms to increase the availability of incident response-related information and support. (2) INCIDENT RESPONSE ASSISTANCE | COORDINATION WITH EXTERNAL PROVIDERS The organization: (a) Establishes a direct, cooperative relationship between its incident response capability and external providers of information system protection capability; and (b) Identifies organizational incident response team members to the external providers.								es the institution or department have ccess, or means of obtaining access quickly, to killed incident response support (e.g., to rform forensics) during an incident? Note: examples may include forensic pecialists in other parts of the institution or xecuted contracts in place with third-parties hat provide such capability]	Obtain incident response policy; procedures addressing incident response assistance; automated mechanisms supporting incident response support and assistance; other relevant documents or records and ascertain if : (1)the organization provides an incident response support resource that offers advice and assistance to users of the information system for the handling and reporting of security incidents. (2)the incident response support resource is an integral part of the organization's incident response capability. (3)the organization employs automated mechanisms to increase the availability of incident response-related information and support for incident response support.	Lack of a Security Incident Response Program may result in improper identification and handling of security events.	8240	6.8										[Cobit5 v5 - High Level Control Objective Deleted—ITIL 3 does not refer to Service Desk as a process.] Controls have been defined for management of the service desk and incidents.
R0077	INCIDENT RESPONSE	INCIDENT RESPONSE PLAN	IR-8	Required	Required	Respond -> Cyber-Security Incident Response	The organization: a. Develops an incident response plan that: 1. Provides the organization with a roadmap for implementing its incident response capability; 2. Describes the structure and organization of the incident response capability; 3. Provides a high-level approach for how the incident response capability fits into the overall organization; 4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions; 5. Defines reportable incidents; 6. Provides metrics for measuring the incident response capability within the organization. 7. Defines the resources and management support needed to effectively maintain and mature an incident response capability; and 8. Is reviewed and approved by [Assignment: organization-defined personnel or roles]; b. Distributes copies of the incident response plan to [Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements]; c. Reviews the incident response plan [at least annually]; d. Updates the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing; e. Communicates incident response plan changes to [Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements]; and f. Protects the incident response plan from unauthorized disclosure and modification.								es the institution or department maintain n effective security Incident Management rocess, that includes: roles and responsibilities, and oversight; a clear and plan for addressing capability hat has been approved by management; a process for ensuring that copies of the ncident response plan are distributed and ade available to incident response personnel; nd d requirements for updating the incident response process and applicable scenarios?	Obtain incident response policy; procedures addressing incident response assistance; incident response plan; other relevant documents or records and ascertain if : (1)the organization develops an incident response plan that: provides the organization with a roadmap for implementing its incident response capability; describes the structure and organization of the incident response capability; provides a high-level approach for how the incident response capability fits into the overall organization; meets the unique requirements of the organization, which relate to mission, size, structure, and functions; defines reportable incidents; provides metrics for measuring the incident response capability within the organization; defines the resources and management support needed to effectively maintain and -mature an incident response capability; and is reviewed and approved by designated officials within the organization	The organization is unable to manage the initial phase of an incident since the plan is not well designed and documented.	8240	6.7										[Cobit5 v5 - High Level Control Objective Deleted—ITIL 3 does not refer to Service Desk as a process.] Controls have been defined for management of the service desk and incidents.
R0078	INCIDENT RESPONSE	**NFORMATION SPILLAGE RESPONSE**	IR-9		Required (1,2,3,4)		The organization responds to information spills by: a. Identifying the specific information involved in the information system contamination; b. Alerting [Assignment: organization-defined personnel or roles] of the information spill using a method of communication not associated with the spill; c. Isolating the contaminated information system or system component; d. Eradicating the information from the contaminated information system or component; e. Identifying other information systems or system components that may have been subsequently contaminated; f. Performing other [Assignment: organization-defined actions]. (1) INFORMATION SPILLAGE RESPONSE | RESPONSIBLE PERSONNEL The organization assigns [Assignment: organization-defined personnel or roles] with responsibility for responding to information spills. (2) INFORMATION SPILLAGE RESPONSE | TRAINING The organization provides information spillage response training [Assignment: organization- defined frequency]. (3) INFORMATION SPILLAGE RESPONSE | POST-SPILL OPERATIONS The organization implements [Assignment: organization-defined procedures] to ensure that organizational personnel impacted by information spills can continue to carry out assigned tasks while contaminated systems are undergoing corrective actions. (4) INFORMATION SPILLAGE RESPONSE | EXPOSURE TO UNAUTHORIZED PERSONNEL The organization employs [Assignment: organization-defined security safeguards] for personnel exposed to information not within assigned access authorizations. Supplemental Guidance: Security safeguards include, for example, making personnel exposed to spilled information aware of the federal laws, directives, policies, and/or regulations regarding the information and the restrictions imposed based on exposure to such information.								es the institution or department have olicies and processes in place to report when ther classified or sensitive nformation is not inadvertently placed on information systems that are not authorized to rocess such information?	Obtain incident response policy; procedures addressing incident response assistance; incident response plan; for information spillage	The organization does not have staff or resources responsible for responding to information spillage												
R0079	MAINTENANCE	SYSTEM MAINTENANCE POLICY AND PROCEDURES	MA-1	Required	Required	Identify-> Enterprise Security Policy, Standards, and Guidelines	The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the system maintenance policy and associated system maintenance controls; and b. Reviews and updates the current: 1. System maintenance policy [at least every 3 years]; and 2. System maintenance procedures [at least annually].								es the institution or department have olicies and procedures in place to maintain ystems in a manner so that security exposure minimized from outdated information ystems (e.g., keeping up system patches as ell as information systems that are still aintained by the vendor)?	Obtain information system maintenance policy and procedures; other relevant documents or records and ascertain if : (1)the organization develops and documents information system maintenance policy and procedures. (2)the organization disseminates information system maintenance policy and procedures to appropriate elements within the organization. (3)responsible parties within the organization periodically review information system maintenance policy and procedures. (4)the organization updates information system maintenance policy and procedures when organizational review indicates updates are required. (5)the information system maintenance policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance (6)the information system maintenance policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and (a)the information system maintenance procedures address all areas identified in the system maintenance policy and address achieving policy-compliant implementations of all associated system maintenance controls.	Commercial software is not supported by a vendor and introduces errors into the information system processing environment	8120	6.2	8220	6.2 - 6.2.4										[Cobit5 v5 - High Level Control Objective BAI03; DSS02Controls have been defined for the acquisition and maintenance of technology infrastructure to ensure that the platforms that support the business applications are aligned with defined IT architecture and technology standards.
R0080	MAINTENANCE	CONTROLLED MAINTENANCE	MA-2	Required	Required	Protect -> Physical and Environmental Protection	The organization: a. Schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements; b. Approves and monitors all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location; c. Requires that [Assignment: organization-defined personnel or roles] explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs; d. Sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs; e. Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions; and f. Includes [Assignment: organization-defined maintenance-related information] in organizational maintenance records.								es the institution or department have ocumented and implemented policies and ractices for maintaining proper security of ystems, equipment, media, and data, in place overed from servers, printers, fax machines, etc.), as well as physical facilities such as doors, ocks, etc., during maintenance, whether on-ite or when removed and taken off-site?	Obtain information system maintenance policy; procedures addressing controlled maintenance for the information system; maintenance records; manufacturer/vendor maintenance specifications; other relevant documents or records and ascertain if: (1)the organization schedules, performs, documents, and reviews records of routine preventative and regular maintenance (including repairs) on the components of the information system in accordance with manufacturer or vendor specifications and/or organizational requirements. (2)the organization maintains maintenance records for the information system that include: (i) the date and time of maintenance; (ii) name of the individual performing the maintenance; (iii) name of escort, if necessary; (iv) a description of the maintenance performed; and (v) a list of equipment removed or replaced (including identification numbers, if applicable).	Unforeseen hardware failures occur due to lack of up to date maintenance records.	8220	6.2.1										[Cobit5 v5 - High Level Control Objective DSS01; DSS02Controls have been defined to manage the physical environment to protect IT assets from access, damage or theft.
R0081	MAINTENANCE	MAINTENANCE TOOLS	MA-3		Required (1,2,3)	Protect -> Physical and Environmental Protection	The organization approves, controls, and monitors information system maintenance tools. Control Enhancement: (1) MAINTENANCE TOOLS | INSPECT TOOLS The organization inspects the maintenance tools carried into a facility by maintenance personnel for improper or unauthorized modifications. (2) MAINTENANCE TOOLS | INSPECT MEDIA The organization checks media containing diagnostic and test programs for malicious code before the media are used in the information system. (3) MAINTENANCE TOOLS | PREVENT UNAUTHORIZED REMOVAL The organization prevents the unauthorized removal of maintenance equipment containing organizational information by: (a) Verifying that there is no organizational information contained on the equipment; (b) Sanitizing or destroying the equipment; (c) Retaining the equipment within the facility; or (d) Obtaining an exemption from [Assignment: organization-defined personnel or roles] explicitly authorizing removal of the equipment from the facility.								es the institution or department have ocumented and implemented policies and ractices for limiting security risk exposure hrough maintenance or diagnostic tools (e.g., n unpatched and unsecure device or ppliance connected to the network etc.) introduced into the institution by third-arties?	Obtain information system maintenance policy; information system maintenance tools and associated documentation; procedures addressing information system maintenance tools; maintenance records; information system media containing maintenance programs (including diagnostic and test programs); other relevant documents or records and ascertain if : (1)the organization maintains maintenance tools on an ongoing basis. (2)the organization inspects all maintenance tools (e.g., diagnostic and test equipment) carried into a facility by maintenance personnel for obvious improper modifications. (3)the organization checks all media containing diagnostic test programs (e.g., software or firmware used for information system maintenance or diagnostics) for malicious code before the media are used in the information system.	Equipment is not available due to improper maintenance.	8220	6.2.2										[Cobit5 v5 - High Level Control Objective DSS01; DSS05Controls have been defined to manage the physical environment to protect IT assets from access, damage or theft.
R0082	MAINTENANCE	NONLOCAL MAINTENANCE	MA-4	Required	Required (2)	Protect -> Network Access and Perimeter Controls	The organization: a. Approves and monitors nonlocal maintenance and diagnostic activities; b. Allows the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information system; c. Employs strong authenticators in the establishment of nonlocal maintenance and diagnostic sessions; d. Maintains records for nonlocal maintenance and diagnostic activities; and e. Terminates session and network connections when nonlocal maintenance is completed. Control Enhancement: (2) NONLOCAL MAINTENANCE | DOCUMENT NONLOCAL MAINTENANCE The organization documents in the security plan for the information system, the policies and procedures for the establishment and use of nonlocal maintenance and diagnostic connections.								es the institution or department have ocumented and implemented policies and ractices to control security exposure from institutional vendors who provide remote upport or maintenance to information ystem(s), through: enabling strong identification and authentication; limiting to ports, services, and access levels needed for business purpose; having appropriate logging enabled for monitoring vendor actions; and a session termination of sessions and network connections when remote maintenance is ompleted?	Obtain information system maintenance policy; procedures addressing remote maintenance for the information system; information system design documentation; information system configuration settings and associated documentation; maintenance records; audit records; security plan; other relevant documents or records and ascertain if : (1)the organization authorizes, monitors, and controls the execution of maintenance and diagnostic activities conducted remotely by individuals communicating through an external, non-organization-controlled network (e.g., the Internet), if employed. (2)the organization documents in the security plan, the remote maintenance and diagnostic tools to be employed. (3)the organization maintains records for all remote maintenance and diagnostic activities. (4)the organization (or information system in certain cases) terminates all sessions and remote connections invoked in the performance of remote maintenance and diagnostic activity when the remote maintenance or diagnostics is completed. (5)the organization changes the passwords following each remote maintenance and diagnostic activity if password-based authentication is used to accomplish remote maintenance. (6)the organization audits all remote maintenance and diagnostic sessions. (7)the organization organizational personnel (as deemed by the organization) review the maintenance records of remote sessions. (8)the organization addresses the installation and use of remote maintenance and diagnostic links in the security plan for the information system.	Unauthorized access is gained through diagnostic and configuration network ports.	8220	6.2.3										[Cobit5 v5 - High Level Control Objective AP013; DSS02; DSS05Controls have been defined to ensure system security by defining IT security policies, procedures and standards, and monitoring, detecting, reporting security vulnerabilities and incidents.
R0083	MAINTENANCE	MAINTENANCE PERSONNEL	MA-5	Required	Required (1)	Protect -> Network Access and Perimeter Controls	The organization: a. Establishes a process for maintenance personnel authorization and maintains a list of authorized maintenance organizations or personnel; b. Ensures that non-escorted personnel performing maintenance on the information system have required access authorizations; and c. Designates organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations. Control Enhancements: (1) NONLOCAL MAINTENANCE | AUDITING AND REVIEW The organization: (a) Audits nonlocal maintenance and diagnostic sessions [Assignment: organization-defined audit events]; and (b) Reviews the records of the maintenance and diagnostic sessions.								es the institution or department have ocumented policies and practices for reventing visitors from physically accessing ensitive areas of the institution through: use of physical controls such as locked doors, requiring management authorization for non-mployees or visitors to enter facilities; requiring visitors to wear a visible badge or ccess device) that expires and that identifies he individual as a non-employee; a use of sign-in sheets or automated visitor ogging; maintenance of records of visits based on institutional records retention schedules?	Obtain information system maintenance policy; procedures addressing maintenance personnel; service provider contracts and/or service level agreements; list of authorized personnel; maintenance records; other relevant documents or records and ascertain if : (1)the organization allows only authorized personnel to perform maintenance on the information system. (2)the organization supervises authorized maintenance personnel who do not have needed access authorizations to the information system during the performance of maintenance activities on the system using organizational personnel with appropriate access authorizations.	Unauthorized visitors gain physical access to facilities due to insufficient physical entry controls.	8220	6.2.4										[Cobit5 v5 - High Level Control Objective DSS01; DSS05Controls have been defined to manage the physical environment to protect IT assets from access, damage or theft.
R0084	MAINTENANCE	TIMELY MAINTENANCE	MA-6		Required	Protect - Network Access and Perimeter Controls	The organization obtains maintenance support and/or spare parts for [Assignment: organization-defined information system components] within [Assignment: organization-defined time period] of failure.								es the institution or department have ecurement maintenance support and/or spare arts for its defined list of security-critical nformation system components and/or key nformation technology components to enable ecovery within a defined time period of failure? [Note: example of security-critical nformation system components can include ntrol management systems like firewalls, and ntrusion systems, badge control systems, etc.]	Obtain information system maintenance policy; procedures addressing timely maintenance for the information system; service provider contracts and/or service level agreements; inventory and availability of spare parts; security plan; other relevant documents or records and ascertain if : (1)the organization defines in the security plan, explicitly or by reference, key information system components. (2)the organization defines in the security plan, explicitly or by reference, the time period within which support and spare parts must be obtained after a failure. (3)the organization obtains maintenance support and spare parts for the organization-defined list of key information system components within the organization-defined time period of failure.	The lack of processes for system maintenance and support may result in compromise of system security due to latest updates not being made to systems in a timely manner.												[Cobit5 v5 - High Level Control Objective BAI03; DSS02Controls have been defined for the acquisition and maintenance of technology infrastructure to ensure that the platforms that support the business applications are aligned with defined IT architecture and technology standards.
R0085	MEDIA PROTECTION	MEDIA PROTECTION POLICY AND PROCEDURES	MP-1	Required	Required	Protect -> Media	The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the media protection policy and associated media protection controls; and b. Reviews and updates the current: 1. Media protection policy [at least every 3 years]; and 2. Media protection procedures [at least annually].								es the institution or department have ocumented and implemented policies and ractices for protecting confidential data ssiding on removable media (e.g., hard-drives, ds, USB drives, backup tapes, etc.)? Note: protection requirements include torage of media, sanitization requirements upon transfer or disposal of media, use of ncryption, etc.).	Obtain media protection policy and procedures; other relevant documents or records and ascertain if : (1)the organization develops and documents media protection policy and procedures. (2)the organization disseminates media protection policy and procedures to appropriate elements within the organization. (3)responsible parties within the organization periodically review media protection policy and procedures. (4)the organization updates media protection policy and procedures when organizational review indicates updates are required. (5)the media protection policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance (6)the media protection policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance. (a)the media protection procedures address all areas identified in the media protection policy and address achieving policy-compliant implementations of all associated media protection controls.	Media (e.g., documents, computer media (e.g. tapes, disks), input/output data, system documentation) is compromised by unauthorized parties due to ineffective handling procedures.	8120	6.2	8250	6.1 - 6.7.2										[Cobit5 v5 - High Level Control Objective DSS01;DSS04;DSS05;DSS06]Controls have been defined to manage data by maintaining the completeness, accuracy, availability and protection of data.
R0086	MEDIA PROTECTION	MEDIA ACCESS	MP-2	Required	Required	Protect -> Media	The organization restricts access to [Assignment: organization-defined types of digital and/or non-digital media] to [Assignment: organization-defined personnel or roles].								es the institution or department have emonstrative, physical, and technical controls n place to manage access to media containing onfidential information?	Obtain information system media protection policy; procedures addressing media access; access control policy and procedures; physical and environmental protection policy and procedures; media storage facilities; access control records; access control records; audit records; other relevant documents or records and ascertain if : (1)the organization restricts access to information system media to authorized users. (2)the organization employs automated mechanisms to restrict access to media storage areas. (3)the organization employs automated mechanisms to audit access attempts and access granted.	Data stored on removable computer media is damaged or disclosed due to ineffective handling procedures.	8250	6.1										[Cobit5 v5 - High Level Control Objective DSS01;DSS04;DSS05;DSS06]Controls have been defined to manage data by maintaining the completeness, accuracy, availability and protection of data.

	Security Control Family	Control Name	NIST 800-53 Control #	Low (Control and Control Enhancements)	MODERATE (Control and Control Enhancements)	Security Program Area (Function Area or Functional Sub-Area)	NIST 800-53 Rev. 4 Control (Control and Control Enhancements) Detailed breakdown of required controls	Vendor's Response (Please Address all the controls and control enhancements in DETAIL Controls and Enhancements identified in Column H)	Overall Control(s) Implementation Status (Reference on Comments Page) Please select from Drop down (Lower right corner)	Where does the Control(s) originate from? Please select from Drop down (Lower right corner)	Supporting Documentation (Policies and procedures must be explicitly referenced (title and date or version) so that it is clear which document is being referred to. Section numbers or similar mechanisms should allow the reviewer to easily find the reference)	Vendor's Compensating Controls (If Control Can't Be Met - What is the alternative security controls employed by organization)	Vendor Non-Compliance (If you can't meet this control at all please explain why) (Please Sex Risk Statement for examples of Non-Compliance language Column R)	General Assessment Questions	Detailed Control Testing Procedure(s)	Risk Statement Examples	SOA Policy Number 1	SOA SubSection 1	SOA Policy Number 2	SOA SubSection 2	SOA Policy Number 3	SOA SubSection 3	SOA Policy Number 4	SOA SubSection 4			Arizona Breach Notification A.R.S. § 44-7501	Arizona Computer Tampering A.R.S. § 13-2316	COBIT Reference (Control Objective)
R0087	MEDIA PROTECTION	MEDIA MARKING	MP-3		Required	Identify -> Data Classification	The organization: a. Marks information system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and b. Exempts [Assignment: organization-defined types of information system media] from marking as long as the media remain within [no removable media types]							es the institution or department plemented procedures to label and handle media containing departmental data in ordance with institutional data classification licy and procedures?	Obtain information system media protection policy; procedures addressing media labeling; physical and environmental protection policy and procedures; security plan; removable storage media and information system output; other relevant documents or records and ascertain if : (i)the organization defines in the security plan, explicitly or by reference, its protected environment for media labeling requirements. (ii)the organization defines in the security plan, explicitly or by reference, media types and hardware components that are exempted from external labeling requirements. (iii)the organization affixes external labels to removable information storage media and information system output not otherwise exempted from this labeling requirement, indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information.	Information is disclosed due to mislabeled, unlabeled or mishandled physical or electronic media.	8250	6.2												COBIT v5 - High Level Control Objective DSS01;DSS04;DSS05;DSS06]Controls have been defined to manage data by maintaining the completeness, accuracy, availability and protection of data.
R0088	MEDIA PROTECTION	MEDIA STORAGE	MP-4		Required	Identify -> Data Classification Protect -> Media	The organization: a. Physically controls and securely stores [all types of digital and non-digital media with sensitive information] within [Assignment: organization-defined controlled areas]; and b. Protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.							es the institution or department's media ntrolling procedures address: proper storage and physical security of digital d non-digital media (e.g., backup tapes, ident & patent records, etc.); destruction or sanitization of media using proved equipment, techniques, and ocedures; and other requirements for media handling, ed on any institution or department's data ssification schema?	Obtain information system media protection policy; procedures addressing media storage; physical and environmental protection policy and procedures; access control policy and procedures; security plan; information system media; other relevant documents or records and ascertain if : (i)the organization selects and documents the media and associated information contained on that media requiring physical protection in accordance with an organizational assessment of risk. (ii)the organization defines the specific measures used to protect the selected media and information contained on that media. (iii)the organization physically controls and securely stores information system media within controlled areas. (iv)the organization protects information system media commensurate with the FIPS 199 security categorization of the information contained on the media.	The lack of formal procedures for handling, processing, storing and communicating information consistent with its classification scheme, may result in potential mishandling or misuse of information by unauthorized parties.	8250	6.3												COBIT v5 - High Level Control Objective DSS01;DSS04;DSS05;DSS06]Controls have been defined to manage data by maintaining the completeness, accuracy, availability and protection of data.
R0089	MEDIA PROTECTION	MEDIA TRANSPORT	MP-5		Required (4)	Protect -> Media	The organization: a. Protects and controls [all media with sensitive information] during transport outside of controlled areas using [prior to leaving secured/controlled environment: for digital media, encryption using a FIPS 140-2 validated encryption module; for non-digital media, secured in locked container]; b. Maintains accountability for information system media during transport outside of controlled areas; c. Documents activities associated with the transport of information system media; and d. Restricts the activities associated with the transport of information system media to authorized personnel. Control Enhancement: (4) MEDIA TRANSPORT	CRYPTOGRAPHIC PROTECTION The information system implements cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.								es the institution or department plemented procedures to protect media in nsport which include logging and monitoring edia transfers, encryption of confidential ata, and use of secured couriers? ote: a common example of media in transit es include backup tapes, mobile devices like ptops and PDAs].	Obtain information system media protection policy; procedures addressing media transport; physical and environmental protection policy and procedures; audit records; access control policy and procedures; security plan; list of organization-defined personnel authorized to transport information system media outside of controlled areas; information system media; information system media transport records; information system audit records; other relevant documents or records and ascertain if : (i)the organization identifies personnel authorized to transport information system media outside of controlled areas. (ii)the organization documents, in policy and procedures, the media requiring protection during transport and the specific measures taken to protect such transported media. (iii)the organization protects and controls information system media during transport outside of controlled areas. (iv)the organization restricts the activities associated with transport of information system media to authorized personnel. (v)the organization defines in the security plan, explicitly or by reference, a system of records for documenting activities associated with the transport of information system media. (vi)the organization documents, where appropriate, activities associated with the transport of information system media using the organization-defined system of records. (vii)the organization employs cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.	Information stored in physical media may be disclosed to or altered by unauthorized parties while being physically transported.	8250	6.5												COBIT v5 - High Level Control Objective DSS01; DSS05]Controls have been defined to manage the physical environment to protect IT assets from access, damage or theft
R0090	MEDIA PROTECTION	MEDIA SANITIZATION	MP-6		Required Required (2)	Protect -> Media	The organization: a. Sanitizes [Assignment: organization-defined information system media] prior to disposal, release out of organizational control, or release for reuse using [Assignment: organization-defined sanitization techniques and procedures] in accordance with applicable federal and organizational standards and policies; and b. Employs sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information. Control Enhancement: (2) MEDIA SANITIZATION	EQUIPMENT TESTING The organization tests sanitization equipment and procedures [At least annually] to verify that the intended sanitization is being achieved.								es the institution or department plemented procedures to dispose of media ntaining departmental data in a manner that equately protects the confidentiality of the ata and renders it unrecoverable (e.g., re- writing or modifying the electronic media make it unreadable or indecipherable or herwise physically destroying the electronic edia), and in accordance with institutional ecords retention schedules?	Obtain information system media protection policy; procedures addressing media sanitization and disposal; NIST Special Publication 800-88; media sanitization records; audit records; other relevant documents or records and ascertain if : (i) the organization identifies information system media requiring sanitization and the appropriate sanitization techniques and procedures to be used in the process. (ii)the organization sanitizes identified information system media, both paper and digital, prior to disposal or release for reuse. (iii)information system media sanitation is consistent with NIST Special Publication 800-88.	Data stored on disposed of media is inappropriately disclosed to unauthorized parties due to ineffective data disposal procedures.	8250	6.6												COBIT v5 - High Level Control Objective DSS01;DSS04;DSS05;DSS06]Controls have been defined to manage data by maintaining the completeness, accuracy, availability and protection of data.
R0091	MEDIA PROTECTION	MEDIA USE	MP-7		Required Required (1)	Protect -> Media	The organization [Selection: restricts; prohibits] the use of [Assignment: organization-defined types of information system media] on [Assignment: organization-defined information systems or system components] using [Assignment: organization-defined security safeguards]; Control Enhancement: (1) MEDIA USE	PROHIBIT USE WITHOUT OWNER The organization prohibits the use of portable storage devices in organizational information systems when such devices have no identifiable owner.							es the institution or department have cumented policies and supporting processes restrict unauthorized information system edia within its environment?	Obtain procedures relating to media use and ascertain if: (i) security safeguards ensure that prohibited or restricted media are not used on information systems; and (ii) portable storage devices with no identifiable owner are not used on information systems.	Inadequate procedures for handling media (disclosure, modification, removal, and destruction) may result in potential compromise of information by unauthorized parties.	8250	6.7												COBIT v5 - High Level Control Objective DSS01;DSS04;DSS05;DSS06]Controls have been defined to manage data by maintaining the completeness, accuracy, availability and protection of data.
R0092	PHYSICAL AND ENVIRONMENTAL PROTECTION	PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES	PE-1		Required	Protect -> Physical and Environmental Protection	The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls; and b. Reviews and updates the current: 1. Physical and environmental protection policy [at least every 3 years]; and 2. Physical and environmental protection procedures [at least annually].							es the institution or department have in ce documented policies and supporting ocedures to protect institutional facilities sed on their criticality, and implement hysical access safeguards to ensure propriate granting, controlling, and onitoring of physical access to institutional cilities?	Obtain physical and environmental protection policy and procedures and ascertain if : (i)the organization develops and documents physical and environmental protection policy and procedures. (ii)the organization disseminates physical and environmental protection policy and procedures to appropriate elements within the organization. (iii)responsible parties within the organization periodically review physical and environmental protection policy and procedures. (iv)the organization updates physical and environmental protection policy and procedures when organizational review indicates updates are required. (v)the physical and environmental protection policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance (vi)the physical and environmental protection policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance. (vii)the physical and environmental protection procedures address all areas identified in the physical and environmental protection policy and address achieving policy-compliant implementations of all associated physical and environmental protection controls.	Unauthorized parties have access to facilities due to security flaws in physical layout.	8120	6.2	8260	6.1 - 6.13										COBIT v5 - High Level Control Objective DSS01; DSS05]Controls have been defined to manage the physical environment to protect IT assets from access, damage or theft
R0093	PHYSICAL AND ENVIRONMENTAL PROTECTION	PHYSICAL ACCESS AUTHORIZATIONS	PE-2		Required	Protect -> Physical and Environmental Protection	The organization: a. Develops, approves, and maintains a list of individuals with authorized access to the facility where the information system resides; b. Issues authorization credentials for facility access; c. Reviews the access list detailing authorized facility access by individuals [at least annually]; and d. Removes individuals from the facility access list when access is no longer required.							es the institution or department established d does it enforce associated access quirements of institutional facilities that ouse systems and confidential data based on cross requirements or function? [e.g., ere student or patient records are ntained] based on business requirements function? ote: this is about formally defining and forcing who can access a specific facility sed on business needs].	Obtain physical and environmental protection policy; procedures addressing physical access authorizations; authorized personnel access list; authorization credentials; other relevant documents or records and ascertain if : (i)the organization identifies areas within the facility that are publicly accessible. (ii)the organization defines in the security plan, explicitly or by reference, the frequency of review and approval for the physical access list and authorization credentials for the facility and the frequency is at least annually. (iii)the organization develops and keeps current lists of personnel with authorized access to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible) (iv)the organization issues appropriate authorization credentials (e.g., badges, identification cards, smart cards) (v)designated officials within the organization review and approve the access list and authorization credentials in accordance with organization-defined frequency.	Unauthorized parties gain physical access to facilities due to insufficient physical entry controls.	8260	6.1												COBIT v5 - High Level Control Objective DSS01; DSS05]Controls have been defined to manage the physical environment to protect IT assets from access, damage or theft
R0094	PHYSICAL AND ENVIRONMENTAL PROTECTION	PHYSICAL ACCESS CONTROL	PE-3		Required	Protect -> Physical and Environmental Protection Protect -> Network Access and Perimeter Controls	The organization: a. Enforces physical access authorizations at [Assignment: organization-defined entry/exit points to the facility where the information system resides] by; 1. Verifying individual access authorizations before granting access to the facility; and 2. Controlling ingress/egress to the facility using [Selection (one or more): [Cloud Service Provider (CSP) defined physical access control systems/devices AND guards]; guards]]; b. Maintains physical access audit logs for [Assignment: organization-defined entry/exit points]; c. Provides [Assignment: organization-defined security safeguards] to control access to areas within the facility officially designated as publicly accessible; d. Escorts visitors and monitors visitor activity [in all circumstances within restricted access area where the information system resides]; e. Secures keys, combinations, and other physical access devices; f. Inventories [Assignment: organization-defined physical access devices] every [at least annually]; and g. Changes combinations and keys [at least annually] and/or when keys are lost, combinations are compromised, or individuals are transferred or terminated.							es the institution or department have propriate processes in place to control ccess through designated entry/exit points to the facility, and to restrict access to a limited number of physical points of entry to the facility; protecting the system that manages control entry/exit (e.g., restricting system access to a badge system); and monitoring for events that indicate ntential unauthorized access attempts to the cility (e.g., unsuccessful badge attempts, loss physical key, etc.)?	Obtain physical and environmental protection policy; procedures addressing physical access control; physical access control logs or records; maintenance records; records of key and lock combination changes; storage locations for keys and access devices; FIPS 201; NIST Special Publications 800-73, 800-76, and 800-78; information system design documentation; other relevant documents or records and ascertain if : (i)the organization controls all physical access points (including designated entry/exit points) to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible). (ii)the organization verifies individual access authorizations before granting access to the facility. (iii)the organization also controls access to areas officially designated as publicly accessible, as appropriate, in accordance with the organization's assessment of risk. (iv)the organization uses physical access devices (e.g., keys, locks, combinations, card readers) and/or guards to control entry to facilities containing information systems. (v)the organization secures and regularly inventories keys, combinations, and other access devices. (vi)the organization changes combinations and keys periodically, and when keys are lost, combinations are compromised, or individuals are transferred or terminated (vii)the access control system is consistent with FIPS 201 and NIST Special Publication 800-73 [where the federal Personal Identity Verification (PIV) credential is used as an identification token and token-based access control function applies]. (viii)the access control system is consistent with NIST Special Publication 800-73 [where the token-based access control function employs cryptographic verification]; and (ix)the access control system is consistent with NIST Special Publication 800-76 [where the token-based access control function employs biometric verification].	Unauthorized parties gain physical access to facilities due to insufficient physical perimeter controls.	8260	6.2, 6.3												COBIT v5 - High Level Control Objective DSS01; DSS05]Controls have been defined to manage the physical environment to protect IT assets from access, damage or theft
R0095	PHYSICAL AND ENVIRONMENTAL PROTECTION	ACCESS CONTROL FOR TRANSMISSION MEDIUM	PE-4		Required	Protect -> Physical and Environmental Protection	The organization controls physical access to [Assignment: organization-defined information system distribution and transmission lines] within organizational facilities using [Assignment: organization-defined security safeguards].							es the institution or department plemented appropriate physical controls to strict access to, and prevent tampering of etwork jacks, wireless access points, and other ayers of access to the institutional network?	Obtain physical and environmental protection policy; procedures addressing access control for transmission medium; information system design documentation; facility communications and wiring diagrams; other relevant documents or records and ascertain if the organization controls physical access to information system distribution and transmission lines within organizational facilities.	Physical equipment is compromised due to the lack of protection from environmental threats and hazards.	8260	6.6.1												COBIT v5 - High Level Control Objective DSS01; DSS05]Controls have been defined to manage the physical environment to protect IT assets from access, damage or theft
R0096	PHYSICAL AND ENVIRONMENTAL PROTECTION	ACCESS CONTROL FOR OUTPUT DEVICES	PE-5		Required	Protect -> Physical and Environmental Protection	The organization controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output.							es the institution or department documented d implemented physical safeguards to otect sensitive documents and/or output vices (e.g., special forms, negotiable cuments, special-purpose printers or curity tokens)?	Obtain physical and environmental protection policy; procedures addressing access control for display medium; facility layout of information system components; actual display from information system components; other relevant documents or records and ascertain if the organization controls physical access to information system devices that display information to prevent unauthorized individuals from observing the display output.	Appropriate physical safeguards have not been established to protect sensitive documents and/or output devices.	8260	6.6.3												COBIT v5 - High Level Control Objective DSS01; DSS05; BAI09]Controls have been defined to manage operations through establishment of service levels for processing, storing, producing, producing sensitive output, and monitoring and maintaining infrastructure.
R0097	PHYSICAL AND ENVIRONMENTAL PROTECTION	MONITORING PHYSICAL ACCESS	PE-6		Required Required (1)	Protect -> Physical and Environmental Protection	The organization: a. Monitors physical access to the facility where the information system resides to detect and respond to physical security incidents; b. Reviews physical access logs [at least monthly] and upon occurrence of [Assignment: organization-defined events or potential indications of events]; and c. Coordinates results of reviews and investigations with the organizational incident response capability. Control Enhancement: (1) MONITORING PHYSICAL ACCESS	INTRUSION ALARMS / SURVEILLANCE EQUIPMENT The organization monitors physical intrusion alarms and surveillance equipment.							es the institution or department have in ce documented standards and procedures ontrolling and monitoring physical access to ese areas periodically, and retain logs in ccordance with institutional records retention hedules?	Obtain physical and environmental protection policy; procedures addressing physical access monitoring; physical access logs or records; intrusion alarm/surveillance equipment logs or records; and ascertain if : (i)the organization monitors physical access to the information system to detect and respond to physical security incidents. (ii)the organization monitors real-time intrusion alarms and surveillance equipment.	Unauthorized parties have inappropriate physical access to all rooms and offices of a facility.	8260	6.4												COBIT v5 - High Level Control Objective DSS01; DSS05]Controls have been defined to manage the physical environment to protect IT assets from access, damage or theft
R0098	PHYSICAL AND ENVIRONMENTAL PROTECTION	VISITOR ACCESS RECORDS	PE-8		Required Required	Protect -> Physical and Environmental Protection Protect -> Network Access and Perimeter Controls	The organization: a. Maintains visitor access records to the facility where the information system resides for [for a minimum of one year]; and b. Reviews visitor access records [at least monthly].							es the institution or department have in ce documented standards and procedures ontrolling and monitoring physical access to ese areas periodically, and retain logs in ccordance with institutional records retention hedules?	Obtain physical and environmental protection policy; procedures addressing facility access records; security plan; facility access control records; other relevant documents or records and ascertain if : (i)the organization defines in the security plan, explicitly or by reference, the frequency of review for visitor access records. (ii)the organization maintains visitor access records to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible) that includes: -name and organization of the person visiting; -signature of the visitor; -form of identification; -date of access; -time of entry and departure; -purpose of visit; -name and organization of person visited . (iii)designated officials within the organization review the visitor access logs in accordance with organization-defined frequency	Failure to protect facilities through sufficient physical entry controls may result in unauthorized parties accessing the organization's facilities.	8260	6.5												COBIT v5 - High Level Control Objective DSS01; DSS05]Controls have been defined to manage the physical environment to protect IT assets from access, damage or theft
R0099	PHYSICAL AND ENVIRONMENTAL PROTECTION	POWER EQUIPMENT AND CABLING	PE-9		Required	Protect -> Physical and Environmental Protection Protect -> Network Access and Perimeter Controls	The organization protects power equipment and power cabling for the information system from damage and destruction.							es the institution or department have ocies and procedures for the physical curity and protection of information systems, ower equipment, and power cabling?	Obtain physical and environmental protection policy; procedures addressing power equipment and cabling protection; facility housing power equipment and cabling; other relevant documents or records and ascertain if the organization protects power equipment and power cabling for the information system from damage and destruction.	Unauthorized access to information resources is obtained through tapping into inappropriately exposed cabling infrastructure.	8260	6.6.5												COBIT v5 - High Level Control Objective DSS01; DSS05]Controls have been defined to manage the physical environment to protect IT assets from access, damage or theft
R0100	PHYSICAL AND ENVIRONMENTAL PROTECTION	EMERGENCY SHUTOFF	PE-10		Required	Protect -> Physical and Environmental Protection Protect -> Network Access and Perimeter Controls Protect -> Business Continuity Risks	The organization: a. Provides the capability of shutting off power to the information system or individual system components in emergency situations; b. Places emergency shutoff switches or devices in [Assignment: organization-defined location by information system or system components] to facilitate safe and easy access to personnel; and c. Protects emergency power shutoff capability from unauthorized activation.							Does the institution or department have in ce procedures and controls to safely shutoff e power to institutional data centers, server oms, and other areas containing information stems in case of an emergency? Are controls in place to ensure authorized ess and activation?	Obtain physical and environmental protection policy; procedures addressing power source emergency shutoff; emergency shutoff controls or switches; other relevant documents or records and ascertain if : (i)the organization identifies the specific locations within a facility containing concentrations of information system resources (e.g., data centers, server rooms, mainframe rooms) (ii)the organization provides, for specific locations within a facility containing concentrations of information system resources, the capability of shutting off power to any information system component that may be malfunctioning or threatened without endangering personnel by requiring them to approach the equipment.	Utility outages disrupt business systems.	8260	6.7.1												COBIT v5 - High Level Control Objective DSS01; DSS05]Controls have been defined to manage the physical environment to protect IT assets from access, damage or theft
R0101	PHYSICAL AND ENVIRONMENTAL PROTECTION	EMERGENCY POWER	PE-11		Required	Protect -> Physical and Environmental Protection Protect -> Network Access and Perimeter Controls	The organization provides a short-term uninterruptible power supply to facilitate [Selection (one or more): an orderly shutdown of the information system; transition of the information system to long-term alternate power]in the event of a primary power source loss.							Does the institution or department have cesses and mechanisms in place, to cilitate an orderly shutdown of the formation system in the event of a primary wer source loss? Have they been tested?	Obtain physical and environmental protection policy; procedures addressing emergency power; uninterruptible power supply documentation; other relevant documents or records and ascertain if :the organization provides a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system in the event of a primary power source loss.	The lack of adequate plans and operational controls to support power contingency mechanisms may lead to potential disruptions of equipment supporting critical business operations.	8260	6.7.2												COBIT v5 - High Level Control Objective DSS01; DSS05]Controls have been defined to manage the physical environment to protect IT assets from access, damage or theft
R0102	PHYSICAL AND ENVIRONMENTAL PROTECTION	EMERGENCY LIGHTING	PE-12		Required Required	Protect -> Physical and Environmental Protection	The organization employs and maintains automatic emergency lighting for the information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.							es the institution or department have in ce procedures and controls to ensure undant power supply to institutional data nters, server rooms, and other areas ntaining information systems and to provide ergency lighting in the event of an ergency or power outage?	Obtain physical and environmental protection policy; procedures addressing emergency lighting; emergency lighting documentation; emergency lighting test records; emergency exits and evacuation routes; other relevant documents or records and ascertain if : (i)the organization employs automatic emergency lighting that activates in the event of a power outage or disruption. (ii)the organization employs automatic emergency lighting that covers emergency exits and evacuation routes (iii)the organization maintains the automatic emergency lighting.	The lack of automatic emergency lighting during power outage or disruption may potentially disrupt continuity of business functions.	8260	6.8												COBIT v5 - High Level Control Objective DSS01; DSS05]Controls have been defined to manage the physical environment to protect IT assets from access, damage or theft
R0103	PHYSICAL AND ENVIRONMENTAL PROTECTION	FIRE PROTECTION	PE-13		Required Required (2,3)	Protect -> Physical and Environmental Protection	The organization employs and maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source. Control Enhancement: (2) FIRE PROTECTION | SUPPRESSION DEVICES / SYSTEMS The organization employs fire suppression devices/systems for the information system that provide automatic notification of any activation to Assignment: organization-defined personnel or roles] and [Assignment: organization-defined emergency responders]. (3) FIRE PROTECTION | AUTOMATIC FIRE SUPPRESSION The organization employs an automatic fire suppression capability for the information system when the facility is not staffed on a continuous basis.							Has the institution or department deployed propriate fire suppression equipment to otect institutional data centers, server oms, and other areas containing information stems in the event of a fire? Has staff received training in appropriate ponse in case of emergencies and use of fire pression equipment?	Obtain physical and environmental protection policy; procedures addressing fire protection; fire suppression and detection devices/systems; fire suppression and detection devices/systems documentation; test records of fire suppression and detection devices/systems; facility housing the information system; alarm service level agreements; facility staffing plans; other relevant documents or records and ascertain if : (i)the organization employs and maintains fire suppression and detection devices/systems that can be activated in the event of a fire. (ii)the organization employs fire detection devices/systems that, without manual intervention, notify the organization and emergency responders in the event of a fire. (iii)the organization employs fire suppression devices/systems that provide automatic notification of any activation to the organization and emergency responders. (iv)the organization employs an automatic fire suppression capability in facilities that are not staffed on a continuous basis.	External and/or environmental threats (e.g., fire, flood, earthquake, civil unrest) disrupt operations due to inadequate physical security controls.	8260	6.9												COBIT v5 - High Level Control Objective DSS01; DSS05]Controls have been defined to manage the physical environment to protect IT assets from access, damage or theft

	Security Control Family	Control Name	NIST 800-53 Control #	Low (Control and Control Enhancements)	MODERATE (Control and Control Enhancements)	Security Program Area (Function Area or Functional Sub-Area)	NIST 800-53 Rev. 4 Control (Control and Control Enhancements) Detailed breakdown of required controls	Vendor's Response (Please Address all the controls and control enhancements in DETAIL. Controls and Enhancements identified in Column H)	Overall Control(s) Implementation Status (Reference on Comments Page) Please select from Drop down (Lower right corner)	Where does the Control(s) originate from? Please select from Drop down (Lower right corner)	Supporting Documentation (Policies and procedures must be explicitly referenced (title and date or version) so that it is clear which document is being referred to. Section numbers or similar mechanisms should allow the reviewer to easily find the reference.)	Vendor's Compensating Controls (If Control Can't Be Met - What is the alternative security controls employed by organization)	Vendor Non-Compliance (If you can't meet this control at all please explain why) (Please See Risk Statement for examples of Non-Compliance language Column R)	General Assessment Questions	Detailed Control Testing Procedure(s)	Risk Statement Examples	SOA Policy Number 1	SOA SubSection 1	SOA Policy Number 2	SOA SubSection 2	SOA Policy Number 3	SOA SubSection 3	SOA Policy Number 4	SOA SubSection 4				Arizona Breach Notification A.R.S. § 44-7501	Arizona Computer Tampering A.R.S. § 13-2316	COBIT Reference (Control Objective)
RI0104	PHYSICAL AND ENVIRONMENTAL PROTECTION	TEMPERATURE AND HUMIDITY CONTROLS	PE-14		**Required**	**Required (2)**	Protect -> Physical and Environmental Protection	The organization: a. Maintains temperature and humidity levels within the facility where the information system resides at [consistent with American Society of Heating, Refrigerating and Air-conditioning Engineers (ASHRAE) document entitled Thermal Guidelines for Data Processing Environments]; and b. Monitors temperature and humidity levels [continuously]. Control Enhancement: (2) TEMPERATURE AND HUMIDITY CONTROLS	MONITORING WITH ALARMS / NOTIFICATIONS The organization employs temperature and humidity monitoring that provides an alarm or notification of changes potentially harmful to personnel or equipment.							es the institution or department have mperature and humidity controls to monitor d maintain acceptable temperature and midity levels in environmental institutional ta centers, server rooms, and other areas ntaining information systems?	Obtain physical and environmental protection policy procedures addressing temperature and humidity control; facility housing the information system; temperature and humidity controls; temperature and humidity controls documentation; temperature and humidity records; other relevant documents or records and ascertain if: (i)the organization regularly maintains, within acceptable levels, the temperature and humidity within the facility where the information system resides. (ii)the organization regularly monitors the temperature and humidity within the facility where the information system resides.	Internal and/or environmental threats (e.g., fire, flood, earthquake, civil unrest) disrupt operations due to inadequate physical security controls.	8260	6.10												CobiT v5 - High Level Control Objective DSS01; DSS05Controls have been defined to manage the physical environment to protect IT assets from access, damage or theft
RI0105	PHYSICAL AND ENVIRONMENTAL PROTECTION	WATER DAMAGE PROTECTION	PE-15		**Required**	**Required**	Protect -> Physical and Environmental Protection	The organization protects the information system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.							es the institution or department have cumented processes and mechanisms to- tect water leakage within institutional data ntes, server rooms, and other areas ntaining information systems; use water shutoff valves to prevent water ter damage to institutional data centers, ms, and other areas containing information stems in the event of water leakage; and perform periodic checks of the accessibility d functioning of shutoff valves?	Obtain physical and environmental protection policy procedures addressing water damage protection; facility housing the information system; master shutoff values; list of key personnel with knowledge of location and activation procedures for master shutoff values for the plumbing system; master shutoff value documentation; other relevant documents or records and ascertain if : (i)the organization protects the information system from water damage resulting from broken plumbing lines or other sources of water leakage by providing master shutoff values that are accessible and working properly. (ii)key personnel within the organization have knowledge of the master water shutoff values.	Information systems are compromised due to the lack of protection from environmental threats and hazards.	8260	6.11												CobiT v5 - High Level Control Objective DSS01; DSS05Controls have been defined to manage the physical environment to protect IT assets from access, damage or theft
RI0106	PHYSICAL AND ENVIRONMENTAL PROTECTION	DELIVERY AND REMOVAL	PE-16		**Required**	**Required**	Protect -> Physical and Environmental Protection	The organization authorizes, monitors, and controls [Assignment: organization-defined types of information system components] entering and exiting the facility and maintains records of those items.							es the institution or department assessed whether physical security to sensitive areas; g., data center, server room, student or ployee records room, etc.) can be numerated?	Obtain physical and environmental protection policy; procedures addressing delivery and removal of information system components from the facility; facility housing the information system; records of items entering and exiting the facility; other relevant documents or records and ascertain if : (i)the organization authorizes and controls information system-related items (i.e., hardware, firmware, software) entering and exiting the facility. (ii)the organization maintains appropriate records of items entering and exiting the facility.	Unauthorized parties gain physical access to critical or sensitive information processing facilities due to inadequate physical security policies and standards.	8260	6.12												CobiT v5 - High Level Control Objective DSS01; DSS05Controls have been defined to manage the physical environment to protect IT assets from access, damage or theft
RI0107	PHYSICAL AND ENVIRONMENTAL PROTECTION	ALTERNATE WORK SITE	PE-17			**Required**	Protect -> Contingency Planning	The organization: a. Employs [Assignment: organization-defined security controls] at alternate work sites; b. Assesses as feasible, the effectiveness of security controls at alternate work sites; and c. Provides a means for employees to communicate with information security personnel in case of security incidents or problems.							es the institution or department documented d implemented policies for physical security quirements for alternative workstes (e.g., DR covery site)?	Obtain physical and environmental protection policy; procedures addressing alternate work sites for organizational personnel; list of management, operational, and technical security controls required for alternate work sites; other relevant documents or records and ascertain if the organization employs appropriate management, operational, and technical information system security controls at alternate work sites.	Unauthorized parties gain physical access to critical or sensitive information processing facilities due to inadequate physical security policies and standards.	8260	6.13												CobiT v5 - High Level Control Objective DSS04; Controls have been defined to ensure continuous service by building resilience into automated solutions and developing, maintaining and testing IT continuity plans.
RI0108	PLANNING	SECURITY PLANNING POLICY AND PROCEDURES	PL-1		**Required**	**Required**	Identify -> Enterprise Security Policy, Standards and Guidelines	The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the security planning policy and associated security planning controls; and b. Reviews and updates the current: 1. Security planning policy [at least every three years]; and 2. Security planning procedures [at least annually].							es the institution or department have a ocess in place to periodically identify and ew information security mission, purpose, les, scope, responsibilities, skills, key ntatives, etc.?	Obtain security planning policy and procedures; other relevant documents or records and ascertain if : (i)the organization develops and documents security planning policy and procedures. (ii)the organization disseminates security planning policy and procedures to appropriate elements within the organization. (iii)responsible parties within the organization periodically review security planning policy and procedures. (iv)the organization updates security planning policy and procedures when organizational review indicates updates are required. (v)the security planning policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance. (vi)the security planning policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance. (vii)the security planning procedures address all areas identified in the security planning policy and address achieving policy-compliant implementations of all associated security planning controls.	Information security is not defined in a framework within the organizational environment.	8120	6.2												CobiT v5 - High Level Control Objective EDM03; APO01Controls have been defined to communicate management aims and direction through providing accurate, understandable and approved policies, procedures, guidelines and other documentation to stakeholders, embedded in an IT control framework.
RI0109	PLANNING	SYSTEM SECURITY PLAN	PL-2		**Required**	**Required (3)**	Identify -> Enterprise Security Policy, Standards and Guidelines	The organization: a. Develops a security plan for the information system that: 1. Is consistent with the organization's enterprise architecture; 2. Explicitly defines the authorization boundary for the system; 3. Describes the operational context of the information system in terms of missions and business processes; 4. Provides the security categorization of the information system including supporting rationale; 5. Describes the operational environment for the information system and relationships with or connections to other information systems; 6. Provides an overview of the security requirements for the system; 7. Identifies any relevant overlays, if applicable; 8. Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions; and 9. Is reviewed and approved by the authorizing official or designated representative prior to plan implementation; b. Distributes copies of the security plan and communicates subsequent changes to the plan to: [at least annually]; c. Reviews the security plan for the information system [Assignment: organization-defined frequency]; d. Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments; and e. Protects the security plan from unauthorized disclosure and modification. Control Enhancement: (3) SYSTEM SECURITY PLAN	PLAN / COORDINATE WITH OTHER ORGANIZATIONAL ENTITIES						es the institution or department develop d maintain information security plan for the formation system(s) that includes, but not ited to: Description of the system environment and ntitlements Interfaces and data flow System classification based on type of formation and business process supported Security controls designed, configured, and plemented ote: these may be maintained in an asset gister that has details of the information stem)	Obtain security planning policy; procedures addressing security plan development and implementation; NIST Special Publication 800-18; security plan for the information system; other relevant documents or records and ascertain if : (i)the organization develops and implements a security plan for the information system. (ii)the security plan provides an overview of the security requirements for the information system and a description of the security controls in place or planned for meeting those requirements. (iii)the organization defines in the security plan, explicitly or by reference, the values for all organization-defined parameters (i.e., assignment and selection operations) in applicable security controls and control enhancements. (iv)the security plan development is consistent with NIST Special Publication 800-18. (v)the security plan is consistent with the organization's information system architecture and information security architecture. (vi)designated organizational officials review and approve the security plan.	Management does not have a documented security plan.	8120	6.1.1												CobiT v5 - High Level Control Objective APO01;APO03Controls have been established for defining the IT processes, organization and relationships to be responsive to business strategy and comply with governance requirements
RI0110	PLANNING	RULES OF BEHAVIOR	PL-4		**Required**	**Required (1)**	Identify -> Data Classification Protect -> Media	The organization: a. Establishes and makes readily available to individuals requiring access to the information system, the rules that describe their responsibilities and expected behavior with regard to information and information system usage; b. Receives a signed acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system; c. Reviews and updates the rules of behavior [At least every 3 years]; and d. Requires individuals who have signed a previous version of the rules of behavior to read and resign when the rules of behavior are revised/updated. Control Enhancement: (1) RULES OF BEHAVIOR | SOCIAL MEDIA AND NETWORKING RESTRICTIONS The organization includes in the rules of behavior, explicit restrictions on the use of social media/networking sites and posting organizational information on public websites.							Does the institution or department have a cumented acceptable use policy relating to stem usage and responsibilities for security ted includes specific considerations for certain es of technologies such as PDAs, laptops, et, etc. and that is effectively communicated faculty, staff, and other users? Does the institution or department have a echanism to validate whether acceptable use licy has been read and acknowledged (e.g., nature from personnel confirming rules of haviour)?	Obtain security planning policy; procedures addressing rules of behavior for information system users; NIST Special Publication 800-18; rules of behavior; other relevant documents or records and ascertain if : (i)the organization establishes a set of rules that describe user responsibilities and expected behavior with regard to information and information system usage. (ii)the organization makes the rules available to all information system users. (iii)the rules of behavior for organizational personnel are consistent with NIST Special Publication 800-18. (iv)the organization receives a signed acknowledgement from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to the information system and its resident information.	Improper use of information or assets occurs inside an information processing facility.	8280	6.1 - 6.7.1	8120	6.2											CobiT v5 - High Level Control Objective DSS01;DSS04;DSS05;DSS06Controls have been defined to manage data by maintaining the completeness, accuracy, availability and protection of data.
RI0111	PLANNING	INFORMATION SECURITY ARCHITECTURE	PL-8			**Required**	Protect -> Enterprise Architecture, Roadmap & Emerging Technology	The organization: a. Develops an information security architecture for the information system that: 1. Describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information; 2. Describes how the information security architecture is integrated into and supports the enterprise architecture; and 3. Describes any information security assumptions about, and dependencies on, external services; b. Reviews and updates the information security architecture [At least annually or when a significant change occurs] to reflect updates in the enterprise architecture; and c. Ensures that planned information security architecture changes are reflected in the security plan, the security Concept of Operations (CONOPS), and organizational procurements/acquisitions.							Does the institution or department have cumented policies and procedures on formation security architecture? Does the institution or department reviews d updates the information security chitecture on a periodic basis and aligns it th the enterprise architecture?	Obtain policies and procedures addressing information security architecture and ascertain if: (i) the documentation describes the requirements and approach to protect confidentiality, integrity and availability of organizational information; (ii) the documentation describes the integration with the enterprise architecture; (iii) the documentation describes assumptions about and dependencies on external services; (iv) the information security architecture is reviewed and updated at an appropriate frequency to reflect updates to enterprise architecture; and (v) the changes in information security architecture are reflected in the security plan, CONOPS and organizational procurements/acquisitions.	The lack of establishing an enterprise information model may result in application development and decision-supporting activities that are inconsistent with IT plans.	8120	6.1.2												CobiT v5 - High Level Control Objective APO01; APO07; APO12Controls have been established for defining the IT processes, organization and relationships to be responsive to business strategy and comply with governance requirements.
RI0112	PERSONNEL SECURITY	PERSONNEL SECURITY POLICY AND PROCEDURES	PS-1		**Required**	**Required**	Protect -> Personnel Security	The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the personnel security policy and associated personnel security controls; and b. Reviews and updates the current: 1. Personnel security policy [at least every three years]; and 2. Personnel security procedures [at least annually].							es the institution or department have a cumented policy and supporting processes d addressing staff background and other ecks needed based on the role of the dividual at the institution?	Obtain personnel security policy and procedures, other relevant documents or records and ascertain if : (i)the organization develops and documents personnel security policy and procedures. (ii)the organization disseminates personnel security policy and procedures to appropriate elements within the organization. (iii)responsible parties within the organization periodically review personnel security policy and procedures. (iv)the organization updates personnel security policy and procedures when organizational review indicates updates are required. (v)the personnel security policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance. (vi)the personnel security policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance. (vii)the personnel security procedures address all areas identified in the personnel security policy and address achieving policy-compliant implementations of all associated personnel security controls.	Employees, contractors and third party users do not maintain their security responsibilities.	8120	6.2	8270	6.1 - 6.9											CobiT v5 - High Level Control Objective APO07; APO01Controls have been defined for the management of IT human resources.
RI0113	PERSONNEL SECURITY	POSITION RISK DESIGNATION	PS-2		**Required**	**Required**	Protect -> Personnel Security	The organization: a. Assigns a risk designation to all organizational positions; b. Establishes screening criteria for individuals filling those positions; and c. Reviews and updates position risk designations [at least every three years].							es the institution or department identified d classified personnel positions based on risk tegory? ne the context for classifying positions by sk level is to identify and enforce background ecks and other controls due to the higher risk sition, e.g., a security administrator with ess" to the "kingdom" has a higher risk ofile and may require higher due diligence an a janitor for instance.]	Obtain personnel security policy; procedures addressing position categorization; appropriate codes of federal regulations; OPM policy and guidance; list of risk designations for organizational positions; security plan; records of risk designation reviews and updates; other relevant documents or records and ascertain if : (i)the organization assigns a risk designations to all positions within the organization. (ii)the organization establishes screening criteria for individuals filling those organizational positions. (iii)the risk designations for the organizational positions are consistent with 5 CFR 731.106(a) and OPM policy and guidance. (iv)the organization define in the security plan, explicitly or by reference, the frequency of risk designation reviews and updates for organizational positions. (v)the organization reviews and revises position risk designations in accordance with the organization-defined frequency.	Security roles and responsibilities are not defined and clearly communicated to job candidates during the pre-employment process.	8270	6.1												CobiT v5 - High Level Control Objective APO07; APO01Controls have been defined for the management of IT human resources.
RI0114	PERSONNEL SECURITY	PERSONNEL SCREENING	PS-3		**Required**	**Required (3)**	Protect -> Personnel Security	The organization: a. Screens individuals prior to authorizing access to the information system; and b. Screens rotinely thereafter, in accordance with the following criteria: a retrescreening is required during the 5th year for top secret security clearance, the 10th year for secret security clearance, and 15th year for confidential security clearance; For moderate risk law enforcement and high impact public trust level, a reinvestigation is required during the 5th year. There is no reinvestigation for other moderate risk positions or any low risk positions] Control Enhancement: (3) PERSONNEL SCREENING | INFORMATION WITH SPECIAL PROTECTION MEASURES The organization ensures that individuals accessing an information system processing, storing, or transmitting information requiring special protection: (a) Have valid access authorizations that are demonstrated by assigned official government duties; and (b) Satisfy [personnel screening criteria – as required by specific information]							Does the institution or department have cumented policies and procedures on ensuring that only suitable potential employees are ntracted to work for the institution and ntracters prior to being hired in order to minimize the risk of attacks from internal ersons? Do employees or contractors in high risk job es require periodic re-screening?	Obtain personnel security policy; procedures addressing personnel screening; records of screened personnel; NIST Special Publications 800-73, 800-76, and 800-78; other relevant documents or records and ascertain if : (i)the organization screens individuals requiring access to organizational information and information systems prior to authorizing access. (ii)the personnel screening is consistent with 5 CFR 731.106, OPM policy, regulations, and guidance, FIPS 201 and NIST Special Publications 800-73, 800-76, and 800-78, and the criteria established for the risk designation for the assigned position.	Employees, contractors and third party users breach security due to lack of management.	8270	6.3												CobiT v5 - High Level Control Objective APO07; APO01Controls have been defined for the management of IT human resources.
RI0115	PERSONNEL SECURITY	PERSONNEL TERMINATION	PS-4		**Required**	**Required (2)**	Protect -> Personnel Security	The organization, upon termination of individual employment: a. Disables information system access within [same day]; b. Terminates/revokes any authenticators/credentials associated with the individual; c. Conducts exit interviews that include a discussion of [Assignment: organization-defined information security topics]; d. Retrieves all security-related organizational information system-related property; e. Retains access to organizational information and information systems formerly controlled by terminated individual; and f. Notifies [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined time period]. Control Enhancements: (2) PERSONNEL TERMINATION | AUTOMATED NOTIFICATION The organization employs automated mechanisms to notify [access control personnel responsible for disabling access to the system] upon termination of an individual							es the institution or department have cumented policies and supporting processes place to: promptly revoke/disable access of ployees, contractors, etc., upon termination; d retrieve all security-related institutional formation and system-related property (e.g., stitutionally provided laptops, PDAs, access rds, keys, etc)?	Obtain personnel security policy; procedures addressing personnel termination; records of personnel termination actions; list of information system accounts; other relevant documents or records and ascertain if : (i)the organization terminates information system access upon termination of individual employment. (ii)the organization conducts exit interviews of terminated personnel. (iii)the organization retrieves all organizational information system-related property from terminated personnel. (iv)the organization retains access to official documents and records on organizational information systems created by terminated personnel.	Security breaches occur during employment terminations or changes due to lack of defined management responsibilities for these situations.	8270	6.4												CobiT v5 - High Level Control Objective APO07; APO01Controls have been defined for the management of IT human resources.
RI0116	PERSONNEL SECURITY	PERSONNEL TRANSFER	PS-5		**Required**	**Required**	Protect -> Personnel Security	The organization: a. Reviews and confirms ongoing operational need for current logical and physical access authorizations to information systems/facilities when individuals are reassigned or transferred to other positions within the organization; b. Initiates [Assignment: organization-defined transfer or reassignment actions] within [Assignment: organization-defined time period]; c. Modifies access authorization as needed to correspond with any changes in operational need due to reassignment or transfer; and d. Notifies [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined time period].							es the institution or department have ocesses in place to timely update access to formation resources and facilities due to anges in role of the employee or contractor?	Obtain personnel security policy; procedures addressing personnel transfer; records of personnel transfer actions; list of information system and facility access authorizations; other relevant documents or records and ascertain if : (i)the organization reviews information systems/facilities access authorizations when personnel are reassigned or transferred to other positions within the organization. (ii)the organization initiates appropriate actions (e.g., reviewing logs, identification cards, building passes; closing old accounts and establishing new accounts; and changing system access authorization) for personnel reassigned or transferred within the organization.	Employee, contractor or third party user terminations or change of responsibilities could result in a security breach due to lack of a defined management process for terminations or changes in responsibilities.	8270	6.5												CobiT v5 - High Level Control Objective APO07; APO01Controls have been defined for the management of IT human resources.
RI0117	PERSONNEL SECURITY	ACCESS AGREEMENTS	PS-6		**Required**	**Required**	Protect -> Personnel Security	The organization: a. Develops and documents access agreements for organizational information systems; b. Reviews and updates the access agreements [at least annually; and c. Ensures that individuals requiring access to organizational information and information systems: 1. Sign appropriate access agreements prior to being granted access; and 2. Re-sign access agreements to maintain access to organizational information systems when access agreements have been updated or [at least annually							es the institution or department ensure dividuals requiring access to organizational formation and information systems sign ppropriate access agreements prior to being anted access and periodically review and pdate those agreements?	Obtain personnel security policy; procedures addressing access agreements for organizational information and information systems; security plan; access agreements; records of access agreement reviews and updates; other relevant documents or records and ascertain if : (i)the organization requires appropriate access agreements for individuals requiring access to organizational information and information systems before authorizing access. (ii)organizational personnel sign appropriate access agreements prior to receiving access . (iii)the organization defines in the security plan, explicitly or by reference, the frequency of reviews/updates for access agreements. (iv)the organization reviews/updates the access agreements in accordance with the organization-defined frequency.	Employees or contractors do not agree or sign terms or conditions of employment.	8270	6.6	8280	6.1											CobiT v5 - High Level Control Objective APO07; APO01Controls have been defined for the management of IT human resources.
RI0118	PERSONNEL SECURITY	THIRD-PARTY PERSONNEL SECURITY	PS-7		**Required**	**Required**	Protect -> Personnel Security	The organization: a. Establishes personnel security requirements including security roles and responsibilities for third-party providers; b. Requires third-party providers to comply with personnel security policies and procedures established by the organization; c. Documents personnel security requirements; d. Requires third-party providers to notify [Assignment: organization-defined personnel or roles] of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges within [Assignment: organization-defined time period-same day]; and e. Monitors provider compliance.							es the institution or department have cumented personnel security requirements third party providers (e.g., requirements ecorded in SLAs based on the company's ecing requirements, etc.), and are there ocesses in place to monitor their compliance such requirements (e.g., sample checks by e institution and / or third-party assessment ganization)?	Obtain personnel security policy; procedures addressing third-party personnel security; list of personnel security requirements; acquisition documents; compliance monitoring process; other relevant documents or records and ascertain if : (i)the organization establishes personnel security requirements, including security roles and responsibilities, for third-party providers (e.g., service bureaus, contractors, and other organizations providing information system development, information technology services, outsourced applications, network and security management). (ii)the organization explicitly includes personnel security requirements in acquisition-related documents in accordance with NIST Special Publication 800-35. (iii)the organization monitors third-party provider compliance with personnel security requirements.	Security is breached by employees, contractors or third party users that leverage access given after termination or change of their employment, contract or agreement.	8270	6.7												CobiT v5 - High Level Control Objective APO07; APO01Controls have been defined for the management of IT human resources.

	Security Control Family	Control Name	NIST 800-53 Control #	Low (Control and Control Enhancements)	MODERATE (Control and Control Enhancements)	Security Program Area (Function Area / Functional Sub-Area)	NIST 800-53 Rev. 4 Control (Control and Control Enhancements) Detailed breakdown of required controls	Vendor's Response (Please Address all the controls and control enhancements in DETAIL. Controls and Enhancements identified in Column H)	Overall Control(s) Implementation Status (Reference on Comments Page) Please select from Drop down (Lower right corner)	Where does the Control(s) originate from? Please select from Drop down (Lower right corner)	Supporting Documentation (Policies and procedures must be explicitly referenced (title and date or version) so that it is clear which document is being referred to. Section numbers or similar mechanisms should allow the reviewer to easily find the	Vendor's Compensating Controls (If Control Can't Be Met - What is the alternative security controls employed by organization)	Vendor Non-Compliance (If you can't meet this control at all please explain why) (Please See Risk Statement for examples of Non-Compliance language Column R)	General Assessment Questions	Detailed Control Testing Procedure(s)	Risk Statement Examples	SOA Policy Number 1	SOA SubSection 1	SOA Policy Number 2	SOA SubSection 2	SOA Policy Number 3	SOA SubSection 3	SOA Policy Number 4	SOA SubSection 4			Arizona Breach Notification A.R.S. § 44-7501	Arizona Computer Tampering A.R.S. § 13-2316	COBIT Reference (Control Objective)
R01.19	PERSONNEL SECURITY	PERSONNEL SANCTIONS	PS-8		**Required**	**Required**	Protect -> Personnel Security	The organization: a. Employs a formal sanctions process for individuals failing to comply with established information security policies and procedures; and b. Notifies [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined time period] when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.						es the institution or department employ al sanctions when personnel fail to comply h established information security policies d procedures (e.g., reprimands to mination depending on the degree and ation of non-compliance)?	Obtain personnel security policy; procedures addressing personnel sanctions; rules of behavior; records of formal sanctions; other relevant documents or records and ascertain if : (i)the organization employs a formal sanctions process for personnel failing to comply with established information security policies and procedures. (ii)the personnel sanctions process is consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.	Security breaches occur by employees due to lack of formal disciplinary process.	8280	6.7												COBIT v5 - High Level Control Objective APO07; APO01] Controls have been defined for the management of IT human resources.
R01.20	RISK ASSESSMENT	RISK ASSESSMENT POLICY AND PROCEDURES	RA-1		**Required**	**Required**	Identify -> Security Assessment and Authorization / Technology Risk Assessments	The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls; and b. Reviews and updates the current: 1. Risk assessment policy [at least annually]; and 2. Risk assessment procedures [at least annually].						es the institution or department develop, nentate, and review/update a formal, umented risk assessment policy that ddresses purpose, scope, roles, responsibilities, management commitment, ordination among organizational entities, compliance as well as procedures to plement the policy?	Obtain risk assessment policy and procedures; other relevant documents or records and ascertain if : (i)the organization develops and documents risk assessment policy and procedures. (ii)the organization disseminates risk assessment policy and procedures to appropriate elements within the organization. (iii)responsible parties within the organization periodically review risk assessment policy and procedures. (iv)the organization updates risk assessment policy and procedures when organizational review indicates updates are required. (v)the risk assessment policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance (vi)the risk assessment policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance. (vii)the risk assessment procedures address all areas identified in the risk assessment policy and address achieving policy-compliant implementations of all associated risk assessment controls.	Management is unable to identify potential events with negative impact and events representing opportunities to be pursued which may lead to unmanageable IT risks.	8120	6.2												COBIT v5 - High Level Control Objective EDM03; APO01; APO12]Controls have been defined to assess and manage IT risks
R01.21	RISK ASSESSMENT	SECURITY CATEGORIZATION	RA-2		**Required**	**Required**	Identify -> Data Classification	The organization: a. Categorizes information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; b. Documents the security categorization results (including supporting rationale) in the security plan for the information system; and c. Ensures that the security categorization decision is reviewed and approved by the authorizing official or authorizing official designated representative.						Does the institution have a documented ssification policy or standard that ides data owners on data categorization, and associated security requirements of ormation systems where such information is ntained? If yes, are information systems categorized cording to the data classification policy or ndard? If yes, are information system security plans ned with the classification of the ormation system?	Obtain risk assessment policy; procedures addressing security categorization of organizational information and information systems; security planning policy and procedures; FIPS 199; NIST Special Publication 800-60; security plan; other relevant documents or records and ascertain if : (i)the organization conducts the security categorization of the information system as an organization-wide exercise with the involvement of senior-level officials including, but not limited to, authorizing officials, information system owners, chief information officer, senior agency information security officer, and mission/information owners. (ii)the security categorization is consistent with FIPS 199 and considers the provisional impact levels and special factors in NIST Special Publication 800-60. (iii)the organization considers in the security categorization of the information system, potential impacts to other organizations and, in accordance with the USA PATRIOT Act of 2001 and Homeland Security Presidential Directives, potential national-level impacts. (iv)the organization includes supporting rationale for impact-level decisions as part of the security categorization. (v)designated, senior-level organizational officials review and approve the security categorizations.	Information is disclosed due to lack of protection based on the need, priorities and expected degree of protection.	8110	6.2	8120	6.3.2										COBIT v5 - High Level Control Objective DSS01;DSS04;DSS05;DSS06]Controls have been defined to manage data by maintaining the completeness, accuracy, availability and protection of data.
R01.22	RISK ASSESSMENT	RISK ASSESSMENT	RA-3		**Required**	**Required**	Identify -> Security Assessment and Authorization / Technology Risk Assessments	The organization: a. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits; b. Documents risk assessment results in [Selection: security plan; risk assessment report; technical report; or other]; c. Reviews risk assessment results [at least every three years or when a significant change occurs]; d. Disseminates risk assessment results to [Assignment: organization-defined personnel or roles]; and e. Updates the risk assessment [at least every three years or when a significant change occurs] or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities) or other conditions that may impact the security state of the system.						Does the institution or department have ies and supporting processes that define gers for when information security related assessments should be conducted, as well the criteria for risk assessment (e.g., ssets, threats, vulnerabilities, ty information security risk assessments ducted at least annually)?	Obtain risk assessment policy; procedures addressing risk assessment; security plan; other relevant documents or records and ascertain if : (i)the organization assesses the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets (including information and information systems managed/operated by external parties). (ii)the risk assessment is consistent with the NIST Special Publication 800-30.	Technical vulnerabilities are exploited to gain inappropriate or unauthorized access to information systems due to lack of controls for these vulnerabilities.	8120	6.3.4												COBIT v5 - High Level Control Objective APO12; DSS05; DSS05] Controls have been defined to ensure system security by defining IT security policies, procedures and standards, and monitoring, detecting, reporting security vulnerabilities and incidents.
R01.23	RISK ASSESSMENT	VULNERABILITY SCANNING	RA-5		**Required**	**Required (1,2,3,5,6,8)**	Detect -> Vulnerability Assessment	The organization: a. Scans for vulnerabilities in the information system and hosted applications [monthly operating system/infrastructure; monthly web applications and databases] and when new vulnerabilities potentially affecting the system/applications are identified and reported; b. Employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for: 1. Enumerating platforms, software flaws, and improper configurations; 2. Formatting checklists and test procedures; and 3. Measuring vulnerability impact; c. Analyzes vulnerability scan reports and results from security control assessments; d. Remediates legitimate vulnerabilities [high-risk vulnerabilities mitigated within thirty days from date of discovery; moderate-risk vulnerabilities mitigated within ninety days from date of discovery] in accordance with an organizational assessment of risk; and e. Shares information obtained from the vulnerability scanning process and security control assessments with [Assignment: organization-defined personnel or roles] to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies). Control Enhancement: (1) VULNERABILITY SCANNING	UPDATE TOOL CAPABILITY The organization employs vulnerability scanning tools that include the capability to readily update the information system vulnerabilities to be scanned. (2) VULNERABILITY SCANNING	UPDATE BY FREQUENCY / PRIOR TO NEW SCAN / WHEN IDENTIFIED The organization updates the information system vulnerabilities scanned [Selection (one or more): [prior to a new scan] ; prior to a new scan; when new vulnerabilities are identified and reported].						es the institution or department have tools ether capability (e.g., third-party service viders), and processes in place for ducting security vulnerability scanning that ludes: ecuting scans on a scheduled basis for its ormation systems (e.g., servers, network ices, databases, applications, workstations, ices scans, etc.); ecuting and reporting scan results to the ropriate stakeholders; emediating vulnerabilities based on risk; sharing information obtained from the nerability scanning process and security trol assessments with designated personnel roughout the institution to help eliminate ilar vulnerabilities in other information tems, i.e., systemic weaknesses or ficiencies?	Obtain risk assessment policy; procedures addressing vulnerability scanning; risk assessment; security plan; vulnerability scanning results; patch and vulnerability management records; vulnerability scanning tools and techniques documentation; other relevant documents or records and ascertain if : (i)the organization defines in the security plan, explicitly or by reference, the frequency of vulnerability scans within the information system. (ii)the organization scans for vulnerabilities in the information system in accordance with the organization-defined frequency and/or random in accordance with organizational policy and assessment of risk, or when significant new vulnerabilities potentially affecting the system are identified and reported. (iii)the organization uses appropriate scanning tools and techniques to conduct the vulnerability scans. (iv)the organization trains selected personnel in the use and maintenance of vulnerability scanning tools and techniques. (v)the organization freely shares the information obtained from the vulnerability scanning process with appropriate personnel throughout the organization to help eliminate similar vulnerabilities in other information systems. (vi) the organization uses vulnerability scanning tools that have the capability to readily update the list of information system vulnerabilities scanned.	Technical vulnerabilities are exploited to gain inappropriate or unauthorized access to information systems due to lack of controls for these vulnerabilities.	8120	6.3.5												COBIT v5 - High Level Control Objective APO13; DSS02; DSS05] Controls have been defined to ensure system security by defining IT security policies, procedures and standards, and monitoring, detecting, reporting security vulnerabilities and incidents.
R01.24	SYSTEM AND SERVICES ACQUISITION	SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES	SA-1		**Required**	**Required**	Protect -> Enterprise Architecture, Roadmap & Emerging Technology	The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A system and services acquisition policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls; and b. Reviews and updates the current: 1. System and services acquisition policy [at least every 3 years]; and 2. System and services acquisition procedures [at least annually].						es the institution or department have umented policies and supporting processes ensuring that system and services quisition, development, and deployment are ne with business requirements, including dit information security considerations?	Obtain system and services acquisition policy and procedures; other relevant documents or records and ascertain if: (i)the organization develops and documents system and services acquisition policy and procedures. (ii)the organization disseminates system and services acquisition policy and procedures to appropriate elements within the organization. (iii)responsible parties within the organization periodically review system and services acquisition policy and procedures. (iv)the organization updates system and services acquisition policy and procedures when organizational review indicates updates are required. (v)the system and services acquisition policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance (vi)the system and services acquisition policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and (vii)the system and services acquisition procedures address all areas identified in the system and services acquisition policy and address achieving policy-compliant implementations of all associated system and services acquisition controls.	Acquiring resources for IT is done inconsistently with unreasonable cost.	8120	6.2												COBIT v5 - High Level Control Objective BAI03.04; APO02]Controls have been defined for the procurement of IT resources.
R01.25	SYSTEM AND SERVICES ACQUISITION	ALLOCATION OF RESOURCES	SA-2		**Required**	**Required**	Protect -> Enterprise Architecture, Roadmap & Emerging Technology	The organization: a. Determines information security requirements for the information system or information system service in mission/business process planning; b. Determines, documents, and allocates the resources required to protect the information system or information system service as part of its capital planning and investment control process; and c. Establishes a discrete line item for information security in organizational programming and budgeting documentation.						dit line entry for incorporating information rity resource requirements for planning d implementing information systems?	Obtain system and services acquisition policy; procedures addressing the integration of information security into the system development life cycle process; NIST Special Publication 800-64; information system development life cycle documentation; other relevant documents or records and ascertain if : (i)the organization determines, documents, and allocates as part of its capital planning and investment control process, the resources required to adequately protect the information system by verifying that the organization: - defines security requirements for the information system in mission/business planning. - establishes a discrete line item for information system security in the organization's programming and budgeting documentation. - integrates information system security into the capital planning and investment control process in accordance with the guidance in NIST Special Publication 800-65.	Management has not aligned the information technology architecture with corporate strategy.	8130	6.1												COBIT v5 - High Level Control Objective APO02; APO07; APO12] Controls have been established for defining the IT processes, organization and relationships to be responsive to business strategy and comply with governance requirements.
R01.26	SYSTEM AND SERVICES ACQUISITION	SYSTEM DEVELOPMENT LIFE CYCLE	SA-3		**Required**	**Required**	Protect -> Secure System Services, Acquisition and Development	The organization: a. Manages the information system using [Assignment: organization-defined system development life cycle] that incorporates information security considerations; b. Defines and documents information security roles and responsibilities throughout the system development life cycle; c. Identifies individuals having information security roles and responsibilities; and d. Integrates the organizational information security risk management process into system development life cycle activities.						es the institution or department have umented systems development lifecycle ies policy and supporting processes that ntify account for information security, and ine roles and responsibilities for the SDLC ocesses?	Obtain system and services acquisition policy; procedures addressing the integration of information security into the system development life cycle process; NIST Special Publication 800-64; information system development life cycle documentation; other relevant documents or records and ascertain if : (i)the organization manages the information system using a system development life cycle methodology that includes information security considerations. (ii)the organization uses a system development life cycle that is consistent with NIST Special Publication 800-64.	Developed and implemented systems do not consider the Design phase of the systems development lifecycle.	8130	6.2												COBIT v5 - High Level Control Objective BAI03]Controls have been defined for the acquisition and maintenance of application software to ensure there is a timely and cost-effective development process.
R01.27	SYSTEM AND SERVICES ACQUISITION	ACQUISITION PROCESS	SA-4		**Required (10)**	**Required 1,2,8,9,10)**	Protect -> Secure System Services, Acquisition and Development	The organization includes the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs: a. Security functional requirements; b. Security strength requirements; c. Security assurance requirements; d. Security-related documentation requirements; e. Requirements for protecting security-related documentation; f. Description of the information system development environment and environment in which the system is intended to operate; and g. Acceptance criteria. Control Enhancement: (1) ACQUISITION PROCESS	FUNCTIONAL PROPERTIES OF SECURITY CONTROLS The organization requires the developer of the information system, system component, or information system service to provide a description of the functional properties of the security controls to be employed. (2) ACQUISITION PROCESS	DESIGN / IMPLEMENTATION INFORMATION FOR SECURITY CONTROLS The organization requires the developer of the information system, system component, or information system service to provide design and implementation information for the security controls to be employed that includes: [to include security-relevant external system interfaces; high-level design, hardware schematics]at [Assignment: organization-defined level of detail]. (8) ACQUISITION PROCESS	CONTINUOUS MONITORING PLAN						es the institution or department have ies and supporting processes to ensure information system contracts, based on level, account for: ormation security risk assessment; security functional requirements / ifications; security-related documentation uirements; and developmental and evaluation-related urance requirements.	Obtain system and services acquisition policy; procedures addressing the integration of information security requirements and/or security specifications into the acquisition process; NIST Special Publications 800-23 and 800-35; information system development life cycle documentation; information systems or services; solicitation documents; other relevant documents or records and ascertain if : (i)the organization includes in acquisition contracts for information systems, either explicitly or by reference, security requirements and/or security specifications based on an assessment of risk and in accordance with applicable laws, Executive Orders, directives, policies, regulations, and standards that describe required: - security capabilities. - design and development processes. - test and evaluation procedures. - documentation. (ii)the organization includes in acquisition contracts, requirements for information system documentation addressing user and systems administrator guidance and information regarding the implementation of the security controls in the information system, and the security capabilities of the IT products in the system. (iii)the organization includes in acquisition contracts requirements for information system documentation that includes security configuration settings and security implementation guidance. (iv)the organization requires in solicitation documents that appropriate documentation be provided describing the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls. (v) the organization explicitly assigns each acquired information system component to an information system. (vi) the owner of the system acknowledges each assignment of information system components to the information system.	The organization's interests are not protected in IT acquisition contractual agreements.	8130	6.3												COBIT v5 - High Level Control Objective BAI03.04; APO02]Controls have been defined for the procurement of IT resources.
R01.28	SYSTEM AND SERVICES ACQUISITION	INFORMATION SYSTEM DOCUMENTATION	SA-5		**Required**	**Required**	Protect -> Secure System Services, Acquisition and Development	The organization: a. Obtains administrator documentation for the information system, system component, or information system service that describes: 1. Secure configuration, installation, and operation of the system, component, or service; 2. Effective use and maintenance of security functions/mechanisms; and 3. Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions; b. Obtains user documentation for the information system, system component, or information system service that describes: 1. User accessible security functions/mechanisms and how to effectively use those security functions/mechanisms; 2. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner; and 3. User responsibilities in maintaining the security of the system, component, or service; c. Documents attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent and [Assignment: organization-defined actions] in response; d. Protects documentation as required, in accordance with the risk management strategy; and e. Distributes documentation to [Assignment: organization-defined personnel or roles].						es the institution or department have ective processes in place to ensure that ropriate levels of information and training ual information systems exist to configure manage systems securely (e.g., vendor umentation on default accounts and secure figuration specs, administration processes, nical training, etc.)?	Obtain system and services acquisition policy; procedures addressing information system documentation; information system documentation including administrator and user guides; other relevant documents or records and ascertain if : (i)the organization obtains, protects as required, and makes available to authorized personnel, information system administrator and user guidance with information on: - configuring, installing, and operating the information system. - effectively using the system's security features. (ii)the organization, when this information is either unavailable or non existent (e.g., due to the age of the system or lack of support from the vendor/manufacturer), actively pursues documents attempts to obtain such documentation and provides compensating security controls, if needed. (iii)the organization obtains, protects as required, and makes available to authorized personnel, information system administrator and user guides, documentation, if available from the vendor/manufacturer, describing the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls. (iv) the organization obtains, protects as required, and makes available to authorized personnel, vendor/manufacturer documentation that describes the high-level design of the information system in terms of subsystems and implementation details of the security controls employed within the system with sufficient detail to permit analysis and testing	Sensitive system configuration information is accessed by unauthorized parties due to inadequate security of system documentation	8130	6.4												COBIT v5 - High Level Control Objective DSS01;DSS04;DSS05;DSS06] Controls have been defined to manage data by maintaining the completeness, accuracy, availability and protection of data.
R01.29	SYSTEM AND SERVICES ACQUISITION	SECURITY ENGINEERING PRINCIPLES	SA-8			**Required**	Protect -> Secure System Services, Acquisition and Development	The organization applies information system security engineering principles in the specification, design, development, implementation, and modification of the information system.						es the institution or department have tem security engineering principles rporated into its System Development cycle (SDLC) to achieve the goal of "secure design" when building, customizing, and/or ifying information systems (e.g., ications, databases, etc.)? ese examples of engineering principles could ude use of "Input Validation Library" for ew applications to reduce exposure from nerabilities from input manipulation (e.g., ection).	Obtain system and services acquisition policy; procedures addressing security engineering principles used in the development and implementation of the information system; NIST Special Publication 800-27; information system design documentation; security requirements and security specifications for the information system; other relevant documents or records and ascertain if : (i)the organization designs and implements the information system using security engineering principles. (ii)the organization considers the security design principles in NIST Special Publication 800-27 in the design, development, and implementation of the information system.	Programming errors or misconfiguration leads to vulnerabilities that can be exploited.	8130	6.5												COBIT v5 - High Level Control Objective BAI03; DSS02] Controls have been defined for the acquisition and maintenance of technology infrastructure to ensure that the platforms that support the business operations are aligned with defined IT architecture and technology standards.
R01.30	SYSTEM AND SERVICES ACQUISITION	EXTERNAL INFORMATION SYSTEM SERVICES	SA-9		**Required**	**Required (1,2,4,5)**	Identify -> External Vendors and Third-Party Providers Identify -> Cloud Usage and Security	The organization: a. Requires that providers of external information system services comply with organizational information security requirements and employ [Assignment: organization-defined security controls] in accordance with applicable laws, federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; b. Defines and documents government oversight and user roles and responsibilities with regard to external information system services; and c. Employs [Arizona Continuous Monitoring requirements must be met for external systems where State information is processed or stored] to monitor security control compliance by external service providers on an ongoing basis. Control Enhancement: (1) EXTERNAL INFORMATION SYSTEMS	RISK ASSESSMENTS / ORGANIZATIONAL APPROVAL The organization: (a) Conducts an organizational assessment of risk prior to the acquisition or outsourcing of dedicated information security services; and (b) Ensures that the acquisition or outsourcing of dedicated information security services is approved by [Assignment: organization-defined personnel or roles]. (2) EXTERNAL INFORMATION SYSTEMS	IDENTIFICATION OF FUNCTIONS / PORTS / PROTOCOLS / SERVICES The organization requires providers of [All external systems where State information is processed or stored] to identify the functions, ports, protocols, and other services required for the use of such services.						es the institution or department have ies and supporting processes in place to nitor information security risks from third-ty providers (e.g., Software as a Service ice, Infrastructure as a Service ice, cloud services, Application Service viders, etc.)? ple: Monitoring of third-parties can be risk ed and can take a number of forms such as ducting on-site assessments, reviewing d-party audit reports like SSAE16, etc.).	Obtain system and services acquisition policy; procedures addressing external information system services; acquisition contracts and service level agreements; organizational security requirements and security specifications for external provider services; security control assessment evidence from external providers of information security compliance; other relevant documents or records and ascertain if : (i)the organization requires that providers of external information system services employ adequate security controls in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, guidance, and established service-level agreements. (ii)the organization monitors security control compliance.	Services, reports and records provided by a third party are not consistently monitored and reviewed by management.	8130	6.6												COBIT v5 - High Level Control Objective APO02] Controls have been defined for managing third-party services to establish roles, relationships and balancing responsibilities with qualified third-party service providers and monitoring the service delivery to verify and ensure adherence to agreements.

	Security Control Family	Control Name	NIST 800-53 Control #	Low (Control and Control Enhancements)	MODERATE (Control and Control Enhancements)	Security Program Area (Function Area + Functional Sub-Area)	NIST 800-53 Rev. 4 Control (Control and Control Enhancements) Detailed breakdown of required controls	Vendor's Response (Please Address all the controls and control enhancements in DETAIL. Controls and Enhancements identified in Column H)	Overall Control(s) Implementation Status (Reference on Comments Page) Please select from Drop down (Lower right corner)	Where does the Control(s) originate from? Please select from Drop down (Lower right corner)	Supporting Documentation (Policies and procedures must be explicitly referenced (title and date or version) so that it is clear which document is being referred to. Section numbers or similar mechanisms should allow the reviewer to easily find the	Vendor's Compensating Controls (If Control Can't Be Met - What is the alternative security controls employed by organization)	Vendor Non-Compliance (If you can't meet this control at all please explain why) (Please See Risk Statement for examples of Non-Compliance language Column R)	General Assessment Questions	Detailed Control Testing Procedure(s)	Risk Statement Examples	SOA Policy Number 1	SOA SubSection 1	SOA Policy Number 2	SOA SubSection 2	SOA Policy Number 3	SOA SubSection 3	SOA Policy Number 4	SOA SubSection 4			Arizona Breach Notification A.R.S. § 44-7501	Arizona Computer Tampering A.R.S. § 13-2316	COBIT Reference (Control Objective)
R(S)31	SYSTEM AND SERVICES ACQUISITION	DEVELOPER CONFIGURATION MANAGEMENT	SA-10		Required (1)	Protect -> Change Management	The organization requires the developer of the information system, system component, or information system service to: a. Perform configuration management during system, component, or service [development, implementation, AND operation]; b. Document, manage, and control the integrity of changes to [Assignment: organization-defined configuration items under configuration management]; c. Implement only organization-approved changes to the system, component, or service; d. Document approved changes to the system, component, or service and the potential security impacts of such changes; and e. Track security flaws and flaw resolution within the system, component, or service and report findings to [Assignment: organization-defined personnel]. Control Enhancement: (1) DEVELOPER CONFIGURATION MANAGEMENT	SOFTWARE / FIRMWARE INTEGRITY VERIFICATION The organization requires the developer of the information system, system component, or information system service to enable integrity verification of software and firmware components.										Does the institution or department have documented change control procedures that require approval for making changes; take into account impact on information security and related configurations; perform appropriate level of testing of changes, including information security, as pilotable; track defects and security flaws; and require approval from appropriate level of management for authorizing changes into solution?	Obtain system and services acquisition policy; procedures addressing information system developer/integrator configuration management; acquisition contracts and service level agreements; information system developer/integrator configuration management plan; security flaw tracking records; system change authorization records; other relevant documents or records and ascertain if : (1)the organization requires that information system developers create and implement a configuration management plan that controls changes to the system during development, tracks security flaws, requires authorization of changes, and provides documentation of the plan and its implementation.	Changes are made to production systems without a formal change process.	8130	6.7											[CobiT v5 - High Level Control Objective BAI06] Controls have been defined to manage changes to information systems in order to minimize the likelihood of disruption, unauthorized alterations and errors.
R(S)32	SYSTEM AND SERVICES ACQUISITION	DEVELOPER SECURITY TESTING AND EVALUATION	SA-11		Required (1,2,8)	Protect -> Secure System Services, Acquisition and Development	The organization requires the developer of the information system, system component, or information system service to: a. Create and implement a security assessment plan; b. Perform [selection (one or more): unit; integration; system; regression] testing/evaluation at [Assignment: organization-defined depth and coverage]; c. Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation; d. Implement a verifiable flaw remediation process; and e. Correct flaws identified during security testing/evaluation. Control Enhancement: (1) DEVELOPER SECURITY TESTING AND EVALUATION | STATIC CODE ANALYSIS The organization requires the developer of the information system, system component, or information system service to employ static code analysis tools to identify common flaws and document the results of the analysis. (2) DEVELOPER SECURITY TESTING AND EVALUATION | THREAT AND VULNERABILITY ANALYSES The organization requires the developer of the information system, system component, or information system service to perform threat and vulnerability analyses and subsequent testing/evaluation of the as-built system, component, or service. (8) DEVELOPER SECURITY TESTING AND EVALUATION | DYNAMIC CODE ANALYSIS The organization requires the developer of the information system, system component, or information system service to employ dynamic code analysis tools to identify common flaws and document the results of the analysis.										Does the institution or department have policies and supporting processes in place to facilitity design and test for information security during development of the information system and/or its components (as part of SDLC) during change management process when changes are made to the information system or component(s)?	Obtain system and services acquisition policy; procedures addressing information system developer/integrator security testing; acquisition contracts and service level agreements; information system developer/integrator security test plans; records of developer/integrator security testing results for the information system; other relevant documents or records and ascertain if : (2)the organization requires that information system developers (and systems integrators) create a security test and evaluation plan, implement the plan, and document the results.	Systems are implemented which are not developed according to internal security standards.	8130	6.8											[CobiT v5 - High Level Control Objective BAI03; DSS05] Controls have been defined for the acquisition and maintenance of technology infrastructure to ensure that the platforms that support the business applications are aligned with defined IT architecture and technology standards.
R(S)33	SYSTEM AND COMMUNICATIONS PROTECTION	SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES	SC-1	Required	Required	Protect -> System Communications Protection	The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls; and b. Reviews and updates the current: 1. System and communications protection policy [At least every 3 years]; and 2. System and communications protection procedures[at least annually].										Does the institution or department have documented policies and supporting processes in place for defining and enforcing requirements to protect data transmissions and system-to-system communications within the institution's identity of communicators (for example, over the Internet, within the institution, private networks, etc.)?	Obtain system and communications protection policy and procedures; other relevant documents or records and ascertain if : (3)the organization disseminates system and communications protection policy and procedures to organizational elements within the organization. (4)responsible parties within the organization periodically review system and communications protection policy and procedures. (5)the organization updates system and communications protection policy and procedures when organizational review indicates updates are required. (6)the system and communications protection policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance. (7)the system and communications protection policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance. (8)the system and communications protection procedures address all areas identified in the system and communications protection policy and address achieving policy-compliant implementations of all associated system and communications protection controls.	IT security procedures are not documentated and communicated.	8120	6.2	8350	6.1 - 6.3.11									[CobiT v5 - High Level Control Objective EDM03; APO01] Controls have been defined to communicate management aims and direction and ensure that policies are understandable and expressed in policies, procedures, guidelines and other documentation to stakeholders, embedded in an IT control framework.
R(S)34	SYSTEM AND COMMUNICATIONS PROTECTION	APPLICATION PARTITIONING	SC-2		Required	Protect -> System Communications Protection	The information system separates user functionality (including user interface services) from information system management functionality.										Does the institution or department have policies and supporting processes to segregate administrative / management tools and modules from general user/application traffic? (Ex. examples include segmenting the network into security zones where administrative tasks and systems are separate from other system areas; use of ACLs and stronger authentication for accessing administrative functions, etc.).	Obtain system and communications protection policy; procedures addressing application partitioning; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records and ascertain if : (3)the information system separates user functionality (including user interface services) from information system management functionality.	The integrity of a business process is compromised due to the lack of segregation of duties (e.g., maker & checker).	8350	6.1.1										[CobiT v5 - High Level Control Objective APO01; APO07; APO11] Controls have been established for defining the IT processes, organization and relationships to be responsive to business strategy and comply with governance requirements.
R(S)35	SYSTEM AND COMMUNICATIONS PROTECTION	INFORMATION IN SHARED RESOURCES	SC-4		Required	Protect -> System Communications Protection Identify -> Cloud Usage and Security	The information system prevents unauthorized and unintended information transfer via shared system resources.										Does the institution or department have policies and supporting processes in place to assure that information remnants (data) through shared resources on multi-tenant (cloud) environments? (For example, often a single instance of a database is used to support multiple applications with different security data profiles, and exposure from one application may expose the data of the other application)	Obtain system and communications protection policy; procedures addressing information remnants; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records and ascertain if : (3)the information system prevents unauthorized and unintended information transfer via shared system resources.	Sensitive systems co-located with less sensitive systems are accessed by unauthorized parties.	8350	6.2										[CobiT v5 - High Level Control Objective APO13; DSS05]Controls have been defined to ensure system security by defining IT security policies, procedures and standards, and monitoring, detecting, reporting security vulnerabilities and incidents.
R(S)36	SYSTEM AND COMMUNICATIONS PROTECTION	DENIAL OF SERVICE PROTECTION	SC-5	Required	Required	Protect -> System Communications Protection	The information system protects against or limits the effects of the following types of denial of service attacks: [Assignment: organization-defined types of denial of service attacks or reference to source for such information] by employing [Assignment: organization-defined security safeguards].										Does the institution or department have controls in place to minimize risk of denial of service attacks (internal and external) on critical information systems? (Ex. examples could include use of tools and techniques to identify and filter malicious traffic such attempts, and/or proactively monitoring for denial of service attempts so timely steps can be taken to address the risk)	Obtain system and communications protection policy; procedures addressing denial of service protection; information system design documentation; security plan; information system configuration settings and associated documentation; other relevant documents or records and ascertain if : (2)the organization defines in the security plan, explicitly or by reference, the types of denial of service attacks (or provides references to sources of current denial of service attacks) that can be addressed by the information system. (3)the information system protects against or limits the effects of the organization-defined or referenced types of denial of service attacks.	Inadequately managed and controlled networks and supporting infrastructure expose systems and applications.	8350	6.3.1										[CobiT v5 - High Level Control Objective APO13; DSS02; DSS05] Controls have been defined to ensure system security by defining IT security policies, procedures and standards, and monitoring, detecting, reporting security vulnerabilities and incidents.
R(S)37	SYSTEM AND COMMUNICATIONS PROTECTION	BOUNDARY PROTECTION	SC-7	Required	Required (3,4,5,7,8,12,13,18)	Protect -> System Communications Protection	The information system: a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; b. Implements subnetworks for publicly accessible system components that are [Selection (physically; logically) separated from internal organizational networks; and c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture. Control Enhancement: (3) BOUNDARY PROTECTION | ACCESS POINTS The organization limits the number of external network connections to the information system. (4) BOUNDARY PROTECTION | EXTERNAL TELECOMMUNICATIONS SERVICES The organization: (a) Implements a managed interface for each external telecommunication service; (b) Establishes a traffic flow policy for each managed interface; (c) Protects the confidentiality and integrity of the information being transmitted across each interface; (d) Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need; and (e) Reviews exceptions to the traffic flow policy [at least annually] and removes exceptions that are no longer supported by an explicit mission/business need. (5) BOUNDARY PROTECTION | DENY BY DEFAULT / ALLOW BY EXCEPTION The information system at managed interfaces denies network communications traffic by default and allows network communications traffic by exception (i.e., deny all, permit by exception).										Does the institution or department have effective mechanisms (i.e., tools and processes) in place for monitoring and controlling network traffic, at the perimeter (either at the institution level and/or security zones within the institution or department)? (Ex. examples include properly placed and configured firewalls, proxies, and other security appliances; routers, and gateways that inspect incoming and outgoing network traffic; and security baselines for such devices and periodic review of configured rules?	Obtain system and communications protection policy; procedures addressing boundary protection; list of key internal boundaries of the information system; information system design documentation; boundary protection hardware and software; information system configuration settings and associated documentation; information system hardware and software; information system architecture; list of mediation vehicles for allowing public access to the organization's internal networks; other relevant documents or records and ascertain if : (2)the organization defines key internal boundaries of the information system. (3)the information system monitors and controls communications at the external boundary of the information system and at key internal boundaries within the system. (4)the organization physically allocates publicly accessible information system components to separate sub networks with separate, physical network interfaces. (5)the organization defines the mediation necessary for public access to the organization's internal networks. (6)the organization prevents public access into the organization's internal networks except as appropriately mediated. (7)the organization limits the number of access points to the information system to allow for better monitoring of inbound and outbound network traffic. (8)the organization implements a managed interface (boundary protection devices in an effective security architecture) with any external telecommunication service, implementing controls appropriate to the required protection of confidentiality and integrity of the information being transmitted. (9)the information system denies network traffic by default and allows network traffic by exception. (10)the information system prevents remote devices that have established a non-remote connection with the system from communicating outside of that communications path with resources in external networks.	Computer connections and information flows breach access control policy as a result of inconsistencies with network routing configurations.	8350	6.1.2,-6.14	8350	6.2.2	8350	6.3.3							[CobiT v5 - High Level Control Objective APO13; DSS05]Controls have been defined to ensure system security by defining IT security policies, procedures and standards, and monitoring, detecting, reporting security vulnerabilities and incidents.
R(S)38	SYSTEM AND COMMUNICATIONS PROTECTION	TRANSMISSION CONFIDENTIALITY AND INTEGRITY	SC-8		Required (1)	Protect -> System Communications Protection Identify -> Privacy & Confidentiality	The information system protects the [confidentiality AND integrity] of transmitted information. Control Enhancement: (1) TRANSMISSION CONFIDENTIALITY AND INTEGRITY | CRYPTOGRAPHIC OR ALTERNATE PHYSICAL PROTECTION The information system implements cryptographic mechanisms to [Selection (one or more): prevent unauthorized disclosure of information; detect changes to information] during transmission unless otherwise protected by [prevent unauthorized disclosure of information AND detect changes to information] [a hardened or alarmed carrier Protective Distribution System (PDS)].										Does the institution or department employ cryptographic mechanisms (e.g., digital signature) to recognize changes to information during transmission unless otherwise protected by alternative physical measures? (Ex. examples include policy and procedures and supporting processes in place specifying requirements, authorizations, and protocols when transmitting or posting confidential data within the institution and outside the institution and encrypting confidential data transmitted over the Internet? Note: the requirement is to minimize risk of unauthorized disclosure of confidential information should not be transmitted unless there is a business need that has been approved by appropriate level of management).	Obtain system and communications protection policy; procedures addressing transmission integrity; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records and ascertain if : (2)the information system protects the integrity of transmitted information. (3)the information system employs cryptographic mechanisms to recognize changes to information during transmission unless otherwise protected by alternative physical measures.	Files may be disclosed or modified by unauthorized parties as they are transferred.	8350	6.3.4										[CobiT v5 - High Level Control Objective DSS05.03;DSS05.05;DSS06] Controls have been defined to manage data by maintaining the completeness, accuracy, availability and protection of data.
R(S)39	SYSTEM AND COMMUNICATIONS PROTECTION	NETWORK DISCONNECT	SC-10		Required	Protect -> System Communications Protection	The information system terminates the network connection associated with a communications session at the end of the session or after [no longer than 30 minutes for RAS-based sessions or no longer than 60 minutes for non-interactive user sessions] of inactivity.										Does the institution or department have policies and supporting processes in place to manner that custodians can, in accordance with the institution's policy, terminate network connections associated with a communication session and "kill" the session in a manner that cannot be circumvented by another user (Ex. examples include policies and procedures that require a session neither 1) at the end of the session, nor 2) after a period of inactivity?	Obtain system and communications protection policy; procedures addressing network disconnect; information system design documentation; organization-defined time period of inactivity before network disconnect; information system configuration settings and associated documentation; other relevant documents or records and ascertain if : (2)the organization defines in the security plan, explicitly or by reference, the time period of inactivity before the information system terminates a network connection. (3)the information system terminates a network connection at the end of a session or after the organization-defined time period of inactivity.	Lack of network connection controls over communications sessions may result in unauthorized access to information systems	8350	6.1.5										[CobiT v5 - High Level Control Objective APO13; DSS05]Controls have been defined to ensure system security by defining IT security policies, procedures and standards, and monitoring, detecting, reporting security vulnerabilities and incidents.
R(S)40	SYSTEM AND COMMUNICATIONS PROTECTION	CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT	SC-12	Required	Required (2,3)	Protect -> System Communications Protection Protect -> Cryptography	The organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with [Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction]. Control Enhancement: (2) CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | SYMMETRIC KEYS The organization produces, controls, and distributes symmetric cryptographic keys using [Selection: NIST-compliant; NSA-approved key management technology and processes]. (3) CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | ASYMMETRIC KEYS The organization produces, controls, and distributes asymmetric cryptographic keys using [Selection: NSA-approved key management technology and processes; approved PKI Class 3 certificates and certificates or prepositioned keying material; approved PKI Class 3 or Class 4 certificates and hardware security tokens that protect the user's private key].										Does the institution or department have documented policies and supporting processes in place that effectively manage the lifecycle of encryption keys? Including: (a) access to cryptographic keys to the fewest number of custodians necessary; (b) storing cryptographic keys securely in the fewest possible locations and forms; (c) preventing unauthorized substitution of cryptographic keys; (d) splitting knowledge among key custodians and establishing dual control of cryptographic keys; and (e) obtaining acknowledgements from cryptographic key custodians stating that they understand and accept their key custodian responsibilities.	Obtain system and communications protection policy; procedures addressing cryptographic key management and establishment; NIST Special Publications 800-56 and 800-57; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records and ascertain if: (2)the organization establishes and manages cryptographic keys using automated mechanisms with supporting procedures or manual procedures, when cryptography is required and employed within the information system.	Cryptographic keys are modified, lost, destroyed or disclosed to unauthorized parties.	8350	6.3.2										[CobiT v5 - High Level Control Objective DSS01;DSS04;DSS05;DSS06] Controls have been defined to manage data by maintaining the completeness, accuracy, availability and protection of data.
R(S)41	SYSTEM AND COMMUNICATIONS PROTECTION	CRYPTOGRAPHIC PROTECTION	SC-13	Required	Required	Protect -> System Communications Protection Protect -> Cryptography	The information system implements [Assignment: organization-defined cryptographic uses and type of cryptography required for each use] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.										Does the institution or department have policies and supporting processes in place that provide requirements for encryption in situations where encryption should be applied; and (a) use of appropriate level of encryption strengths based on current practices, and in compliance with State and Federal requirements?	Obtain system and communications protection policy; procedures addressing use of cryptography; FIPS 140-2 (as amended); NIST Special Publications 800-56 and 800-57; information system design documentation; information system configuration settings and associated documentation; cryptographic module validation certificates; other relevant documents or records and ascertain if : (2)the information system implements cryptographic mechanisms that comply with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.	Encryption and other cryptographic controls are inconsistently used to protect information assets and devices with policy.	8350	6.3.2										[CobiT v5 - High Level Control Objective DSS01;DSS04;DSS05;DSS06] Controls have been defined to manage data by maintaining the completeness, accuracy, availability and protection of data.
R(S)42	SYSTEM AND COMMUNICATIONS PROTECTION	COLLABORATIVE COMPUTING DEVICES	SC-15	Required	Required	Protect -> System Communications Protection	The information system: a. Prohibits remote activation of collaborative computing devices with the following exceptions: [Assignment: organization-defined exceptions where remote activation is to be allowed]; and b. Provides an explicit indication of use to users physically present at the devices.										Does the institution or department have policies and practices in place to minimize security exposure from collaborative computing devices (Ex. examples include video conferencing, microphones, etc.)? (Note: examples include proper baseline secure configuration of such devices, restriction on remote activation of collaborative computing devices, etc.).	Obtain system and communications protection policy; procedures addressing collaborative computing; access control policy and procedures; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records and ascertain if : (1)the information system prohibits remote activation of collaborative computing mechanisms and provides an explicit indication of use to the local users.	Unauthorized parties gain access to sensitive, secure areas due to the lack of implemented physical security controls.	8350	6.3.6										[CobiT v5 - High Level Control Objective DSS01; DSS05] Controls have been defined to manage IT physical environment to protect IT assets from access, damage or theft.
R(S)43	SYSTEM AND COMMUNICATIONS PROTECTION	PUBLIC KEY INFRASTRUCTURE CERTIFICATES	SC-17		Required	Protect -> System Communications Protection	The organization issues public key certificates under an [Assignment: organization-defined certificate policy] or obtains public key certificates from an approved service provider.										Does the institution or department issue public key certificates under an appropriate certificate policy or obtain public key certificates from an appropriate certificate policy from an approved service provider? (Note: A public key certificate (also known as a digital certificate or identity certificate) is an electronic document that uses a digital signature to bind a public key with an identity or information such as the name of a person or organization, their address, and so forth. A certificate can be used to verify that a public key belongs to an individual. For example, in a PKI, certificates are issued for keys to private in situations that include access to corporate resources, external business partner communications, or computers that do not run a Kerberos V5 authentication protocol. This assumes that at least one trusted root CA is safeguarded on your network and that client computers have an associated computer certificate.)	Obtain system and communications protection policy; procedures addressing public key infrastructure certificates; public key certificate policy or policies; public key issuing process; NIST Special Publication 800-32; other relevant documents or records and ascertain if : (2)the organization issues public key certificates under an appropriate certificate policy or obtains public key certificates under an appropriate certificate policy from an approved service provider.	Cryptographic keys are modified, lost, destroyed or disclosed to unauthorized parties.	8350	6.3.2.3										[CobiT v5 - High Level Control Objective DSS01;DSS04;DSS05;DSS06]Controls have been defined to manage data by maintaining the completeness, accuracy, availability and protection of data.

	Security Control Family	Control Name	NIST 800-53 Control #	Low (Control and Control Enhancements)	MODERATE (Control and Control Enhancements)	Security Program Area (Function Area or Functional Sub-Area)	NIST 800-53 Rev. 4 Control (Control and Control Enhancements) Detailed breakdown of required controls	Vendor's Response (Please Address all the controls and control enhancements in DETAIL. Controls and Enhancements identified in Column H)	Overall Control(s) Implementation Status (Reference on Comments Page) Please select from Drop down (Lower right corner)	Where does the Control(s) originate from? Please select from Drop down (Lower right corner)	Supporting Documentation (Policies and procedures must be explicitly referenced (title and date or version) so that it is clear which document is being referred to. Section numbers or similar mechanisms should allow the reviewer to easily find the	Vendor's Compensating Controls (If Control Can't Be Met - What is the alternative security controls employed by organization)	Vendor Non-Compliance (If you can't meet this control at all please explain why) (Please See Risk Statement for examples of Non-Compliance language Column R)	General Assessment Questions	Detailed Control Testing Procedure(s)	Risk Statement Examples	SOA Policy Number 1	SOA SubSection 1	SOA Policy Number 2	SOA SubSection 2	SOA Policy Number 3	SOA SubSection 3	SOA Policy Number 4	SOA SubSection 4			Arizona Breach Notification A.R.S. § 44-7501	Arizona Computer Tampering A.R.S. § 13-2316	COBIT Reference (Control Objective)
RIS44	SYSTEM AND COMMUNICATIONS PROTECTION	MOBILE CODE	SC-18		**Required**	Protect -> System Communications Protection	The organization: a. Defines acceptable and unacceptable mobile code and mobile code technologies; b. Establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and c. Authorizes, monitors, and controls the use of mobile code within the information system.							Is the institution or department established policy and supporting procedures related to mobile code development or acquisition to minimize risk of introduction of unacceptable mobile code within the information system? (ex: Mobile code technologies include, for example, Java, JavaScript, ActiveX, PDF, postscript, Shockwave movies, Flash animations, and VBScript. The development of mobile code for organizational information systems are based on the potential for the code to cause damage to the system if used maliciously.)	Obtain system and communications protection policy procedures addressing mobile code; mobile code usage restrictions, mobile code implementation guidance; NIST Special Publication 800-28; other relevant documents or records and ascertain if: (1)the organization establishes usage restrictions and implementation guidance for mobile code technologies based on the potential to cause damage to the information system if used maliciously; (2)the organization authorizes, monitors, and controls the use of mobile code within the information system.	Unauthorized mobile code disrupts the production environment due to lack of built-in security controls.	8360	6.3.5											[Cobit5 v5 - High Level Control Objective APO13: DSS05]Controls have been defined to ensure system security by defining IT security policies, procedures and standards, and monitoring, detecting, reporting security vulnerabilities and incidents.
RIS45	SYSTEM AND COMMUNICATIONS PROTECTION	VOICE OVER INTERNET PROTOCOL	SC-19		**Required**	Protect -> System Communications Protection	The organization: a. Establishes usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously; and b. Authorizes, monitors, and controls the use of VoIP within the information system.							Is the institution or department documented and established usage restrictions and implementation guidance for Voice Over Internet Protocol (VoIP) technologies based on the past to the institution and risk? (Note: implementation guidance could offer solutions such as authentication using the MAC address on IP phone; disabling automatic registration function of the call processing server).	Obtain system and communications protection policy procedures addressing VoIP; NIST Special Publication 800-58; VoIP usage restrictions; other relevant documents or records and ascertain if: (1)the organization establishes usage restrictions and implementation guidance for Voice over Internet Protocol technologies based on the potential to cause damage to the information system if used maliciously; (2)the organization authorizes, monitors, and controls the use of VoIP within the information system.	Users have access to networks that they are not authorized to use.	8360	6.3.7											[Cobit5 v5 - High Level Control Objective APO13, DSS02, DSS05] Controls have been defined to ensure system security by defining IT security policies, procedures and standards, and monitoring, detecting, reporting security vulnerabilities and incidents.
RIS46	SYSTEM AND COMMUNICATIONS PROTECTION	SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)	SC-20	**Required**	**Required**	Protect -> System Communications Protection	The information system: a. Provides additional data origin and integrity artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries; and b. Provides the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.							Is the institution or department implemented the DNS server service in a manner that supports cryptographically signed responses and it validates DNS results to reduce risk of traffic diversion through DNS spoofing, cache poisoning, etc.? (Note: example of enhancement could include separation of external and internal DNS, validating DNS results, etc.).	Obtain system and communications protection policy; procedures addressing secure name/address resolution service (authoritative source); NIST Special Publication 800-81; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records and ascertain if: (1)the information system; (if the system provides a name/address resolution service); provides artifacts for name/address resolution service that support assertion and data integrity artifacts along with the authoritative data it returns in response to resolution queries; (2)the information system, when operating as part of a distributed, hierarchical namespace, provides the means to indicate the security status of child subspaces and (if the child supports secure resolution services) enable verification of a chain of trust among parent and child domains.	Networks and supporting infrastructure are exposed to unauthorized parties due to lack of defined network security and administration policies, procedures and standards.	8360	6.3.9											[Cobit5 v5 - High Level Control Objective APO13, DSS02, DSS05] Controls have been defined to ensure system security by defining IT security policies, procedures and standards, and monitoring, detecting, reporting security vulnerabilities and incidents.
RIS47	SYSTEM AND COMMUNICATIONS PROTECTION	SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER)	SC-21	**Required**	**Required**	Protect -> System Communications Protection	The information system requests and performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.							Does the institution or department have documented processes on secure addressing practices and mechanisms to verify the authenticity and integrity of name/address resolution (such as recursive resolving or caching domain name system (DNS) servers)?	Obtain processes addressing secure addressing practices and ascertain if the organization performs data origin authentication and data integrity verification on the name/address resolution responses (such as recursive resolving or caching domain name system (DNS) servers)	Lack of procedures to verify the authenticity and data integrity of the name/address resolution responses might result in potential breaks to the chain of trust in the DNS infrastructure.	8360	6.3.9											[Cobit5 v5 - High Level Control Objective DSS01,DSS04,DSS05,DSS06] Controls have been defined to manage data by maintaining the completeness, accuracy, availability and protection of data.
RIS48	SYSTEM AND COMMUNICATIONS PROTECTION	ARCHITECTURE AND PROVISIONING FOR NAME / ADDRESS RESOLUTION SERVICE	SC-22	**Required**	**Required**	Protect -> System Communications Protection Protect -> Enterprise Architecture, Roadmap & Emerging Technology	The information systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation.							Is the institution or department implemented the DNS architecture in a manner that addresses fault tolerance and appropriate security (e.g. reduce risk of traffic diversion through DNS spoofing, cache poisoning, etc.)? (ex: example of proper security includes separation of external and internal DNS results.)	Obtain system and communications protection policy; procedures addressing architecture and provisioning for name/address resolution service; access control policy and procedures; NIST Special Publication 800-81; information system design documentation; assessment results from independent, testing organizations; information system configuration settings and associated documentation; other relevant documents or records and ascertain if: (1)the information systems that collectively provide name/address resolution service for an organization are fault tolerant and implement role separation.	Information systems fail due to improper fault tolerant or redundant architectures.	8360	6.3.9											[Cobit5 v5 - High Level Control Objective BAI03, DSS02]Controls have been defined for the acquisition and maintenance of technology infrastructure to ensure that the platforms that support the business applications are aligned with defined IT architecture and technology standards.
RIS49	SYSTEM AND COMMUNICATIONS PROTECTION	SESSION AUTHENTICITY	SC-23		**Required**	Protect -> System Communications Protection	The information system protects the authenticity of communications sessions.							Is the institution or department have a control in place to protect the authenticity of communications sessions? (Note: For example, this control addresses man-in-the-middle attacks including session hijacking or insertion of false information into a session. This control is only implemented where deemed necessary by the institution (e.g., sessions in service-oriented architecture providing web-based services))	Obtain system and communications protection policy; procedures addressing session authenticity; NIST Special Publications 800-52, 800-77, and 800-95; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records and ascertain if: (1)the information system provides mechanisms to protect the authenticity of communications sessions.	Unauthorized users access operating systems by physically or logically accessing valid inactive and/or unattended sessions.	8360	6.3.8											[Cobit5 v5 - High Level Control Objective APO13: DSS05]Controls have been defined to ensure system security by defining IT security policies, procedures and standards, and monitoring, detecting, reporting security vulnerabilities and incidents.
RIS50	SYSTEM AND COMMUNICATIONS PROTECTION	PROTECTION OF INFORMATION AT REST	SC-28		**Required (1)**	Protect -> System Communications Protection	The information system protects the [Selection (one or more): confidentiality; integrity] of [Assignment: organization-defined information at rest]. Control Enhancement: SC-28 PROTECTION OF INFORMATION AT REST Control: The information system protects the [Selection (one or more): confidentiality; integrity] of [Assignment: organization-defined information at rest].							Is the institution or department provide controls for the protection of confidentiality and integrity of information at rest. (Information at rest refers to the state of information when it is located on a secondary storage device (e.g., disk drive, tape drive) within an organizational information system. Institutions may choose to employ different mechanisms to achieve confidentiality and integrity protections, as appropriate)	Obtain system and communications protection policy; procedures addressing protection of information at rest; information system design documentation; information system configuration settings and associated documentation; cryptographic mechanisms and associated configuration documentation; list of information at rest requiring confidentiality and integrity protections; other relevant documents or records and ascertain if: (1) if the information system protects the confidentiality and integrity of information at rest.	Sensitive data is exposed to unauthorized disclosure or modification while in storage.	8360	6.3.10											[Cobit5 v5 - High Level Control Objective DSS01,DSS04,DSS05,DSS06] Controls have been defined to manage data by maintaining the completeness, accuracy, availability and protection of data.
RIS51	SYSTEM AND COMMUNICATIONS PROTECTION	PROCESS ISOLATION	SC-39	**Required**	**Required**	Protect -> System Communications Protection	The information system maintains a separate execution domain for each executing process.							Is the institution or department have established mechanisms to securely control communications and interfaces between the system processes (such that one process cannot modify the executing code of another process)?	Obtain procedures addressing process isolation and ascertain if: (1) information systems maintain separate execution domains for each executing process (2) Each information system process has a distinct address space to securely control the communications and interfaces between the two processes (such that one process cannot modify the executing code of another process)	Insufficient segregation of communications and interfaces between the system processes, may expose sensitive information resources to unauthorized access.													[Cobit5 v5 - High Level Control Objective DSS01,DSS04,DSS05,DSS06] Controls have been defined to manage data by maintaining the completeness, accuracy, availability and protection of data.
RIS52	SYSTEM AND INFORMATION INTEGRITY	SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES	SI-1	**Required**	**Required**	Protect -> Enterprise Architecture, Roadmap & Emerging Technology	The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls; and b. Reviews and updates the current: 1. System and information integrity policy [at least every 3 years]; and 2. System and information integrity procedures [at least annually].							Is the institution or department have documented policy or other directive(s) that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. (Note: this may be embedded in institution's IT policy, change management processes, security policy, etc.)	Obtain system and information integrity policy and procedures; other relevant documents or records and ascertain if: (1)the organization develops and documents system and information integrity policy and procedures. (2)the organization disseminates system and information integrity policy and procedures to appropriate elements within the organization. (3)responsible parties within the organization periodically review system and information integrity policy and procedures. (4)the organization updates system and information integrity policy and procedures when organizational review indicates updates are required. (5)the system and information integrity policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance. (6)the system and information integrity policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance. (7)the system and information integrity procedures address all areas identified in the system and information integrity policy and address achieving policy-compliant implementations of all associated system and information integrity controls.	Applications fail to process correctly and accurately due to a failure to design control during application development.	8120	6.2											[Cobit5 v5 - High Level Control Objective BAI03, DSS02]Controls have been defined for the acquisition and maintenance of technology infrastructure to ensure that the platforms that support the business applications are aligned with defined IT architecture and technology standards.
RIS53	SYSTEM AND INFORMATION INTEGRITY	FLAW REMEDIATION	SI-2		**Required**	**Required (2,3)**	Detect -> Vulnerability Assessment	The organization: a. Identifies, reports, and corrects information system flaws; b. Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation; c. Installs security-relevant software and firmware updates within [Within 30 days of release of updates] of the release of the updates; and d. Incorporates flaw remediation into the organizational configuration management process. Control Enhancement: (2) FLAW REMEDIATION	AUTOMATED FLAW REMEDIATION STATUS The organization employs automated mechanisms [at least monthly] to determine the state of information system components with regard to flaw remediation. (3) FLAW REMEDIATION	TIME TO REMEDIATE FLAWS/ BENCHMARKS FOR CORRECTIVE ACTIONS The organization: (a) Measures the time between flaw identification and flaw remediation; and (b) Establishes [Assignment: organization-defined benchmarks] for taking corrective actions.							Is the institution or department have policies and supporting processes for timely identification and implementation of patches applicable information systems (e.g., operating systems, applications, databases, etc.) based on risk? (ex: An organization may consider applying a risk-based approach to prioritize their patch installations.)	Obtain system and information integrity policy; procedures addressing flaw remediation; NIST Special Publication 800-40; list of flaws and vulnerabilities potentially affecting the information system; list of recent security flaw remediation actions performed on the information system (e.g., list of installed patches, service packs, hot fixes, and other software updates to correct information system flaws); test results from the installation of software to correct information system flaws; automated mechanisms supporting flaw remediation; information system design documentation; information system configuration settings and associated documentation; list of information system flaws; information system audit records; other relevant documents or records and ascertain if: (1)the organization identifies, reports, and corrects information system flaws. (2)the organization tests software updates related to flaw remediation for hot fixes on the information system in a reasonable timeframe in accordance with organizational policy and procedures. (3)the organization addresses flaws discovered during security assessments, continuous monitoring, or incident response activities in an expeditious manner in accordance with organizational policy and procedures. (4)the organization tests information system patches, service packs, and hot fixes for effectiveness and potential side effects before installation. (5)the organization employs automated mechanisms to periodically and upon demand determine the state of information system components with regard to flaw remediation.	Security vulnerabilities may not be identified timely.	8220	6.3.1,6.3.2											[Cobit5 v5 - High Level Control Objective Deleted – ITS.3 does not refer to Service Desk as a process.]Controls have been defined for management of the service desk and incidents.
RIS54	SYSTEM AND INFORMATION INTEGRITY	MALICIOUS CODE PROTECTION	SI-3	**Required**	**Required (1,2,7)**	Detect -> Malware Protection	The organization: a. Employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code; b. Updates malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures; c. Configures malicious code protection mechanisms to: 1. Perform periodic scans of the information system [at least weekly] and real-time scans of files from external sources at [to include endpoints] as the files are downloaded, opened, or executed in accordance with organizational security policy; and 2. [Selection (one or more): block malicious code; quarantine malicious code; send alert to administrator; in response to malicious code detection] and [Assignment: organization-defined security personnel] in response to malicious code detection; and d. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system. Control Enhancement: (1) MALICIOUS CODE PROTECTION	CENTRAL MANAGEMENT The organization centrally manages malicious code protection mechanisms. (2) MALICIOUS CODE PROTECTION	AUTOMATIC UPDATES The information system automatically updates malicious code protection mechanisms. (7) MALICIOUS CODE PROTECTION	NONSIGNATURE-BASED DETECTION The information system implements nonsignature-based malicious code detection mechanisms.							Is the institution or department have policies, supporting processes and measures in guarding against, detecting, and reporting malicious software (e.g., anti-virus, anti-spyware, etc.) across applicable information systems like servers and endpoints? (Note: processes include ensuring that tools are properly deployed across applicable information systems mechanisms, as well as properly updating rules, signature, and heuristic patterns, etc.)	Obtain system and information integrity policy; procedures addressing malicious code protection; NIST Special Publication 800-83; malicious code protection mechanisms; records of malicious code protection updates; information system configuration settings and associated documentation; information system design documentation; other relevant documents or records and ascertain if: (1) if the information system prevents non-privileged users from circumventing malicious code protection capabilities.	Unauthorized, malicious code is executed on systems without authorization.	8220	6.3.3											[Cobit5 v5 - High Level Control Objective APO13, DSS02, DSS05] Controls have been defined to ensure system security by defining IT security policies, procedures and standards, and monitoring, detecting, reporting security vulnerabilities and incidents.
RIS55	SYSTEM AND INFORMATION INTEGRITY	INFORMATION SYSTEM MONITORING	SI-4	**Required**	**Required (1,2,4,5,14,16,23)**	Detect -> Security Monitoring and Event Analysis	The organization: a. Monitors the information system to detect: 1. Attacks and indicators of potential attacks in accordance with [Assignment: organization-defined monitoring objectives]; and 2. Unauthorized local, network, and remote connections; b. Identifies unauthorized use of the information system through [Assignment: organization-defined techniques and methods]; c. Deploys monitoring devices: (i) strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization; d. Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion; e. Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information; f. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations; and g. Provides [Assignment: organization-defined information system monitoring information] to [Assignment: organization-defined personnel or roles] [Selection (one or more): as needed; [Assignment: organization-defined frequency]]. Control Enhancement: (1) INFORMATION SYSTEM MONITORING	AUTOMATED TOOLS FOR REAL-TIME ANALYSIS The organization employs automated tools to support near real-time analysis of events. (4) INFORMATION SYSTEM MONITORING	INBOUND AND OUTBOUND COMMUNICATIONS							Does the institution or department have effective tools and processes in place to actively detect and respond to security events (including effectively placed and configured intrusion-detection system(s) and/or intrusion-prevention system(s) to guard against or monitor for malicious network traffic at the perimeter; effective placement and use of monitoring tools with configured applicable use cases to detect potential events relevant to the institution (e.g., DLP, SIEM, Netflow, etc.); effective monitoring processes (e.g., alerts from IDS/IPS alerts) for taking timely actions; defined processes (e.g., use cases) that guide the responders to take appropriate level of action?	Obtain system and information integrity policy; procedures addressing information system monitoring tools and techniques; information system design documentation; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; information system protocols; other relevant documents or records and ascertain if: unauthorized, security plan; other relevant documents or records and ascertain if: (1)the organization employs tools and techniques to monitor events on the information system, detect attacks, and provide identification of unauthorized use of the system. (2)the organization deploys monitoring devices strategically within the information system (e.g., at selected perimeter locations, near server farms supporting critical applications) to collect essential information. (3)the organization deploys monitoring devices at ad hoc locations within the information system to track specific transactions. (4)the organization uses the monitoring devices to track the impact of security changes to the information system. (5)the organization determines the granularity of the information collected based upon its monitoring objectives and the capability of the information system to support such activities. (6)the organization consults appropriate legal counsel with regard to all information system monitoring activities. (7)the organization heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation, based on law enforcement information, intelligence information, or other credible sources of information. (8)the organization employs automated tools to support near-real-time analysis of events. (9)the organization identifies the types of activities or conditions considered unusual or unauthorized; and (10)the organization employs automated mechanisms to monitors inbound and outbound communications for unusual or unauthorized activities or conditions. (11)the organization defines in the security plan, explicitly or by reference, indications of compromise or potential compromise to the security of the information system.	Suspicious or anomalous activities are not are not detected due to lack of intrusion detection systems.	8220	6.3.4											[Cobit5 v5 - High Level Control Objective APO13, DSS02, DSS05] Controls have been defined to ensure system security by defining IT security policies, procedures and standards, and monitoring, detecting, reporting security vulnerabilities and incidents.
RIS56	SYSTEM AND INFORMATION INTEGRITY	SECURITY ALERTS, ADVISORIES, AND DIRECTIVES	SI-5	**Required**	**Required**	Protect -> System Communications Protection	The organization: a. Receives information system security alerts, advisories, and directives from: [to include US-CERT] on an ongoing basis; b. Generates internal security alerts, advisories, and directives as deemed necessary; c. Disseminates security alerts, advisories, and directives to: [to include system security personnel and administrators with configuration/patch-management responsibilities]; and d. Implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.							Does the institution or department, receive and provide, timely security notifications and advisories to appropriate institution personnel (e.g., security advisories from external sources, institutional or departmental administrators, general security advisories like phishing scam to institutional users)?	Obtain system and information integrity policy; procedures addressing security alerts and advisories; NIST Special Publication 800-40; records of security alerts and advisories; other relevant documents or records and ascertain if: (1)the organization receives information system security alerts/advisories on a regular basis. (2)the organization issues security alerts/advisories to appropriate organizational personnel. (3)the organization takes appropriate actions in response to security alerts/advisories. (4)the organization maintains contact with special interest groups (e.g., information security forums) that: facilitate sharing of security-related information (e.g., threats, vulnerabilities, and latest security technologies); provide access to advice from security professionals. improve knowledge of security best practices.	Contacts with special interest groups or other specialists security forums and professional associations is not coordinated or performed as a result of ID defined processes.	8220	6.3.5											[Cobit5 v5 - High Level Control Objective EDM02, APO01, APO03, APO05] Controls have been defined for creation and maintenance of IT strategic plans.
RIS57	SYSTEM AND INFORMATION INTEGRITY	SECURITY FUNCTION VERIFICATION	SI-6		**Required**	Identify/verify/manage system functions /identification	The information system: a. Verifies the correct operation of [Assignment: organization-defined security functions]; b. Performs this verification [to include upon system startup and/or restart and at least monthly]; c. Notifies [to include system administrators and security personnel] of failed security verification tests; and d. [Selection (one or more): shuts the information system down; restarts the information system; [to include notification of system administrators and security personnel] when anomalies are discovered.							Does the institution or department, perform security function verification upon system startup and restart, upon command by user with appropriate privilege, periodically? Do you have a process in place for notification if the test fails	Obtain system and information integrity policy; procedures addressing security verification, and testing	Verifies that all Security Functions in the information system are well defined													
RIS58	SYSTEM AND INFORMATION INTEGRITY	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY	SI-7		**Required (1,7)**	Identify -> Privacy & Confidentiality	The organization employs integrity verification tools to detect unauthorized changes to [Assignment: organization-defined software, firmware, and information]; Control Enhancement: (1) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY	INTEGRITY CHECKS The information system performs an integrity check of [Assignment: organization-defined software, firmware, and information] [Selection (one or more): at startup; at [Assignment: organization-defined transitional states or security-relevant events]; [Assignment: organization-defined frequency]]. (7) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY	INTEGRATION OF DETECTION AND RESPONSE The organization incorporates the detection of unauthorized [Assignment: organization-defined security-relevant changes to the information system] into the organizational incident response capability.							Does the institution or department have mechanisms in place to prevent or detect unauthorized changes to critical system files (e.g., through use of file integrity monitoring (FIM) tools and monitoring processes to investigate alerts from such tools)?	Obtain system and information integrity policy; procedures addressing software and information integrity; information system design documentation; information system configuration settings and associated documentation; integrity verification tools and applications documentation; security plan; records of integrity scans; other relevant documents or records and ascertain if : (1)the information system detects and protects against unauthorized changes to software and information. (2)the organization employs commercial off-the-shelf integrity mechanisms (e.g., parity checks, cyclical redundancy checks, cryptographic hashes) in accordance with good software engineering practices and uses them to monitor software and firmware components and user installed software and applications. (3)the organization defines in the security plan, explicitly or by reference, the frequency of integrity scans on the information system; and (4)the organization reassesses the integrity of software and information by performing integrity scans of the information system in accordance with the organization-defined frequency.	Unauthorized tampering of system and/or configuration files is undetected due to the absence of file integrity mechanisms.	8220	6.3.6											[Cobit5 v5 - High Level Control Objective BAI10, BAI02, BAI03, DSS02]Controls have been defined to manage the configuration of IT hardware and software.
RIS59	SYSTEM AND INFORMATION INTEGRITY	SPAM PROTECTION	SI-8		**Required (1,2)**	Protect -> Spam Filtering Protect - Internet Content Filtering	The organization: a. Employs spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages; and b. Updates spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures. Control Enhancement: (1) SPAM PROTECTION	CENTRAL MANAGEMENT The organization centrally manages spam protection mechanisms. (2) SPAM PROTECTION	AUTOMATIC UPDATES The information system automatically updates spam protection mechanisms.							Does the institution or department have mechanisms in place to guard against and phishing attempts? (ex: mechanisms include tools and reporting processes like timely updates from vendors on signatures).	Obtain system and information integrity policy; procedures addressing spam protection; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records and ascertain if: (1)the information system implements spam protection by verifying that the organization: employs spam protection mechanisms at critical information system entry points and at workstations, servers, or mobile computing devices on the network employs spam protection mechanisms to detect and take appropriate action on unsolicited messages transported by electronic mail, electronic mail attachments, Internet accesses, or other common means.	Unauthorized information processing activities occur undetected due to lack of consistent logging and monitoring activities.	8220	6.3.7											[Cobit5 v5 - High Level Control Objective APO13, DSS02, DSS05] Controls have been defined to ensure system security by defining IT security policies, procedures and standards, and monitoring, detecting, reporting security vulnerabilities and incidents.

	Security Control Family	Control Name	NIST 800-53 Control #	Low (Control and Control Enhancements)	MODERATE (Control and Control Enhancements)	Security Program Area (Function Area -> Functional Sub-Area)	NIST 800-53 Rev. 4 Control (Control and Control Enhancements) Detailed breakdown of required controls	Vendor's Response (Please Address all the controls and control enhancements in DETAIL. Controls and Enhancements identified in Column H)	Overall Control(s) Implementation Status (Reference on Comments Page) Please select from Drop down (Lower right corner)	Where does the Control(s) originate from? Please select from Drop down (Lower right corner)	Supporting Documentation (Policies and procedure must be explicitly referenced (title and date or version) so that it is clear which document is being referred to. Section numbers or similar mechanisms should allow the reviewer to easily find the reference)	Vendor's Compensating Controls (If Control Can't Be Met - What is the alternative security controls employed by organization)	Vendor Non-Compliance (If you can't meet this control at all please explain why) (Please Sex Risk Statement for examples of Non-Compliance language Column R)	General Assessment Questions	Detailed Control Testing Procedure(s)	Risk Statement Examples	SOA Policy Number 1	SOA SubSection 1	SOA Policy Number 2	SOA SubSection 2	SOA Policy Number 3	SOA SubSection 3	SOA Policy Number 4	SOA SubSection 4				Arizona Breach Notification A.R.S. § 44-7501	Arizona Computer Tampering A.R.S. § 13-2316	COBIT Reference (Control Objective)
RI0580	SYSTEM AND INFORMATION INTEGRITY	INFORMATION INPUT VALIDATION	SI-10		**Required**	Protect -> Enterprise Architecture, Roadmap & Emerging Technology	The information system checks the validity of [Assignment: organization-defined information inputs].	[redacted]			Does the institution or department have explicit requirements for data input validation controls as part of the institution's or department's SDLC and change management processes, to prevent the altering of input provided to information systems especially web applications? (Note: many vulnerabilities to data confidentiality and integrity stem from unauthorized users manipulating data input causing issues such as SQL injection).	Obtain System and information integrity policy; procedures addressing information accuracy, completeness, validity, and authenticity; access control policy and procedures; separation of duties policy and procedures; documentation for automated tools and applications to verify accuracy, completeness, validity, and authenticity of information; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records and ascertain if: (1)the information system checks information for accuracy, completeness, validity, and authenticity by verifying that the system: checks for accuracy, completeness, validity, and authenticity of information is accomplished as close to the point of origin as possible; employs rules to check the valid syntax of information inputs to verify that inputs match specified definitions of format and content; prescreens information inputs passed to interpreters to prevent the content from being unintentionally interpreted as commands. checks the accuracy, completeness, validity, and authenticity of information to the extent guided by organizational policy and operational requirements.	Data is input into applications that cause unexpected or incorrect results, possibly crashing or placing the application in an unknown and unplanned for state.	8220	6.3.8			