Security Controls Excluded from POAM

Confidently Compliant

Level	Domain	ID	Requirement	Points
2	Access Control AC.L2-3.1.1	Authorized Access Control (CUI Data)	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	5
2	Access Control AC.L2-3.1.2	Transaction & Function Control (CUI Data)	Limit system access to the types of transactions and functions that authorized users are permitted to execute.	5
2	Access Control AC.L2-3.1.5	Least Privilege	Employ the principle of least privilege, including for specific security functions and privileged accounts.	3
2	Access Control AC.L2-3.1.12	Control Remote Access	Monitor and control remote access sessions.	5
2	Access Control AC.L2-3.1.13	Remote Access Confidentiality	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	5
2	Access Control AC.L2-3.1.16	Wireless Access Authorization	Authorize wireless access prior to allowing such connections.	5
2	Access Control AC.L2-3.1.17	Wireless Access Protection	Protect wireless access using authentication and encryption.	5
2	Access Control AC.L2-3.1.18	Mobile Device Connection	Control connection of mobile devices.	5
2	Access Control AC.L2-3.1.19	Encrypt CUI on Mobile	Encrypt on mobile devices and mobile computer platforms.	3
2	Awareness and Training AT.L2-3.2.1	Role-Based Risk Awareness	Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards and procedures related to the security of those systems.	5
2	Awareness and Training AT.L2-3.2.2	Role-Based Training	Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.	5
2	Audit and Accountability AU.L2-3.3.1	System Auditing	Create and retain system audit logs and records to the extend needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.	5
2	Audit and Accountability AU.L2-3.3.2	User Accountability	Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.	3
2	Audit and Accountability AU.L2-3.3.5	Audit Correlation	Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.	5
2	Security Assessment CA.L2-3.12.1	Security Control Assessment	Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.	5
2	Security Assessment CA.L2-3.12.2	Plan of Action	Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.	3
2	Security Assessment CA.L2-3.12.3	Security Control Monitoring	Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.	5
2	Configuration Management CM.L2-3.4.1	System Baselining	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	5
2	Configuration Management CM.L2-3.4.2	Security Configuration Enforcement	Establish and enforce security configuration settings for information technology products employed in organizational systems.	5
2	Configuration Management CM.L2-3.4.5	Access Restrictions for Change	Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.	5
2	Configuration Management CM.L2-3.4.6	Least Functionality	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	5
2	Configuration Management CM.L2-3.4.7	Nonessential Functionality	Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.	5
2	Configuration Management CM.L2-3.4.8	Application Execution Policy	Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.	5
2	Identification and Authentication IA.L2-3.5.1	Identification (CUI Data)	Identify system users, processes acting on behalf of users, and devices.	5
2	Identification and Authentication IA.L2-3.5.2	Authentication (CUI Data)	Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems.	5
2	Identification and Authentication IA.L2-3.5.3	Multifactor Authentication	Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.	2/5
2	Identification and Authentication IA.L2-3.5.10	Cryptographically-Protected Passwords	Store and transmit only cryptographically-protected passwords.	5
2	Incident response IR.L2-3.6.1	Incident Handling	Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.	5
2	Incident response IR.L2-3.6.2	Incident Reporting	Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.	5
2	Maintenance MA.L2-3.7.1	Perform Maintenance	Perform maintenance on organizational systems.	3
2	Maintenance MA.L2-3.7.2	System Maintenance Control	Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.	5
2	Maintenance MA.L2-3.7.4	Media Inspection	Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.	3
2	Maintenance MA.L2-3.7.5	Nonlocal Maintenance	Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.	5
2	Media Protection MP.L2-3.8.1	Media Protection	Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.	3
2	Media Protection MP.L2-3.8.2	Media Access	Limit access to CUI on system media to authorized users.	3
2	Media Protection MP.L2-3.8.3	Media Disposal (CUI Data)	Sanitize or destroy system media containing CUI before disposal or release for reuse.	5
2	Media Protection MP.L2-3.8.7	Removable Media	Control the use of removable media on system components.	5
2	Media Protection MP.L2-3.8.8	Shared Media	Prohibit the use of portable storage devices when such devices have no identifiable owner.	3
2	Physical Protection PE.L2-3.10.1	Limit Physical Access (CUI Data)	Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.	5
2	Physical Protection PE.L2-3.10.2	Monitor Facility	Protect and monitor the physical facility and support infrastructure for organizational systems.	5
2	Personnel Security PS.L2-3.9.1	Screen Individuals	Screen individuals prior to authorizing access to organizational systems containing CUI.	3
2	Personnel Security PS.L2-3.9.2	Personnel Actions	Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.	5
2	Risk Assessment RA.L2-3.11.1	Risk Assessments	Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.	3
2	Risk Assessment RA.L2-3.11.2	Vulnerability Scan	Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.	5
2	System and Communications Protection SC.L2-3.13.1	Boundary Protection (CUI Data)	Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.	5
2	System and Communications Protection SC.L2-3.13.2	Security Engineering	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	5
2	System and Communications Protection SC.L2-3.13.5	Public-Access System Separation (CUI Data)	Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.	5
2	System and Communications Protection SC.L2-3.13.6	Network Communication by Exception	Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).	5
2	System and Communications Protection SC.L2-3.13.8	Data in Transit	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.	3
2	System and Communications Protection SC.L2-3.13.11	CUI Encryption	Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.	2/5
2	System and Communications Protection SC.L2-3.13.15	Communications Authenticity	Protect the authenticity of communications sessions.	5
2	System and Information Integrity SI.L2-3.14.1	Flaw Remediation (CUI Data)	Identify, report, and correct system flaws in a timely manner.	5
2	System and Information Integrity SI.L2-3.14.2	Malicious Code Protection (CUI Data)	Provide protection from malicious code at designated locations within organizational systems.	5
2	System and Information Integrity SI.L2-3.14.3	Security Alerts & Advisories	Monitor system security alerts and advisories and take action in response.	5
2	System and Information Integrity SI.L2-3.14.4	Update Malicious Code Protection (CUI Data)	Update malicious code protection mechanisms when new releases are available.	5
2	System and Information Integrity SI.L2-3.14.5	System & File Scanning (CUI Data)	Perform periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed.	3
2	System and Information Integrity SI.L2-3.14.6	Monitor Communications for Attacks	Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	5
2	System and Information Integrity SI.L2-3.14.7	Identify Unauthorized Use	Identify unauthorized use of organizational systems.	3