Security Control Family Descriptions

| * + - * 1. Family (and Identifier) | * + - * 1. Description |
| --- | --- |
| * + - * 1. Access Control (AC) | * + - * 1. The standards listed in this section focus on how the organization shall limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise. |
| * + - * 1. Awareness and Training (AT) | * + - * 1. The standards listed in this section focus on how the organization shall: (i) ensure that managers and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, or procedures related to the security of organizational information systems; and (ii) ensure that organizational personnel are adequately trained to carry out their assigned IS-related duties and responsibilities. |
| * + - * 1. Audit and Accountability (AU) | * + - * 1. The standards listed in this section focus on how the organization shall: (i) create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions. |
| * + - * 1. Security Assessment and Authorization (CA) | * + - * 1. The standards listed in this section focus on how the organization shall: (i) periodically assess the security controls in organizational information systems to determine if the controls are effective in their application; (ii) develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems; (iii) authorize the operation of organizational information systems and any associated information system connections; and (iv) monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls. |
| * + - * 1. Configuration Management (CM) | * + - * 1. The standards listed in this section focus on how the organization shall: (i) establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (ii) establish and enforce security configuration settings for information technology products employed in organizational information systems. |
| * + - * 1. Contingency Planning (CP) | * + - * 1. The standards listed in this section focus on how the organization shall establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery for organizational information systems to ensure the availability of critical information resources and continuity of operations in emergency situations. |
| * + - * 1. Identification and Authentication (IA) | * + - * 1. The standards listed in this section focus on how the organization shall identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems. |
| * + - * 1. Incident Response (IR) | * + - * 1. The standards listed in this section focus on how the organization shall: (i) establish an operational incident handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and (ii) track, document, and report incidents to appropriate organizational officials and/‌or authorities. |
| * + - * 1. Maintenance (MA) | * + - * 1. The standards listed in this section focus on how the organization shall: (i) perform periodic and timely maintenance on organizational information systems; and (ii) provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance. |
| * + - * 1. Media Protection (MP) | * + - * 1. The standards listed in this section focus on how the organization shall: (i) protect information system media, both paper and digital; (ii) limit access to information on information system media to authorized users; and (iii) sanitize or destroy information system media before disposal or release for reuse. |
| * + - * 1. Physical and Environmental Protection (PE) | * + - * 1. The standards listed in this section focus on how the organization shall: (i) limit physical access to information systems, equipment, and the respective operating environments to authorized individuals; (ii) protect the physical plant and support infrastructure for information systems; (iii) provide supporting utilities for information systems; (iv) protect information systems against environmental hazards; and (v) provide appropriate environmental controls in facilities containing information systems. |
| * + - * 1. Planning (PL) | * + - * 1. The standards listed in this section focus on how the organization shall develop, document, periodically update, and implement security plans for organizational information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems. |
| * + - * 1. Personnel Security (PS) | * + - * 1. The standards listed in this section focus on how the organization shall: (i) ensure that individuals occupying positions of responsibility within organizations (including third-party service providers) are trustworthy and meet established security criteria for those positions; (ii) ensure that organizational information and information systems are protected during and after personnel actions such as terminations and transfers; and (iii) employ formal sanctions for personnel failing to comply with organizational security policies and procedures. |
| * + - * 1. Risk Assessment (RA) | * + - * 1. The standards listed in this section focus on how the organization shall periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of organizational information. |
| * + - * 1. System and Services Acquisition (SA) | * + - * 1. The standards listed in this section focus on how the organization shall: (i) allocate sufficient resources to adequately protect organizational information systems; (ii) employ system development life cycle processes that incorporate information security and privacy assurance considerations; (iii) employ software usage and installation restrictions; and (iv) ensure that third-party providers employ adequate security measures to protect information, applications, and/‌or services outsourced from the organization. |
| * + - * 1. System and Communications Protection (SC) | * + - * 1. The standards listed in this section focus on how the organization shall: (i) monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems; and (ii) employ architectural designs, software development techniques, and systems engineering principles that promote effective information security and privacy assurance within organizational information systems. |
| * + - * 1. System and Information Integrity (SI) | * + - * 1. The standards listed in this section focus on how the organization shall: (i) identify, report, and correct information and information system flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within organizational information systems; and (iii) monitor information system security alerts and advisories, and take appropriate actions in response. |
| * + - * 1. Program Management (PM) | * + - * 1. The PM family provides controls for information security programs required by Federal Information Security Management Act (FISMA). This family, while not specifically referenced in FIPS 200, provides security controls at the organization level rather than the information system level. |
| * + - * 1. Authority and Purpose (AP) | * + - * 1. This family furthers compliance with the Privacy Act by ensuring that organizations: (i) identify the legal bases that authorize a particular Personally Identifiable Information (PII) collection or activity that impacts privacy; and (ii) specify the purpose(s) for which they collect PII in their notices. |
| * + - * 1. Accountability, Audit, and Risk Management (AR) | * + - * 1. This family is intended to enhance public confidence through effective governance controls, monitoring controls, risk management, and assessment controls to demonstrate that an organization is complying with all applicable privacy protection requirements and minimizing its overall privacy risk. |
| * + - * 1. Data Quality and Integrity (DI) | * + - * 1. This family ensures compliance with Section 552a (e)(2) of the Privacy Act of 1974 and enhances public confidence that any PII collected and maintained by the organization is accurate, relevant, timely, and complete for the purpose for which it is to be used, as specified in the public notice. |
| * + - * 1. Data Minimization and Retention (DM) | * + - * 1. This family assists organizations in implementing the data minimization and retention elements of the Privacy Act, which requires organizations to collect, use, and retain only PII that is relevant and necessary for the specified purpose for which it was originally collected. Organizations retain PII for only as long as necessary to fulfill the specified purpose(s) and in accordance with a NARA-approved record retention schedule. |
| * + - * 1. Individual Participation and Redress (IP) | * + - * 1. This family addresses the need to make individuals active participants in the decision-making process regarding the collection and use of their PII, as required by the Privacy Act. By providing individuals with access to PII and the ability to have their PII corrected or amended, as appropriate, the controls in this family enhance public confidence in organizational decisions made based on the PII. |
| * + - * 1. Security (SE) | This family supplements the security controls in Appendix F to ensure administrative, technical, and physical measures are in place to protect PII collected or maintained by organizations against loss, unauthorized access, or disclosure, as required by the Privacy Act, and to ensure that organizational planning and responses to privacy incidents comply with Office of Management and Budget (OMB) policies and guidance. The controls in this family are implemented in coordination with information security personnel using the existing NIST Risk Management Framework. |
| * + - * 1. Transparency (TR) | * + - * 1. This family implements Sections 552a (e)(3) and (e)(4) of the Privacy Act and Section 208 of the E-Government Act, which require public notice of an organization’s information practices and the privacy impact of government programs and activities. |
| * + - * 1. Use Limitation (UL) | * + - * 1. This family is intended to assist organizations in complying with the Privacy Act, which prohibits uses of PII that are either not specified in notices, incompatible with the specified purposes, or not otherwise permitted by law. Implementation of the Controls in this Family will ensure that the scope of PII use is limited accordingly. |