41 Audit Logging & Accountability – Detect

Processes, policies, and procedures that enable organizations to establish an accurate and verifiable record of system relevant actions whether manual or automated for investigatory and accountability purposes.

Level 0: Non-existent – Audit logging policies do not exist. Log storage and capability may be inadequate or non-existent.

Level 1: Ad-hoc – Audit logs are reviewed occasionally when there is a suspected security incident. Logs are rarely, if ever, reviewed. Logging is performed on a system by system basis with no overarching standards applied.

Level 2: Repeatable – Logging practices are treated in a uniform manner throughout the organization, appropriate stakeholders have input into logging standards and retention.

Level 3: Defined – Logging policies and standards are documented and enforced throughout the organization. Logs are stored for the appropriate retention periods and periodically checked for accuracy and adherence to defined policies. There are sufficient controls in place to provide auditable evidence for system transactions and that key records are available for a sufficient amount of time.

Level 4: Risk-based – The organization routinely assesses system logs for signs of system errors. Logs are stored for the appropriate amount of time. Automated detection and notification processes may assist with logging analysis.

Level 5: Optimized – Logging practices are treated as an organizational asset. Policies and procedures are clearly defined, adhered to across the organization, and updated regularly. Logs from multiple systems are correlated and automated detection and alerting mechanisms are in place.

42 Information Systems Currency – Protect

Ensures that the necessary knowledge, skills, hardware, software, and supporting infrastructure are available at a reasonable cost to support information systems operations. Includes the monitoring and planning of future system developments that enable the organization to leverage modern technology and reduce technical debt.

Level 0: Non-existent – Information systems currency policies and modernization roadmap do not exist. The organization has no defined approach to ensuring the currency of its information assets.

Level 1: Ad-hoc – Information systems currency is taken into consideration by IT staff, but no normal policies or roadmap for addressing aging systems components exist.

Level 2: Repeatable – Information systems currency policies exist, and standards exist for maintaining a stated level of currency.

Level 3: Defined – Information systems currency policies and modernization roadmap exist and are developed with appropriate stakeholder input. Standards exist for maintaining the organizationally defined level of currency. Exceptions to currency are documented and a roadmap or plan for modernize outdated components is documented and adhered to.

Level 4: Risk-based – Information systems currency strategy is based upon risk assessment decisions. Modernization strategies are prioritized according to risk. Remediation plans and exceptions are routinely re-visited, and modernization efforts are communicated to appropriate stakeholders.

Level 5: Optimized – Information systems are continuously assessed for currency. Exceptions to currency policies are documented and approved by organizationally defined stakeholders. Long-term currency strategies are implemented, and modernization approaches are prioritized and optimized based on risk decisions.