	STATEWIDE **STANDARD**	**State of Arizona**

STATEWIDE STANDARD (8120): INFORMATION SECURITY PROGRAM

DOCUMENT NUMBER:	**S8120**
EFFECTIVE DATE:	**February 2, 2026**
REVISION:	**1.2**

1. AUTHORITY

To effectuate the mission and purposes of the Arizona Department of Homeland Security, the Agency shall establish a coordinated plan and program for information security and privacy protections implemented and maintained through policies, standards and procedures (PSPs) as authorized by Arizona Revised Statutes (A.R.S.)§ 41-4254 and § 41-4282.

2. PURPOSE

The purpose of this standard is to provide additional specificity to the associated policy (P8120) requirements.

3. SCOPE

3.1 Application to Budget Units (BUs) - This policy shall apply to all BUs as defined in A.R.S. § 18-101(1).

3.2 Application to Systems - This policy shall apply to all state information systems. Policy statements preceded by "(P)" are required for state information systems categorized as Protected. Categorization of systems is defined within the Information Security Program Policy.

3.3 Federal Government Information - Information owned or under the control of the United States Government shall comply with the Federal classification authority and Federal protection requirements.

4. EXCEPTIONS

4.1 PSPs may be expanded or exceptions may be taken by following the Statewide Policy Exception Procedure.

4.1.1 Existing IT Products and Services

- **a.** BU subject matter experts (SMEs) should inquire with the vendor and the state or agency procurement office to ascertain if the contract provides for additional products or services to attain compliance with PSPs prior to submitting a request for an exception in accordance with the Statewide Policy Exception Procedure.

4.1.2 IT Products and Services Procurement

- **a.** Prior to selecting and procuring information technology products and services, BU SMEs shall consider statewide information security PSPs when specifying, scoping, and evaluating solutions to meet current and planned requirements.

4.1.3 GovRAMP Exception - GovRAMP exceptions may be requested if any of the following situations apply. However, the vendor would still need to undergo an internal “AZRAMP” review by AZDOHS.

- **a.** Vendor is solely operating in the State of Arizona, and/or;
- **b.** Vendor is a small business, as defined in A.R.S. § 41-1001 , and/or;
- **c.** Vendor is an accredited higher education institution, and/or;
- **d.** A GovRAMP authorized solution will be cost-prohibitive for the BU to procure (i.e. cost more than the product itself).

BUs requesting a GovRAMP exception shall submit a detailed description of the exception request to ADOHS for review and approval.

4.2 BU has taken the following exceptions to the Statewide Policy Framework:

Section Number	Exception	Rationale

5. ROLES AND RESPONSIBILITIES

5.1 Arizona Department of Homeland Security Director shall:

a. Be ultimately responsible for the correct and thorough completion of statewide information security PSPs throughout all state BUs.

b. Ensure that by July 1 of each year all BUs have submitted the following information for approval:

1. A state information system inventory with a system classification assignment and system owner for each state information system
2. A system security plan and system security assessment plan for each Protected state information system
3. A Plan of Actions and Milestones (POAM) for each Protected state information system

c. Ensure that information security risks identified in Protected state information system risk assessment documentation are adequately addressed for all BUs.

d. Enforce a course of action where security risks are not adequately addressed. Course of action may include, but is not limited to, the following mandates:

1. Identification of a plan to address the documented risks
2. Implementation of recommended security controls
3. Independent security assessment on selected state information systems or controls
4. Hosting of state information system or state information system components in a state approved solution(s)
5. Adoption of additional security requirements or procedures for the BU or selected by State information systems, controls, or control environments

5.2 State Chief Information Security Officer (CISO) shall:

a. Provide a format for the required compliance documents;

b. Advise the Director on the completeness and adequacy of the BU

activities and documentation provided to ensure compliance with statewide information security PSPs throughout all state BUs;

c. Review and approve BU security and privacy PSPs and requested

exceptions from the statewide security and privacy PSPs;

d. Identify and convey to the State CIO the risk to state information systems and data based on a review of the BU-supplied state information system inventory, system security plans, system security assessment plans and the Plan of Actions and Milestones (POAM);

e. Identify and convey to the State CIO the risk to state information systems and data based on current implementation of security controls and mitigation options to improve security; and

f. Recommend a course of action where security risks are not adequately addressed. Course of action may include, but is not limited to, the following recommendations:

1. Identify a plan to address the documented risks
2. Implement recommended security controls
3. Perform independent security assessment on selected state information systems or controls
4. Hosting of state information system or state information system components in a state approved solution(s)
5. Adopt any additional security requirements or procedures for the BU or selected by state information systems, controls, or control environments

5.3 Enterprise Security Program Advisory Council (ESPAC) shall:

a. Advise the State CISO on matters related to statewide information security policies and standards.

5.4 BU Director shall:

a. Be responsible for the correct and thorough completion of information security PSPs within the BU;

b. Ensure BU compliance with Information Security Program Policy; and

c. Promote efforts within the BU to establish and maintain effective use

d. of state information systems and assets.

5.5 BU Chief Information Officer (CIO) shall:

a. Work with the BU Director to ensure the correct and thorough completion of statewide information security PSPs within the BU;

b. Ensure all BU managed systems have submitted the following

documents for approval by the State CIO or designated alternate by July 1 of each year:

1. A complete list of state information systems with a system classification assignment and system owner for each state information system
2. A system security plan and system security assessment plan for each Protected state information system
3. A Plan of Actions and Milestones (POAM) for each Protected state information system

c. Ensure information security risks to Protected state information systems, are adequately addressed according to the Protected state information system risk assessment documentation; and

d. Be system owner for all state information systems or delegate a system owner for BU state information systems.

5.6 BU Information Security Officer (ISO) shall:

a. Advise the BU CIO on the completeness and adequacy of the BU provided documentation and reports and recommend a course of action where security risks are not adequately addressed;

b. Ensure all system owners understand their responsibilities for the security planning, management, and authorization of state information systems; and

c. Ensure the correct execution of the system security assessment plans.

5.7 System Owner shall:

a. Be responsible for the overall procurement, development, integration, modification, or operation and maintenance of the state information system; [NIST SP 800-18]

b. Advise BU ISO as to the state information system categorization;

c. Ensure creation of required system security plans, system security assessment plans, Plan of Actions and Milestones (POAM); and

d. Ensure the implementation of information security controls as described in system security plans and POAM.

6. STATEWIDE STANDARD

6.1 System Security Plan Template - The following template may be used to create a state system security plan.

6.1.1 State System Name/Title: Unique identifier and name of the state information system.

6.1.2 State System Categorization: [Assign a single system categorization to the identified state information system according to the requirements in the Information Security Program Policy (P8120), requirements 6.3.1 – 6.3.3.]

a. Standard; or
b. Protected

6.1.3 Information System Owner: Assign an owner to the identified state information system. An owner must be a state employee and has the overall responsibility for procurement, development, integration, modification, or operation and maintenance of the state information system.

6.1.4 Authorizing Official: [Document the authorizing official for the state information system. An authorizing official has the authority to formally assume responsibility for operating the state information system at an acceptable level of risk to BU operations or assets.]

	State Information System Owner	Authorizing Official
Name		
Title		
Agency		
Address		
Email Address		
Phone Number		

6.1.5 Other Designated Contacts: [List the other key personnel associated with the operations and maintenance of the state information system.]

6.1.6 Assignment of Security Responsibility: [List the personnel assigned to security responsibilities with the state information system.]

	1	2
Name		
Title		
Agency		
Address		
Email Address		
Phone Number		

6.1.7 State Information System Operational Status: [Indicate the current operational status of the state information system. If required, indicate specific parts or subsystems of the state information system if more than one status is selected.]

	System Name	Subsystem Name (use if needed)
Operational		
Under Development		
Major Modification		

6.1.8 Information System Type: [Indicate the type of system: Major Application – An application that requires special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application; or General Support System – An interconnected set of information resources under the same direct management control that shares common functionality (including hardware, software, information, data, minor applications, communications, and people).]

6.1.9 General System Description/Purpose: [Describe the function or purpose of the system and the information processes.]

6.1.10 System Environment: [Provide a general technical description of the state information system. Include hardware, software, and communications equipment.]

6.1.11 System Interconnections/Information Sharing: [List interconnected systems and system identifiers, indicate if there is an agreement on file (e.g., Information Sharing Agreement, Memorandum of Understanding, Service Level Agreement, or other agreement), date of agreement, and name of authorizing official.]

System Name	Business Unit	Type	Agreement	Date	Official

6.1.12 Related Laws/Regulations/Policies: [List any laws or regulations that establish specific security or privacy requirements for the state information system or data residing on the system. State PSPs may be used for guidance but only include relevant and applicable laws and regulations.]

6.1.13 Minimum Security Control Exceptions: *[Minimum Security Controls are based on the categorization of the system and the statewide security and privacy policy set.* List any exceptions with the statewide security and privacy policies below or planned controls (e.g., controls not yet in place but budgeted and planned, together with rationale, compensating controls for the exception, and expected date of implementation for planned controls.)]

Policy #	Policy Name	Exceptions	Compensating Controls	Rationale for Exception
P8110	Data Classification	[None / List Exceptions]		
P8120	Information Security Program	[None / List Exceptions]		
P8130	System Security Acquisition	[None / List Exceptions]		
P8210	Security Awareness Training	[None / List Exceptions]		
P8220	System security Maintenance	[None / List Exceptions]		
P8230	Contingency Planning	[None / List Exceptions]		
P8240	Incident Response Planning	[None / List Exceptions]		
P8250	Media Protection Policy	[None / List Exceptions]		
P8260	Physical Protections	[None / List Exceptions]		
P8270	Personnel Security Controls	[None / List Exceptions]		
P8280	Acceptable Use	[None / List Exceptions]		
P8310	Account Management	[None / List Exceptions]		
P8320	Access Control	[None / List Exceptions]		
P8330	System Security Audit	[None / List Exceptions]		
P8340	Identification and Authentication	[None / List Exceptions]		
P8350	System and Communication Protection	[None / List Exceptions]		
P8410	System Privacy	[None / List Exceptions]		

6.1.14 State Information System Security Plan Dates: [List completion date of plan, approval date of plan, along with approver.]

	Security Plan Completion	Security Plan Approval
Name		
Title		
Date		

6.2 Security Risk Assessment Guidance – The following guidance is provided for the performance of information security risk assessments. This guidance is presented within the context of the phases of an information security risk assessment process. Namely, the preparation, the performance, and the communication of the results for an information security risk assessment.

6.2.1 Information Security Risk Assessment Preparation: Preparation for an information security risk assessment helps to ensure that the business unit derives the most value from this exercise and establishes the context of the risk management process. Business units shall consider the following steps in preparing for an information security risk assessment.

a. Identify Purpose: The obvious purpose for an information security risk assessment is to provide information to the system owners regarding the risk to sensitive data and critical systems so that they may make appropriate decisions regarding how to address those risks. However, information security risk assessments are also required periodically based on applicable regulations, provide oversight to the security operations of the system, or could be the direct (and required) action from a recent audit or inspection. It is important that the business unit clearly understand and identify the purpose of the information security risk assessment and convey that to the team performing and overseeing the assessment in order to ensure project success.

b. Define Assessment Boundaries: An information security risk assessment shall be limited to defined physical and logical boundaries. A physical boundary identifies the physical limit of the assessment such as network components (e.g., workstations, servers, routers, switches), security components (e.g., IDS, firewalls), network media (e.g., cabling), peripherals, buildings, and rooms. A logical boundary identifies the logical limit of the assessment such as the functions of the system, services provided, applications, and network segments.

c. Define Level of Rigor: An information security risk assessment shall have a defined level of rigor specifying the depth of analysis to be performed. The level of rigor may be specified by hours (or other resources metrics) to be expended, or by listing the methods of data gathering.

d. **Document Scope Limitations and Constraints:** An information security risk assessment is generally expected to cover all relevant administrative, technical, and physical controls. When the scope is limited or constraints are placed on the task of assessing the risk to the state information system the budget unit needs to ensure that these constraints are reasonable. If a budget unit chooses to limit the scope of the risk assessment (e.g., physical security controls are out of scope) then there should be some rationale provided on why such a limitation is reasonable (e.g., physical security controls are reviewed under another assessment program).

e. **Document Risk Model:** There are a variety of reasonable security risk models that may be used in the performance of an information security risk assessment (e.g., NIST 800-30). The budget unit (or the contractor for the budget unit) may use any reasonable security risk model provided the model accounts for the following aspects of a baseline information security risk assessment:
    1. **Document Risk Elements:** The information security risk model shall identify and document the elements to be reviewed, assessed, and analyzed in order to determine the risk to the state information system. These elements typically include: threats, assets, vulnerabilities, likelihood, and impact.
    2. **Document Risk Calculation:** The information security risk model shall identify the process by which risk is determined. This is typically in the form of a risk calculation, estimate based on parameters, or a risk determination table based on the risk elements listed above.

6.2.2 Information Security Risk Assessment Performance: The effective performance of an information security risk assessment is critical to the accuracy and usefulness of the assessment. Business units shall consider the following steps in the performance of an information security risk assessment.

a. **Objectivity:** Consistent with requirement 6.5.2 of P8120 (Information Security Program Policy), an information security risk assessment shall be performed by impartial assessors or assessment teams. Impartiality requires that the assessment team have no conflict of interest between the development, selection, and/or operation of the security controls under assessment.

b. **Adequate Data Gathering:** An information security risk assessment shall have adequate data gathered on the controls within the physical and logical boundaries of the assessment. Adequacy of the data gathering is

largely subjective but BUs shall be hesitant to rely on information security risk assessments that have too few data points to draw an accurate conclusion or assessments that rely on interviews of surveys alone from those in charge of the assessed controls. To the extent possible the BU should ensure that effective data gathering approaches from reviewing documents, interviewing personnel, observing behavior, inspecting controls, and testing controls are utilized.

c. **Defendable Analysis:** An information security risk assessment shall include a documented and defendable analysis of the data gathered to support findings. Information security risk assessments typically provide such analysis in the form of tables or charts. Each finding / recommendation shall be traceable to sufficient evidence of the vulnerability that is being addressed.

6.2.3 Information Security Risk Assessment Documentation: The effective and accurate communication of results from an information security risk assessment is critical to the usefulness of the assessment. Business units shall consider the following steps in the documentation of an information security risk assessment.

a. **Communication with Key Staff:** The results of an information security risk assessment provide pertinent information and guidance to system owners, information security officers, and chief information officers within the budget unit. The results of the assessment shall be shared with budget unit director, CIO, information security officer, and system owners at a minimum. The state CISO may also be included in the dissemination of the assessment results.

b. **Communication with Custodians and Others:** The results of the information security risk assessment includes recommendations for improvements (e.g., patch systems, develop procedures, implement additional controls) that will need to be conveyed to those in charge of implementing these changes. When relevant, all available evidence of the associated vulnerabilities and details of the recommended solutions shall be made available to the system custodians, staff members, or contractors tasked with confirming the vulnerability and/or implementing the recommended solution. Keep in mind that the principle of least privilege shall be applied here and there may be some details deemed irrelevant and sensitive and therefore not conveyed to others.

c. **Clear Recommendations:** An information security risk assessment shall provide a report with clear recommendations that identify the control gap or risk and the recommended solution or solution set to address the

control gap or risk. Business units may want to require that the information security risk assessment recommendations provide information on the cost of the recommendation as well.

6.2.4 Vulnerability Scanning – All State of Arizona agencies shall perform ongoing vulnerability scanning using an industry standard automated tool supported by the statewide enterprise vulnerability management solution. Vulnerabilities should be regularly remediated to insure that potential risks have been mitigated.

a. All devices connected to State of Arizona agency networks shall be scanned and uploaded at least twice monthly into the Statewide enterprise vulnerability management solution.

b. Equipment specific plug-ins shall be enabled within the scan policy.

c. Credentialed or agent-based scans shall be used on all devices. Scans using credentials shall be periodically validated to ensure the credentials work properly.

d. When conducting scans, the automated vulnerability scanning tool shall have full access to all devices connected to the agency network without restrictions through hardware or software firewalls, intrusion detection/prevention systems or other intermediary devices or software.

e. Review the statewide enterprise vulnerability management solution twice monthly for awareness of the risk score and ensure proper management of vulnerabilities and risk.

f. Validate scanned asset inventory in the statewide enterprise vulnerability management solution twice monthly to ensure elimination of duplicate information and identification and reduction of unknown or retired devices.

g. The State CISO, or delegate, will periodically review agency compliance with vulnerability scanning policies and standards.

6.3 Third Party (Cloud Service Providers and other Vendors) Risk Assessment Guidance – The following guidance is provided for the performance of third party security risk assessments. This guidance is presented utilizing the guidance from NIST Cybersecurity Framework (NIST CSF) the context of the phases of an information security risk assessment process. Namely, vendor risk process identification, vendor identification, contract management, vendor risk assessment, and continuity testing.

6.3.1 Vendor Risk Management Process - Vendor risk management processes are identified, established, assessed, managed, and agreed to by BU stakeholders.

[NIST 800-53 SA-9, PM-9, CSF ID.SC-1]

6.3.2 **Cloud Products Third Party Risk Assessments** – The Business Unit (BU) must utilize the GovRAMP program to conduct a risk assessment, as applicable, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, modification, or destruction of confidential data by third parties authorized by the BU to process, store, or transmit such data.

6.3.3 The BU must develop a vendor risk management process that is most appropriate for the entity.

- **a.** Determine needs, measurement approach, vendor selection, define contract term, monitor relationship, end contract.
- **b.** Identify the owner of the vendor risk management process.

6.3.4 Prior to publishing a Solicitation related to a cloud product, the BU System Owner shall assess the product's/system's data impact level considering the following:

- **a.** Data the BU plans to provide to the cloud provider and its classification (as defined under P8110 6.2);
- **b.** Impact to critical infrastructure; and
- **c.** Any associated regulatory compliance needs.

6.3.5 Matrix 1 is provided to BUs to conduct the aforementioned assessment.

6.3.6 Based on the data impact level, the BU System Owner shall select the appropriate GovRAMP Security Designation Level required for the procurement to be defined within the solicitation for the product. There are three GovRAMP Security Designation Levels: GovRAMP Snapshot, Core, and Provisionally Authorized/ Authorized. ADOHS/BUs shall ensure compliance with NIST 800-53 Rev 5 (or current) based on third-party assessments provided by GovRAMP, FedRAMP, and/or by the ADOHS exception process identified in Section 4 of this Standard.

6.3.7 Any additional security requirements, such as regulatory compliance including, but not limited to CJIS, HIPAA, etc, shall also be determined by AZDOHS and incorporated into the contract terms (see Matrix 1).

6.3.8 As noted in Matrix 1, for confidential data stored, transmitted, and processed in protected systems or systems that maintain critical infrastructure, a verified level of GovRAMP Core may be required to satisfy ADOHS' minimum requirements. If applicable, this level must be achieved no later than 12 months from contract execution. Should the BU require a higher-level of Provisionally Authorized/Authorized, this requirement shall be included in the solicitation, and the products must meet this status within the

timeframe outlined in the resulting contract, which shall be in conformance with the timeframes below:

a. If a verified status of Core is required, the status must be achieved no later than 12 months of the resulting contract effective date.

b. If a verified status of Authorized is required, a provider will be allowed a minimum of 18 months from contract effective date to ensure the contracted product has achieved Authorized status, not to exceed 24 months.

6.3.9 Upon contract award, if the protected system that maintains critical infrastructure or stores, transmits, or processes confidential data does not hold the appropriate GovRAMP Security Designation Level of GovRAMP Core or GovRAMP Authorized, the provider will be required to participate in the GovRAMP Progressing Snapshot program prior to any data being transferred, stored, or processed. The provider will be expected to make progress on a quarterly basis. Alternatively, a provider may also provide a letter from the GovRAMP Project Management Office indicating that the product currently holds an Active, In Process, or Pending status, indicating that the product is in the pipeline to receive a GovRAMP Ready, Provisionally Authorized, or Authorized status.

To use Matrix 1, BUs should first look at Column 1 and determine what "data type" will be processed, stored, or transmitted by the cloud product. There are four rows in Matrix 1 which correspond with the types of data for the purposes of this assessment. Column 2 lists a handful of examples of various laws, regulations, and security policies that may apply to the types of data listed in Column 1. The examples are provided for illustrative purposes only, in order to give BUs an idea of the types of regulatory authorities that may apply to their data. However, other authorities may also apply and BUs are expected to be familiar with the various authorities that apply to their particular data. Column 3 contains the corresponding data classification types (reference: AZ Statewide Policy 8110 - Data Classification). Column 4 will assist BUs in determining the minimum security designation based on whether the product maintains critical infrastructure as defined in A.R.S. § 41-1801.[1] *Lastly, BUs should refer to Column 5 to determine which minimum security designation level applies to their cloud product based on the information in columns 1 through 4. BUs may select higher levels for cloud products than required by the matrix if it is in their best interest. Each of the GovRAMP designation levels require different NIST 800-53 controls to be in place. Additional information on GovRAMP statuses and the controls required for authorization under them can be found at https://govramp.org/providers/.*

[1] "Critical infrastructure" means systems and assets, whether physical or virtual, that are so vital to this state and the United States that the incapacity or destruction of those systems and assets would have a debilitating impact on security, economic security, public health, or safety.

Matrix 1

1 - Data Type	2 - Compliance / Regulatory Requirement	3 - Data Sensitivity Classification as defined under Statewide Policy 8110 Sec. 6.2	4 - Maintains Critical Infrastructure as defined in A.R.S. § 41-1801	5 - Minimum Security Designation Level Required
Data that is not required to be kept confidential by law, by contract, for business reasons, or for any other reason and/or is already available to the public (i.e. subject to disclosure under Arizona Public Records Law, already posted on a State website, or has been distributed to the public).	None	Public	No	GovRAMP Core (GovRAMP Authorized is required if product maintains critical infrastructure–i.e answer to column 4 would be yes)
Data that is confidential by law, by contract, for business reasons, or for any other reason		Confidential	No	GovRAMP Core
Data that includes PII, PHI, FTI, PCI Data, SSA Data, education records, unemployment records, any other information that is required to be kept confidential by law, by contract, for business reasons, or for any other reason	IRS Pub 1075, HIPAA, PCI DSS, CMS, FISMA, 20 CFR 603, FERPA, others as applicable	Confidential	Yes	GovRAMP Authorized
Criminal Justice Information System (CJIS) Data	CJIS Security Policy	Confidential	Not a determining factor for this data type	GovRAMP Authorized + CJIS Overlay

6.3.10 Professional Services Applicability - If a professional services provider uses a cloud-based product that processes State data and is not owned by the professional services provider, the BU, at its sole discretion, may require that the provider facilitate compliance with the security requirements outlined in this section for the product(s). The BU shall assess any data security risks in determining the applicability of the requirement of this section to a professional service provider, such as considering and assessing the criteria in Matrix 1.

6.3.11 FedRAMP Products - For products that hold a FedRAMP Rev. 5 status and require a GovRAMP Core or GovRAMP Authorized Designation Level (as determined by the BU), providers are required to ensure the cloud product has enrolled in the GovRAMP Fast Track program to ensure ADOHS has access to continuous monitoring reports.

6.3.12 Continuous Monitoring - Providers with cloud products that require a GovRAMP Core or GovRAMP Authorized Designation Level (as determined by the BU) must ensure that ADOHS is provided access to continuous monitoring reports and progressing reports for each product offered within 10 business days of ADOHS's request for access and for the lifecycle of the executed contract.

AZDOHS shall utilize GovRAMP's Continuous Monitoring program to review the monthly, quarterly, and/or annual reports for products. GovRAMP Continuous Monitoring can be requested for Standard Access or Elevated Access.

a. **Standard Access:** For cloud products with a Low or Moderate security category, service providers will upload packages to GovRAMP Box Portal. Documents include:

    1. POA&Ms (Plan of Action and Milestones)
    2. An updated inventory workbook
    3. OS, DB, and web application vulnerability scans
    4. Deviation Request Form to support POA&M Risk Adjustments, Operational Requirements, and False Positives
    5. Executive summary of the above items

b. **Elevated Access:** Includes all documentation included in Standard Access and access to a product's System Security Plan (SSP), Security Assessment Plan (SAP), and/or Security Assessment Report (SAR).

c. **Progress Reporting:** If a product is participating in the GovRAMP Progressing Snapshot program but it requires GovRamp Core or GovRAMP Authorized, access to progress reports may be requested to ensure that a product's security posture is improving on a quarterly basis.

6.3.13 Vendor Identification - Vendors are identified, prioritized, and assessed using a vendor risk assessment process. [NIST 800-53 RA-2, RA-3, SA-15, PM-9, CSF ID.SC-2]

a. Identify all manufacturers, service providers, contactors, and external staff.

b. Determine a "choke point" or company process that would allow the most efficient and effective identification of all vendors. For many BUs this could be the procurement or legal department. The procurement process should include vendor identification and inventory process and a vendor risk management process.

6.3.14 Vendor Contracts - Contracts with vendors are used to implement appropriate measures designed to meet the objectives of a BU's information security program and vendor risk management plan. [NIST 800-53 SA-9, SA-11, PM-9, CSF ID.SC-3]

Require the following measures to reduce vendor risk:

- **a.** References
- **b.** Financial stability
- **c.** Liability insurance
- **d.** Regulation knowledge
- **e.** Background checks
- **f.** Service Level Agreements
- **g.** Business Continuity and Disaster Recovery Requirements
- **h.** Data Confidentiality, privacy, and destruction
- **i.** Security and Privacy incident notification
- **j.** Ensure vendors meet and maintain applicable GovRAMP and other State information security requirements

All contracts for cloud products must include the data impact level associated and the GovRAMP assessment requirements, as applicable.

6.3.15 Vendor Assessment - Vendors are routinely assessed using audits, test results, or other forms of evaluation to confirm they are meeting their contractual obligations. [NIST 800-53 AU-2, AU-6, AU-12, AU-16, PS-7, SA-9, CSF ID.SC-4]

- **a.** Regularly review GovRAMP authorizations and Cloud Service Provider continuous monitoring activities, if applicable.
- **b.** Create vendor categories based on the context of the relationship, potential exposure, and third-party relationship.
- **c.** Upper categories should require questionnaires, independent evaluations, or testing.

6.3.16 Continuity Testing – Response and recovery planning and testing are conducted with vendors. [NIST 800-53 CP-2, CP-4, IR-3, IR-4, IR-6, IR-8, IR-9, CSF ID.SC-5]

6.4 Plan of Actions and Milestones Guidance - The following guidance is provided for the implementation and management of the state information system plan of actions and milestones (POAM) document.

6.4.1 POAM Overview. The POAM (aka POA&M) is a document designed to assist in the management of identified weaknesses in the state information system. The POAM document identifies known weaknesses (or compliance gaps) and lists the tasks necessary to mitigate these weaknesses. The documentation of these tasks together with an assignment of dates and resources provides system owners and other key personnel with the necessary information to manage the risk to the state information system.

6.4.2 Use of POAM for System Funding. The information regarding system weaknesses and mitigation tasks contained in the POAM is useful in the justification for system funding. The following guidance is provided to assist in making the POAM most useful for system funding assistance.

a. Link POAM with Investment Planning: Any requests or analysis for funding to support the state information system should be consistent with the POAM and the identified tasks within.

b. Include Resources Required: The POAM should include information and estimations for resources required to complete the tasks associated with identified weaknesses. These resource estimates should include staff levels and/or funding required and include an indication as to the frequency by which such funding will be required (e.g., quarterly, full-time, every other year).

c. Integrate Security Assessment Efforts: The POAM is typically the result of a system security plan, however, many other assessment efforts may identify weaknesses in the state information system and should integrate with the POAM. Assessments such as IG audit self-assessments, information security risk assessments, and penetration testing may result in the identification of system weaknesses. The POAM process should be utilized as a single source to track and manage system weaknesses. It is important to include a reference for the source of the weakness identification in an integrated POAM.

d. Prioritize Mitigation Efforts: The POAM may list system weaknesses which may be beyond the current funding initiatives. It is important to carefully consider the prioritization of the weaknesses and their associated mitigation tasks to ensure state resources are properly utilized. Prioritization of these tasks should consider relevant criteria when prioritizing such as current integrated tasks, system development life cycles, cost considerations, effectiveness of the proposed tasks, the perceived

impact of the weakness, and the effort/time required to implement the mitigation tasks.

e. **Assign Dates and Responsible Parties:** Each mitigation task should have an assigned date of estimated completion and a responsible party (or point of contact) for the implementation of the task.

f. **Monitor and Report POAM Activity:** The weaknesses, mitigation tasks, and progress made should be maintained quarterly in the POAM and reported to appropriate BU staff members such as the BU CIO and BU Information Security Officer. The following metrics are useful in monitoring and reporting POAM activity:

1. Total number of weaknesses identified at the start of the quarter;
2. Number of weaknesses for which corrective action was completed on time by end of the quarter;
3. Number of weaknesses for which corrective action is ongoing and is on track to complete as originally scheduled;
4. Number of weaknesses for which corrective action has been delayed, including explanation for delay; and
5. Number of new weaknesses discovered following the last POAM update and brief description of how they were identified.

g. **Validate and Age Completed Weaknesses:** When a mitigation task has been completed, the weakness associated with the mitigation task should be tested and marked as "completed" if the test demonstrates the weakness has been adequately addressed. Once a weakness has been marked as "completed" for 12 months, the weakness may be "aged off' or removed from the POAM.

h. **POAM Template:** The following template may be used to complete a POAM for a state information system:

System Name					System Owner					
					POAM Last Updated					
Weakness Identifie	Weakness Description	POC	Resources Required	Scheduled Date of Completion	Description of Milestone	Date Changes (if necessary)	Reporting Source	Status	Comments	Severity

6.5 Continuous Monitoring – Each BU should implement continuous monitoring that includes:

1. Security metrics identified through the risk assessment or industry standards

2. Continuous logging
3. Real-time reporting with escalation procedures

6.6 Penetration Testing Guidance – Penetration testing should be performed by a qualified third-party at least annually. Results from each test should be documented. Vulnerabilities should be remediated timely and retested to insure that potential risks have been mitigated.

6.6.1 The scope of a Web Application Penetration Test and/or Network Assessment includes:

a. One web application available by HTTP and/or HTTPS, including associated systems involved in the collection, saving, processing, and presenting of data for this web application, or;

b. For agencies without confidential data, a complete network assessment every 3 years.
1. All systems and devices controlled and managed by an agency, and;
2. All systems connected to on-premise, cloud, virtual and physical networks, and;
3. All internal and external facing devices.

c. For agencies without confidential data, a complete assessment every 3 years or one-third (⅓) of the web applications annually.

d. External Applications shall be completed by a 3rd party. Internal facing may be completed by either 3rd party or the agency.

e. This shall include, at a minimum,
1. Passive Reconnaissance
   - Gain information about targeted web applications and associated systems without actively engaging with the systems.
2. Attack Surface Enumeration
3. Enumerate the sum of the web application's security risk exposure.
4. Automated Scanning
   - Use of scanning tools to gather information about the web application.
5. Penetration Testing
   - Controlled attack simulation that helps identify susceptibility to web application, associated systems, and data breaches. https://www.doi.gov/ocio/customers/penetration-testing
   - Black box (no knowledge) and white box (with knowledge and/or privileges).
6. Reporting - Shall include, at a minimum:
   - Executive Summary

- Information Security risks including vulnerabilities, exploits, and severity
- Recommended actions for remediation
- The agency shall develop a plan of action based on report findings in accordance with Statewide Standard 8120 Section 6.4.2.

7. For agencies with confidential data,
   - All requirements listed above, and;
   - Requirements as identified in the State of Arizona Statewide Information Security Policies for protected systems, and;
   - Requirements as identified by applicable federal rules and regulations.

7. DEFINITIONS AND ABBREVIATIONS

7.1 Refer to the PSP Glossary of Terms located on the ADOA-ASET and NIST Computer Security Resource Center websites.

8. REFERENCES

8.1 CMS Information Security Program, CMS Plan of Action & Milestones (POA&M) Guidelines, Version 1.0, July 6, 2007

8.2 Guide for Developing Security Plans for Federal Information Systems, NIST Special Publication 800-18 Revision 1, February 2006.

8.3 Guide for Conducting Risk Assessments, NIST Special Publication 800-30, Revision 1, September 2012.

8.4 The Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments, 2nd Edition, Douglas J. Landoll, 2010.

9. ATTACHMENTS

None.

10. REVISION HISTORY

Date	Change	Revision	Signature
05/26/2021	**Annual Updates**	**1.0**	**Tim Roemer, Director of Arizona Department of Homeland Security & State Chief Information Security Officer** *Tim Roemer* Tim Roemer (May 25, 2021 22:14 PDT)
04/05/2024	**Review**	**1.1**	**Ryan Murray, Deputy Director of Arizona Department of Homeland Security & Interim State Chief Information Security Officer**
02/02/2026	**Changes to Include Cloud Product Assessment Requirements**	**1.2**	**Errika Celsy, Chief Privacy and Compliance Officer;** **Ryan Murray, Deputy Director of Arizona Department of Homeland Security & Interim State Chief Information Security Officer**