**Gap Analysis to Support the Implementation of the South Carolina**

**Risk Management Policy**

The below Gap Analysis is developed based on the feedback provided by the policy implementation team of the (SC State Agency). The table outlines the policy requirements (procedures, standards and policies which may/may not be implemented), relevant questions to address and identify gaps in the Agency’s environment.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Policy Requirement** | **Questions** asset inventory? | **YES , NO or N/A** | **Gap** | **Comments** |
| **InfoSec Policy has been reviewed and approved by the key stakeholders.** | **Has the InfoSec Policy been reviewed and approved by the key stakeholders?** |  |  |  |
| **InfoSec Policy has been approved and received sign off by the authorized executives.** | **Has the policy been approved and received sign off by the authorized executive?** |  |  |  |
| **The policy has been socialized across the Agency for personnel awareness.** | **Has the policy been shared with all personnel across-Agency?** |  |  |  |
| Establish a Risk Management Strategy | Has your Agency documented an on-going risk assessment and risk mitigation process?  Additional guidance: Typically, a risk assessment process has to be based on a security framework (e.g., NIST 800-53). The State of South Carolina Self-Assessment Tool is recommended to be used by agencies to perform risk assessments internally. Link: (http://dis.sc.gov/PoliciesAndProcedures/Pages/default.aspx#Self Assessment Tool) |  |  |  |
| If yes, has your Agency defined a schedule (e.g., to be conducted annually) for this process? |  |  |  |
| Establish a Risk Evaluation Process | Does your Agency review and evaluate an identified risk based on system categorization level (e.g., data classification model)?  Additional guidance: Agencies should use the Data Inventory Tool to define, document and categorize systems according to the data classification schema (found in the Data Protection & Privacy policy). After classifying the assets, the Agency should evaluate the risks of each system based on the data classification. |  |  |  |
| Establish a Risk Assessment Framework | Has your Agency established a risk assessment framework based on applicable State and federal laws, regulation and industry standards?  Additional guidance: For conducting risk assessments, an Agency can leverage the self-assessment tool provided by Deloitte. However, it is important to note that Agencies shall revise the framework to help ensure requirements from applicable laws and regulations are included to better comply with requirements from the State policies and additional restrictions internally at the Agency. |  |  |  |
| If yes, does this framework clearly define accountability in terms of risk, roles, and responsibilities within Agency departments? |  |  |  |
| Establish a Security Assessment Process | Does your Agency conduct a formal assessment of the IT security processes and controls to evaluate if the controls are operating as intended and producing the desired outcome?  For example, an Agency might have an internal control that states “*User access reviews shall be conducted on a semi-annual basis*”. As part of the formal assessment, the evaluator would look to obtain evidence documented from the completed user access review. Within the evidence, the evaluator should find evidence of approvals from managers/leadership, mentions for edits to change (removals/additions/alterations) access for particular users and ultimately, evidence documenting that the access request change was followed through and adjusted accordingly. If the access review was not completed, than the control did not have the desired outcome. |  |  |  |
| If yes, does the Agency verify whether the desired outcome is meeting the security requirements of the systems (e.g., NIST SP 800-15)?  Additional guidance: Refer to the IT Compliance Policy for further details and specific security requirements for IT systems. |  |  |  |
| Does the formal assessment occur at least on an annual basis? |  |  |  |
| Establish a Risk Prioritization and Acceptance Process | Has your Agency established a process to identify, quantify (e.g., provide a description), and prioritize risks against the Agency defined risk acceptance criteria and (information security) objectives? |  |  |  |
| Develop a Plan of Action and Milestones (POAM) and a Corrective Action plan (CAP) documents | Has the Agency developed a POAM and is this document updated at least annually? |  |  |  |
| Does the POAM effectively identify gaps related to the internal security controls (e.g., access management, patch management, etc.)? |  |  |  |
| Are remedial actions planned, implemented, or evaluated against the identified gaps? |  |  |  |
| Does your Agency develop and update at least annually, a Corrective Action Plan (CAP)?  Additional guidance: CAP or Correction Action Plan is a strategy for correcting or eliminating a non-conformance that has occurred in a management system. The non-conformities are usually identified during an internal audit in a firm or company or obtained from feedback given by customers as well as the staff. |  |  |  |
| Do the POAM and the CAP address implementation of security controls to reduce or eliminate known risks within the Agency’s systems? |  |  |  |
| Appointment of an Information Security Risk Officer | Has the Agency appointed a senior-level executive (e.g., information security risk officer or equivalent) to decide on the assignment of risk remediation measures to designated Agency individuals?  (e.g., Assigning risks related to patch management to the network and applications team heads respectively) |  |  |  |
| Establish a process to Monitor Information Systems on an on-going basis | Has your Agency established a process to continuously monitor information systems to ensure controls are operating as intended?  (e.g., Auto-generating access logs for systems holding critical data and having a designated individual review these logs to check for irregularities, such as, failed login attempts) |  |  |  |
| Establish a Risk Mitigation Process | Has the Agency established a process to convert identified risks into acceptable remediation goals?  (e.g., If access de-provisioning has been identified as a risk, where access of an individual leaving the Agency is not immediately revoked, the Agency must convert this risk into a remedial procedure wherein the required goal would be achieved) |  |  |  |
| Establish a Risk Acceptance Process | Has the Agency identified and documented a risk acceptance level for various identified threats based on business requirements? |  |  |  |
| Has the Agency established a process to identify the impact of a potential risk? |  |  |  |