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

**IT Compliance 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 compliance with legal and contractual requirements | Has your Agency identified and documented its obligations to applicable laws and regulations?Additional guidance: obligations may relate to security controls that are required to be implemented, including technical, procedural, and governance; as well as monitoring and reporting. Also, applicable laws and regulations may come in the form of Federal, State, and local laws, regulations, and mandates.  |  |  |  |
| Establish compliance with security policies and standards | Does your Agency perform reviews/audits of employees’ compliance with security policies, standards, and procedures?(e.g., The Agency may have an internal control that states “*Annually, employees must complete security training to comply with updates or changes to the security policies, standards, and procedures*”. The evaluator would be responsible for checking the security training mechanism to ensure the employee participated in the training and if applicable, passed or signed off on acknowledging an understanding of the updates or changes.) |  |  |  |
| Does your Agency perform reviews/audits of information systems’ compliance with security policies, standards, and procedures?(e.g., The Agency may have an internal control that states “*Passwords must be changed every sixty (60) days*”. The evaluator would be responsible for determining whether the system was set to enforce the password maximum age and trigger a password change. If during the audit the system has user’s with passwords greater than 60 days old, the system would be out of compliance with the Access (or subsequent) policy.) |  |  |  |
| If so, does this review or audit occur at least on an annually basis? |  |  |  |
| Does your Agency initiate corrective actions when either an employee or information system is not in compliance?(e.g., If any employee is found not to be in compliance with reviewing of policies and procedures, this employee is asked to do so within a defined timeline. If the employee fails to achieve the necessary compliance, the issue is escalated through the applicable channels to the Human Resources department) |  |  |  |
| Does your Agency document compliance reviews/audits?(e.g., The Agency should maintain documentation in the form of reports, working papers, etc., to collaborate the reviews/audits ) |  |  |  |
| Does your Agency report these reviews/audits with the senior management?Additional guidance: traditionally, a detailed report with findings and recommendations has to be generated for each review/audit, in addition to an executive with key findings and recommendations to be shared with executive management.  |  |  |  |
| Define an Audit and Accountability Policy and establish associated procedures for the effective implementation of selected security controls and control enhancements. | Has your Agency established an audit and accountability policy? |  |  |  |
| Has your Agency established the associated procedures to support this policy? |  |  |  |
| Does your Agency review and update the policy and associated procedures at least annually? |  |  |  |
| Develop Information Systems Audit Controls | Has your Agency established audit procedures such that review/audit activities of operational systems are conducted in a manner that minimizes risks of causing disruptions?Additional guidance: for example, if system reports are required these can be obtained during off-hours, or by the use of specialized tools such as in-house developed scripts that minimize time to gather data.  |  |  |  |
| Establish procedures for the Protection of Information System Audit Tools | Has your Agency implemented security controls to prevent unauthorized access or access abuse of audit related tools?Additional guidance: for example, setting access controls to only authorized individuals that can use the audit related tools to look at compliance, reporting capabilities or modify user actions  |  |  |  |
| Establish procedures to handle Audit Events | Has the Agency established the types of events that need to be audited within the information systems?Additional guidance: each system should have a list of controls that are required to be operational, including events to be logged and later be audited during a compliance review/audit.  |  |  |  |
| Does the Agency review and update the list of audited events annually? |  |  |  |
| Has coordination between the audit function, information security function, and business functions occurred to identify auditable events? |  |  |  |
| Develop the content of Audit Events | Are systems enabled to generate audit records that contain details of:* The type of event that occurred;
* The source of the event;
* The outcome of the event; and
* Identity of individuals/ information security subjects associated with the event.
 |  |  |  |
| Establish procedures for Audit Records Review and Reporting | Does the Agency review information system audit records periodically (i.e., at least annually)Additional guidance: By review of the information system audit records, an agency could be reviewing audit trails and audit logs that offer a back-end view of system use. The audit trails and logs review record key activities, shows system threads of access, changes, and transactions, potential failures and |  |  |  |
| Does the Agency report findings of audit records reviews to information security personnel and senior management?  |  |  |  |
| Does the Agency correlate the information generated by security assessments and through monitoring?  |  |  |  |
| Establish Audit Storage Capacity | Has your Agency allocated enough data storage capacity to help ensure compliance with audit logs retention requirements? Additional guidance: To reduce costs logs may be stored offline; however the Agency shall implement procedures to help ensure logs can be retrieved timely. Also, some laws/regulations may require logs to be retained on-line for a period of time.  |  |  |  |
| Has the Agency established a procedure to off-load audit records at regular interval (e.g., monthly) onto a different media than the system that is being audited? |  |  |  |
| Develop Continuous Monitoring procedures | Does the Agency employ assessment teams to monitor the security controls on an ongoing basis? |  |  |  |
| Does the Agency ensure that the assessment teams are independent from operational or business functions or hired third parties? |  |  |  |
| Develop and review a Plan of Action and Milestones | Has the Agency developed a plan of action and milestones (POA&M)?Additional guidance: The POA&M should include details on the weakness or gap, elements to describe the weakness, scheduled dates to close the weakness, task leads, overall status, etc.  |  |  |  |
| Does this plan document planned remedial actions to correct deficiencies identified as a result of (internal/external) risk assessments, security reviews, and audits? |  |  |  |
| Does the Agency update its (POA&M) at least annually based on findings from continuous security monitoring activities? |  |  |  |