Your Logo
Will Be
Placed Here

CYBERSECURITY & DATA PROTECTION PROGRAM (CDPP)

[NIST SP 800 53 REV5 LOW-MODERATE-HIGH BASELINES]

ACME Advanced Manufacturing, LLC

NIST SP 800-53 R5

CDPP

Cybersecurity & Data Protection Program

REFERENCED FRAMEWORKS & SUPPORTING PRACTICES

ACME's Cybersecurity & Data Protection Program (CDPP) contains policies, control objectives, standards and guidelines that references numerous leading industry frameworks in an effort to provide a comprehensive and holistic approach to implementing and maintaining secure systems, applications and processes. With the intent to incorporate both security and privacy concepts in all stages of the System Development Life Cycle (SDLC), the following external content is referenced by or supports this document:

- National Institute of Standards and Technology (**NIST**): [1]
  - NIST SP 800-37: *Guide for Applying the Risk Management Framework to Federal Information Systems*
  - NIST SP 800-39: *Managing Cybersecurity Risk: Organization, Mission and Information System View*
  - NIST SP 800-53: *Security and Privacy Controls for Federal Information Systems and Organizations*
  - NIST SP 800-56A: *Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography*
  - NIST SP 800-56B: *Recommendation for Pair-Wise Key-Establishment Using Integer Factorization Cryptography*
  - NIST SP 800-56C: *Recommendation for Key-Derivation Methods in Key-Establishment Schemes*
  - NIST SP 800-63-3: *Digital Identity Guidelines*
  - NIST SP 800-57-1: *Recommendation for Key Management: Part 1 – General*
  - NIST SP 800-57-2: *Recommendation for Key Management: Part 2 – Best Practices for Key Management Organizations*
  - NIST SP 800-57-3: *Recommendation for Key Management, Part 3: Application-Specific Key Management Guidance*
  - NIST SP 800-64: *Security Considerations in System Development Lifecycle*
  - NIST SP 800-122: *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*
  - NIST SP 800-128: *Guide for Security-Focused Configuration Management of Information Systems*
  - NIST SP 800-160 vol1: *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*
  - NIST SP 800-160 vol2: *Developing Cyber Resilient Systems: A Systems Security Engineering Approach*
  - NIST SP 800-161: *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*
  - NIST SP 800-171: *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*
  - NIST SP 800-172: *Enhanced Security Requirements for Protecting CUI: A Supplement to NIST SP 800-171*
  - NIST SP 800-207: *Zero Trust Architecture (ZTA)*
  - NIST IR 8062: *An Introduction to Privacy Engineering and Risk Management in Federal Systems*
  - NIST IR 8179: *Criticality Analysis Process Model: Prioritizing Systems and Components* [draft]
  - NIST *Framework for Improving Critical Cybersecurity* (Cybersecurity Framework)
- International Organization for Standardization (**ISO**):[2]
  - ISO 15288: *Systems and Software Engineering - System Life Cycle Processes*
  - ISO 27001: *Information Technology - Security Techniques - Information Security Management Systems - Requirements*
  - ISO 27002: *Information Technology - Security Techniques - Code of Practice for Cybersecurity Controls*
  - ISO 27018: *Information Technology - Security Techniques - Code of Practice for Protection of Personally Identifiable Information (PII) in Public Clouds Acting as PII Processors*
- Other Frameworks:
  - Cybersecurity Maturity Model Certification (**CMMC**)[3]
  - Secure Controls Framework (SCF) [4]
  - Cloud Security Alliance Cloud Controls Matrix (**CSA CCM**)[5]
  - Center for Internet Security (**CIS**)[6]
  - Open Web Application Security Project (**OWASP**)[7]
  - Department of Defense Cybersecurity Agency (**DISA**) Secure Technology Implementation Guides (**STIGs**)[8]
  - Fair Information Practice Principles (**FIPP**)[9]
  - European Union Regulation 2016/279 (General Data Protection Regulation (**EU GDPR**))[10]
  - Payment Card Industry Data Security Standard (**PCI DSS**)[11]

[1] National Institute of Standards and Technology - http://csrc.nist.gov/publications/PubsSPs.html
[2] International Organization for Standardization - https://www.iso.org
[3] Office of the Under Secretary of Defense for Acquisition & Sustainment - https://www.acq.osd.mil/cmmc/draft.html
[4] Secure Controls Framework - https://www.securecontrolsframework.com
[5] Cloud Security Alliance - https://cloudsecurityalliance.org/
[6] Center for Internet Security - https://www.cisecurity.org/
[7] Open Web Application Security Project - https://www.owasp.org/index.php/Main_Page
[8] DoD Information Security Agency - http://iase.disa.mil/stigs/Pages/index.aspx
[9] Federal Trade Commission - https://www.ftc.gov
[10] EU General Data Protection Regulation - http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf
[11] Payment Card Industry Security Standards Council - https://www.pcisecuritystandards.org/

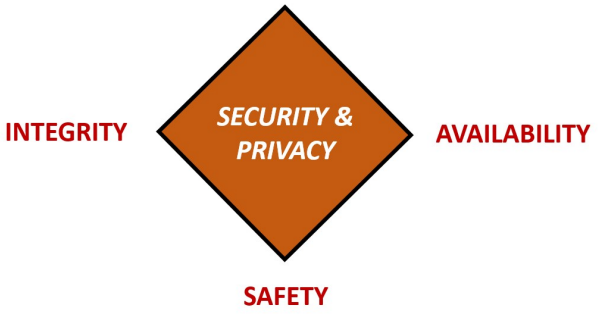
TABLE OF CONTENTS

INTRODUCTION

The Cybersecurity & Data Protection Program (CDPP) provides definitive information on the prescribed measures used to establish and enforce the cybersecurity and privacy program at ACME Advanced Manufacturing, LLC (ACME). The CDPP is authorized and supported by ACME's executive leadership.

ACME is committed to protecting its employees, partners, clients and ACME from damaging acts that are intentional or unintentional. Effective security is a team effort involving the participation and support of every entity that interacts with ACME data and systems, applications and services. Therefore, it is the responsibility of both ACME personnel and third-parties to be aware of and adhere to ACME's cybersecurity and data protection requirements.

Protecting ACME data and the systems that collect, process and maintain this data is of critical importance. Commensurate with risk, security and privacy measures must be implemented to guard against unauthorized access to, alteration, disclosure or destruction of data and systems, applications and services. This also includes protection against accidental loss or destruction. The security of systems, applications and services must include controls and safeguards to offset possible threats, as well as controls to ensure confidentiality, integrity, availability and safety:



- **CONFIDENTIALITY** – Confidentiality addresses preserving restrictions on information access and disclosure so that access is limited to only authorized users and services.
- **INTEGRITY** – Integrity addresses the concern that sensitive data has not been modified or deleted in an unauthorized and undetected manner.
- **AVAILABILITY** – Availability addresses ensuring timely and reliable access to and use of information.
- **SAFETY** – Safety addresses reducing risk associated with embedded technologies that could fail or be manipulated by nefarious actors.

PURPOSE

The purpose of the Cybersecurity & Data Protection Program (CDPP) is to prescribe a comprehensive framework for:

- Creating a NIST SP 800-53 R5-based Information Security Management System (ISMS);
- Protecting the confidentiality, integrity and availability of ACME data and systems;
- Protecting ACME, its employees and its clients from illicit use of ACME systems and data;
- Ensuring the effectiveness of security controls over data and systems that support ACME's operations.
- Recognizing the highly-networked nature of the current computing environment and provide effective company-wide management and oversight of those related cybersecurity risks; and
- Providing for the development, review and maintenance of minimum security controls required to protect ACME's data and systems.

The formation of these cybersecurity policies is driven by many factors, with the key factor being a risk. These policies set the ground rules under which ACME operates and safeguards its data and systems to both reduce risk and minimize the effect of potential incidents.

These policies, including their related standards, procedures and guidelines, are necessary to support the management of information risks in daily operations. The development of policies provides due care to ensure ACME users understand their day-to-day security responsibilities and the threats that could impact the company.

Implementing consistent security controls across the company will help ACME comply with current and future legal obligations to ensure long-term due diligence in protecting the confidentiality, integrity and availability of ACME data.

Scope & Applicability

ACME's policies, standards, procedures and guidelines apply to all ACME data, systems, activities and assets owned, leased, controlled or used by ACME, its agents, contractors or other business partners on behalf of ACME. These policies, standards, procedures and guidelines aldo apply to all ACME employees, contractors, sub-contractors and their respective facilities supporting ACME business operations, wherever ACME data is stored or processed, including any third-party contracted by ACME to handle, process, transmit, store or dispose of ACME data.

Some standards apply specifically to persons with a specific job function (e.g., a System Administrator); otherwise, all personnel supporting ACME business functions must comply with the policies. ACME departments must use these policies or may create a more restrictive policy, but none that are less restrictive, less comprehensive or less compliant than these policies.

These policies do not supersede any other applicable law, regulation, higher-level company directive or existing labor management agreement in effect as of the effective date of these policies and standards.

ACME's documented cybersecurity roles & responsibilities provides a detailed description of ACME's cybersecurity and privacy-related user roles and responsibilities.

ACME reserves the right to revoke, change or supplement these policies, standards, procedures and guidelines at any time without prior notice. Such changes must be effective immediately upon approval by management unless otherwise stated.

Policy Overview

To ensure an acceptable level of cybersecurity risk, ACME must design, implement and maintain a coherent set of policies, standards, procedures and guidelines to manage risks to its data and systems.

ACME users must protect and ensure the Confidentiality, Integrity, Availability and Safety (CIAS) of data and systems, regardless of how its data is created, distributed or stored. Security and privacy controls must be:

- Tailored accordingly so that cost-effective controls can be applied commensurate with the risk and sensitivity of the data and system; and
- Designed and maintained to ensure compliance with all legal requirements.

Violations of Policies, Standards and/or Procedures

Any ACME user found to have violated a ACME policy, standard or procedure is subject to disciplinary action, up to and including termination of employment. Violators of local, state, Federal, and/or international law may be reported to the appropriate law enforcement agency for civil and/or criminal prosecution.

Exceptions To Standards

While every exception to a standard potentially weakens protection mechanisms for ACME systems and underlying data, occasionally exceptions will exist. Users must submit a request for an exception to a cybersecurity standard and receive approval for the exception, before any deviation from a standard can be implemented.

Updates To Policies & Standards

Updates to the Cybersecurity & Data Protection Program (CDPP) will be announced to employees via management updates or email announcements. Changes will be noted in the Record of Changes to highlight the pertinent changes from the previous policies, procedures, standards and guidelines.

Key Terminology

In the realm of cybersecurity terminology, the National Institute of Standards and Technology (NIST) IR 7298, *Glossary of Key Information Security Terms*, is the primary reference document that ACME uses to define common cybersecurity terms. [12] Key terminology to be aware of includes:

[12] NIST IR 7298 - https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.7298r3.pdf

Adequate Security. A term describing protective measures that are commensurate with the consequences and probability of loss, misuse or unauthorized access to or modification of information.

Asset: A term describing any data, device, application, service or other component of the environment that supports information-related activities. An asset is a resource with economic value that a ACME owns or controls.

Asset Custodian: A term describing a person or entity with the responsibility to assure that the assets are properly maintained, are used for the purposes intended and that information regarding the equipment is properly documented.

Cloud Computing. A term describing a technology infrastructure model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. It also includes commercial offerings for Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS).

Control Objective: A term describing any management, operational or technical method that is used to manage risk. Controls are designed to monitor and measure specific aspects of standards to help ACME accomplish stated goals or objectives. All controls map to standards, but not all standards map to Controls.

Cybersecurity / Information Security: A term that covers the protection of information against unauthorized disclosure, transfer, modification or destruction, whether accidental or intentional. The focus is on the Confidentiality, Integrity, Availability and Safety (CIAS) of data.

Data: A term describing an information resource that is maintained in electronic or digital format. Data may be accessed, searched or retrieved via electronic networks or other electronic data processing technologies. *Annex 1: Data Classification & Handling Guidelines* provides guidance on data classification and handling restrictions.

Data Controller. A term describing the privacy stakeholder (or privacy stakeholders) that determines the purposes and means for processing Personally Identifiable Information (PII) other than natural persons who use data for personal purposes

Data Principle. A term describing the natural person to whom the Personally Identifiable Information (PII) relates

Data Processor. A term describing the privacy stakeholder that processes Personally Identifiable Information (PII) on behalf of and in accordance with the instructions of a PII controller

Encryption: A term describing the conversion of data from its original form to a form that can only be read by someone that can reverse the encryption process. The purpose of encryption is to prevent unauthorized disclosure of data.

Guidelines: A term describing recommended practices that are based on industry-recognized leading practices. Unlike Standards, Guidelines allow users to apply discretion or leeway in their interpretation, implementation or use.

Information Technology (IT). A term includes computers, ancillary equipment (including imaging peripherals, input, output and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services) and related resources.

Least Privilege: A term describing the theory of restricting access by only allowing users or processes the least set of privileges necessary to complete a specific job or function.

Personally Identifiable Information (PII) / Personally Identifiable Information (PII) / Personal Information (PI). A term describing any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.[13]

Policy: A term describing a formally established requirement to guide decisions and achieve rational outcomes. Essentially, a policy is a statement of expectation that is enforced by standards and further implemented by procedures.

[13] European Union General Data Protection Requirement – Article 4(1)

MANAGEMENT DIRECTION FOR CYBERSECURITY & DATA PROTECTION

The objective is to provide management direction and support for cybersecurity and data protection in accordance with business requirements and relevant laws and regulations. [14]

An Information Security Management System (ISMS) focuses on cybersecurity management and technology-related risks. The governing principle behind ACME's ISMS is that, as with all management processes, the ISMS must remain effective and efficient in the long-term, adapting to changes in the internal organization and external environment.

In accordance with leading practices, ACME's ISMS incorporates the typical "Plan-Do-Check-Act" (PDCA) or Deming Cycle, approach:

- Plan: This phase involves designing the ISMS, assessing IT-related risks and selecting appropriate controls.
- Do: This phase involves implementing and operating the appropriate security controls.
- Check: This phase involves reviewing and evaluating the performance (efficiency and effectiveness) of the ISMS.
- Act: This involves making changes, where necessary, to bring the ISMS back to optimal performance.

POLICIES, CONTROLS, STANDARDS, PROCEDURES & GUIDELINES STRUCTURE

ACME's cybersecurity and data protection documentation is comprised of five (5) core components:

(1) Policies are established by ACME's corporate leadership establishes "management's intent" for cybersecurity and data protection requirements that are necessary to support ACME's overall strategy and mission;
(2) Controls / Control Objectives identify the technical, administrative and physical protections that are generally tied to a law, regulation, industry framework or contractual obligation;
(3) Standards provide ACME-specific, quantifiable requirements for cybersecurity and data protection;
(4) Procedures (also known as Control Activities) establish the defined practices or steps that are performed to meet to implement standards and satisfy controls / control objectives; and
(5) Guidelines are additional guidance that is recommended, but not mandatory.

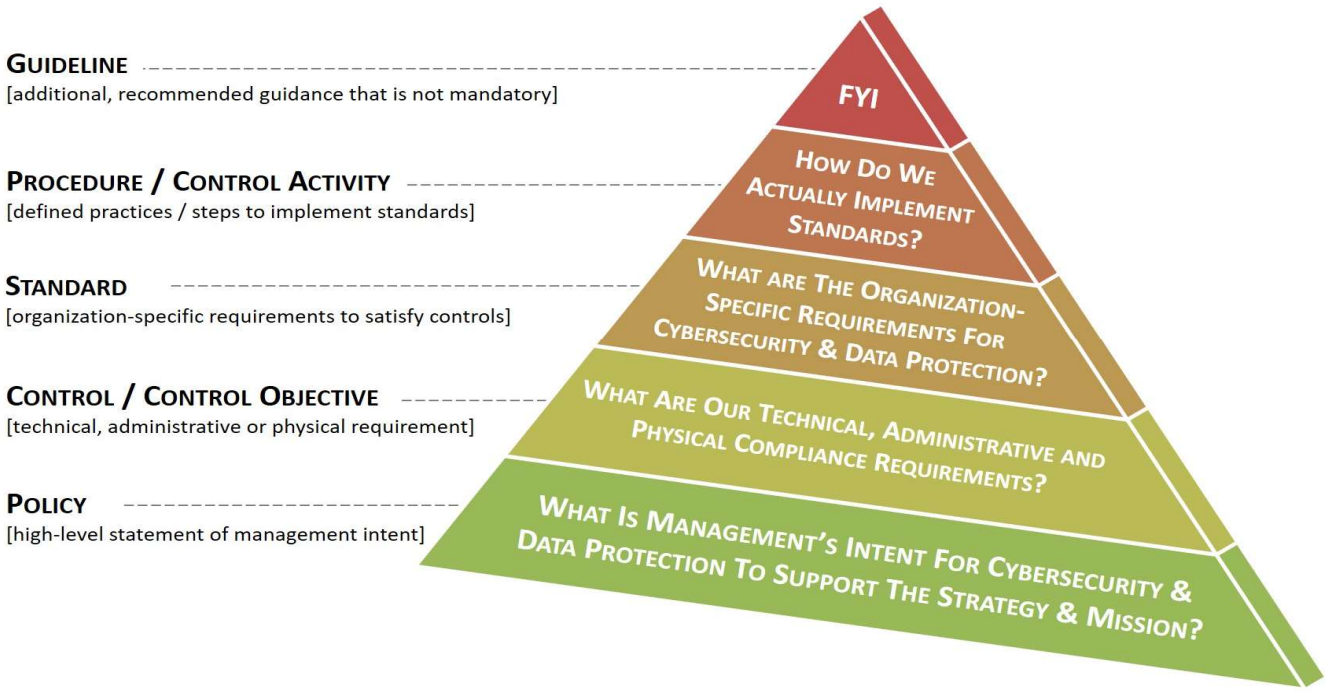


Figure 1: Cybersecurity Documentation Hierarchy

[14] ISO 27002:2013 5.1

NIST SP 800-53 R5 Controls Alignment

ACME's standards are organized into classes and families for ease of use in the control selection and specification process. There are three (3) general classes of security control objectives that align with FIPS 199.[15] These classes are further broken down into twenty (20) families of security control objectives.

- **Management**
  - Management controls are non-technical mechanisms that define and guide employee actions in dealing with cybersecurity topics.
  - Management controls also play an important role in policy enforcement, since these focus on the management of the cybersecurity program and the management of risk within ACME.
- **Operational**
  - Operational controls are primarily focused on resource the execution of the day-to-day cybersecurity program.
  - These controls generally focus on the means to control logical and physical access to information and to protect the security of supporting systems.
- **Technical**
  - Technical controls are primarily technical in nature. These controls, such as devices, processes, protocols and other measures, are used to protect the confidentiality, integrity and availability of the organization's technology assets and data.
  - These are dependent upon the proper functioning of the system for their effectiveness and therefore require significant operational considerations.

Each family contains security controls related to the security functionality of the family. A two-character identifier is assigned to uniquely identify each control family. The table below summarizes the classes and families in the security control catalog and the associated family identifiers.

Figure 2: NIST SP 800-53 R5 Controls Families & Identifiers

Control Grouping	Policy #	NIST 800-53 R5 Control Family	Identifier
Management	1	Assessment, Authorization & Monitoring	**CA**
Management	2	Planning	**PL**
Management	3	Program Management	**PM**
Management	4	Risk Assessment	**RA**
Management	5	System & Services Acquisition	**SA**
Management	6	Supply Chain Risk Management	**SR**
Operational	7	Awareness & Training	**AT**
Operational	8	Contingency Planning	**CP**
Operational	9	Incident Response	**IR**
Operational	10	Media Protection	**MP**
Operational	11	Personnel Security	**PS**
Operational	12	Physical & Environmental Protection	**PE**
Operational	13	Personally Identifiable Information (PII) Processing & Transparency	**PT**
Technical	14	Access Control	**AC**
Technical	15	Audit & Accountability	**AU**
Technical	16	Configuration Management	**CM**
Technical	17	Identification & Authentication	**IA**
Technical	18	Maintenance	**MA**
Technical	19	System & Communications Protection	**SC**
Technical	20	System & Information Integrity	**SI**

[15] FIPS 199 - http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf

MANAGEMENT CONTROLS

Management controls are non-technical mechanisms that define and guide employee actions in dealing with cybersecurity topics. These cybersecurity controls address broader Information Security Management System (ISMS)-level governance of the security program that impact operational, technical and privacy controls.

PROGRAM MANAGEMENT (PM)

Cybersecurity Program Management Policy: ACME must implement Cybersecurity program management controls to provide a foundation for ACME's cybersecurity Management System (ISMS).

Management Intent: The purpose of the Program Management (PM) policy is for ACME to specify the development, implementation, assessment, authorization and monitoring of the Cybersecurity program management. The successful implementation of security controls for organizational systems depends on the successful implementation of the organization's program management controls. The Cybersecurity Program Management (PM) controls are essential for managing the Cybersecurity program.

Supporting Documentation: Program Management (PM) control objectives, standards and guidelines directly support this policy.

PM-1: INFORMATION SECURITY PROGRAM PLAN

Control Objective:[16]

a. Develop and disseminate an organization-wide information security program plan that:
   1. Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements;
   2. Includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities and compliance;
   3. Reflects the coordination among organizational entities responsible for information security; and
   4. Is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image and reputation), organizational assets, individuals, other organizations and the Nation;

b. Review and update the organization-wide information security program plan per an organization-defined frequency and following organization-defined events; and

c. Protect the information security program plan from unauthorized disclosure and modification.

Standard: ACME's cybersecurity policies and standards must be consolidated in a single document, the Cybersecurity & Data Protection Program (CDPP). The CDPP:

(1) Documents ACME's security and privacy program and makes it available to authorized personnel that:
   (A) Identifies the requirements for ACME's security and privacy program, including Program Management (PM)-related controls;
   (B) Identifies applicable statutory, regulatory and contractual obligations (see CDPP Applicability Matrix); and
   (C) Includes the identification and assignment of roles and responsibilities among stakeholders that reflects the coordination among the organizational entities responsible for security and privacy practices;

(2) Is approved by ACME's Chief Information Security Officer (CISO), who is ACME's designated official with the responsibility and accountability for security and privacy-related policies and standards;

(3) Establishes quantifiable requirements for people, processes and technologies to facilitate the development of procedures that are sufficient to document how ACME's policies and standards are implemented and enforced by stakeholders (e.g., data/process owners and asset custodians);

(4) Shall be reviewed annually, or as needed based on assessed need, by the CISO, or delegates who are qualified to perform review functions. Based on the review, any necessary updates to the CDPP will be implemented and distributed per ACME's established change management practices; and

(5) Must be protected from unauthorized disclosure and modification.

Guidelines: An information security program plan is a formal document that provides an overview of the security requirements for an organization-wide information security program and describes the program management controls and common controls in place

[16] NIST SP 800-53 Rev 5 control PM-1

or planned for meeting those requirements. An information security program plan can be represented in a single document or compilations of documents. Privacy program plans and SCRM plans are addressed separately in PM-18 and SR-2, respectively.

An information security program plan documents implementation details about program management and common controls. The plan provides sufficient information about the controls (including specification of parameters for assignment and selection operations, explicitly or by reference) to enable implementations that are unambiguously compliant with the intent of the plan and a determination of the risk to be incurred if the plan is implemented as intended.

Updates to information security program plans include organizational changes and problems identified during plan implementation or control assessments.

Program management controls may be implemented at the organization level or the mission or program. Program management controls are distinct from common, system-specific and hybrid Together, the individual system security plans and the organization-wide information security program plan provide complete coverage for security and privacy controls employed within the organization.

Common controls available for inheritance by organizational systems are documented in an appendix to the organization's information security program plan unless the controls are included in a separate security plan for a system. The organization-wide information security program plan indicates which separate security plans contain descriptions of common controls.

Events that may precipitate an update to the information security program plan include, but are not limited to, organization-wide assessment or audit findings, security or privacy incidents or changes in laws, executive orders, directives, regulations, policies, standards and guidelines.

PM-2: Information Security Program Leadership Role

Control Objective: Appoint a senior agency information security officer with the mission and resources to coordinate, develop, implement and maintain an organization-wide information security program.[17]

Standard: The authority and responsibility for managing the cybersecurity program are delegated to ACME's Chief Information Security Officer (CISO). The CISO is required to perform, or delegate, the following security and privacy management responsibilities:

(1) Coordinate, develop, implement and maintain:
   (A) A proactive security posture that is appropriate to meet ACME's requirements and risks;
   (B) Protections from reasonably-expected threats;
   (C) Situational awareness that is capable of detecting incidents;
   (D) Trained personnel and tested processes to respond to incidents; and
   (E) Capabilities to recover from incidents and sustain key business operations; and
(2) Establish, document and distribute security policies, standards and procedures.

Guidelines: The senior agency information security officer is an organizational official. For federal agencies (as defined by applicable laws, executive orders, regulations, directives, policies and standards), this official is the senior agency information security officer. Organizations may also refer to this official as the senior information security officer or chief information security officer.

PM-3: Information Security and Privacy Resources

Control Objective: [18]

a. Include the resources needed to implement the information security and privacy programs in capital planning and investment requests and document all exceptions to this requirement;
b. Prepare documentation required for addressing information security and privacy programs in capital planning and investment requests in accordance with applicable laws, executive orders, directives, policies, regulations, standards; and
c. Make available for expenditure, the planned information security and privacy resources.

Standard: ACME's Chief Information Security Officer (CISO), or the CISO's designated representative(s), are tasked with:

(1) Managing security and privacy resources according to a multi-year business plan (e.g., roadmap); and
(2) Providing oversight for the cybersecurity-related aspects of the planning and service / tool selection process.

[17] NIST SP 800-53 Rev 5 control PM-2
[18] NIST SP 800-53 Rev 5 control PM-3

Standard: ACME's Chief Information Security Officer (CISO), or the CISO's designated representative(s), are authorized to conduct or contract an outside organization to perform a technical surveillance countermeasures survey.

Guidelines: A technical surveillance countermeasures survey is a service provided by qualified personnel to detect the presence of technical surveillance devices and hazards and to identify technical security weaknesses that could be used in the conduct of a technical penetration of the surveyed facility. Technical surveillance countermeasures surveys also provide evaluations of the technical security posture of organizations and facilities and include visual, electronic and physical examinations of surveyed facilities, internally and externally. The surveys also provide useful input for risk assessments and information regarding organizational exposure to potential adversaries.

RA-7: Risk Response

Control Objective: Respond to findings from security and privacy assessments, monitoring and audits in accordance with organizational risk tolerance.[98]

Standard: ACME's Chief Information Security Officer (CISO), or the CISO's designated representative(s), must respond to findings from security and privacy assessments, monitoring and audits in accordance with ACME's Risk Management Program (RMP) to ensure response is in accordance with ACME's established risk tolerance.

Guidelines: Organizations have many options for responding to risk including mitigating risk by implementing new controls or strengthening existing controls, accepting risk with appropriate justification or rationale, sharing or transferring risk or avoiding risk. The risk tolerance of the organization influences risk response decisions and actions. Risk response addresses the need to determine an appropriate response to risk before generating a plan of action and milestones entry. For example, the response may be to accept risk or reject risk or it may be possible to mitigate the risk immediately so that a plan of action and milestones entry is not needed. However, if the risk response is to mitigate the risk and the mitigation cannot be completed immediately, a plan of action and milestones entry is generated.

RA-8: Privacy Impact Assessments (PIA)

Control Objective: Conduct privacy impact assessments for systems, programs or other activities before:[99]

a. Developing or procuring information technology that processes PII; and
b. Initiating a new collection of PII that:
    1. Will be processed using information technology; and
    2. Includes PII permitting the physical or virtual (online) contacting of a specific individual, if identical questions have been posed to or identical reporting requirements imposed on, ten or more individuals, other than agencies, instrumentalities or employees of the federal government.

Standard: ACME's Chief Privacy Officer (CPO), Data Protection Officer (DPO), or their designated representative(s), must ensure that data/process owners and asset custodians conduct Privacy Impact Assessments (PIAs) for systems, application or service before:[100]

(1) Developing or procuring information technology that processes PII; and
(2) Initiating a new collection of PII that will be processed using information technology.

Guidelines: The PIA process is required to consist of gathering data from a project on privacy issues, identifying and resolving the privacy risks and approval. Specifically:

- New Systems. New systems and systems under development or undergoing major modifications must complete a PIA.
- Legacy Systems. Legacy systems, as they exist today, do not have to complete a PIA. However, if the upgrading of these systems puts the data at risk, a PIA should be performed.
- Current Systems: Currently operational systems are not required to complete a PIA. However, if privacy is a concern, a PIA be completed.

The following websites offer examples of PIAs, with varying levels of complexity. It is up to the asset custodian and data data/process owner to determine the proper level of complexity for the PIA:

- http://www.justice.gov/opcl/docs/doj-pia-template.pdf
- http://www.gsa.gov/portal/content/102237

[98] NIST SP 800-53 Rev 5 control RA-7
[99] NIST SP 800-53 Rev 5 control RA-8
[100] NIST SP 800-53 Rev 5 control RA-8

external providers. Weaknesses or deficiencies in supply chain elements or processes represent potential vulnerabilities that can be exploited by adversaries to cause harm to the organization and affect its ability to carry out its core missions or business functions. Supply chain personnel are individuals with roles and responsibilities in the supply chain.

SR-5: Acquisition Strategies, Tools & Methods

Control Objective: Employ organization-defined acquisition strategies, contract tools and procurement methods to protect against, identify and mitigate supply chain risks.[141]

Standard: For sensitive projects or for overseas locations, ACME must:

(1) Tailor acquisition strategies, contract tools and procurement methods to ensure the integrity of system, applications and services;
(2) Utilize enhanced acquisition techniques, such as:
    (A) Obscuring the end use of a system or system component; and
    (B) Using blind or filtered buys;
(3) Creating incentives for suppliers who:
    (A) Implement required security safeguards;
    (B) Promote transparency into their organizational processes and security practices;
    (C) Provide additional vetting of the processes and security practices of subordinate suppliers, mission-critical (SC1) and business-critical (SC2) technology assets components and services;
    (D) Restrict purchases from specific suppliers or countries; and
    (E) Provide contract language regarding the prohibition of tainted or counterfeit components; and
(4) Reduce the probability of adversaries successfully identifying and targeting the supply chain include, for example:
    (A) Avoiding the purchase of custom configurations to reduce the risk of acquiring systems, components or products that have been corrupted via supply chain actions targeted at specific organizations;
    (B) Employing a diverse set of suppliers to limit the potential harm from any given supplier in the supply chain;
    (C) Employing approved vendor lists with standing reputations in industry; and
    (D) Using procurement carve outs (e.g., exclusions to commitments or obligations).

Guidelines: See *Annex 4: Baseline Security Categorization Guidelines* for Safety & Criticality (SC) categorization. The use of the acquisition process provides an important vehicle to protect the supply chain. There are many useful tools and techniques available, including obscuring the end use of a system or system component, using blind or filtered buys, requiring tamper-evident packaging or using trusted or controlled distribution. The results from a supply chain risk assessment can guide and inform the strategies, tools and methods that are most applicable to the situation. Tools and techniques may provide protections against unauthorized production, theft, tampering, insertion of counterfeits, insertion of malicious software or backdoors and poor development practices throughout the SDLC. Organizations also consider providing incentives for suppliers who implement controls, promote transparency into their processes and security and privacy practices, provide contract language that addresses the prohibition of tainted or counterfeit components and restrict purchases from untrustworthy suppliers. Organizations consider providing training, education and awareness programs for personnel regarding supply chain risk, available mitigation strategies and when the programs should be employed. Methods for reviewing and protecting development plans, documentation and evidence are commensurate with the security and privacy requirements of the organization. Contracts may specify documentation protection requirements.

SR-6: Supplier Assessments & Reviews

Control Objective: Assess and review the supply chain-related risks associated with suppliers or contractors and the system, system component or system service they provide per organization-defined frequency.[142]

Standard: ACME's data/process owners and asset custodians must conduct supplier reviews prior to entering into a contractual agreement to acquire mission-critical (SC1) and business-critical (SC2) technology assets, system components or system services. Supplier reviews must include:

(1) Analysis of supplier processes used to design, develop, test, implement, verify, deliver and support systems, system components and system services; and
(2) Assessment of supplier training and experience in developing systems, components or services with the required security capability.

[141] NIST SP 800-53 Rev 5 control SR-5
[142] NIST SP 800-53 Rev 5 control SR-6

Guidelines: See *Annex 4: Baseline Security Categorization Guidelines* for Safety & Criticality (SC) categorization. An assessment and review of supplier risk includes security and SCRM processes, foreign data/process ownership, control or influence (FOCI) and the ability of the supplier to effectively assess subordinate second-tier and third-tier suppliers and contractors. The reviews may be conducted by the organization or by an independent third party. The reviews consider documented processes, documented controls, all-source intelligence and publicly available information related to the supplier or contractor. Organizations can use open-source information to monitor for indications of stolen information, poor development and quality control practices, information spillage or counterfeits. In some cases, it may be appropriate or required to share assessment and review results with other organizations in accordance with any applicable rules, policies or inter-organizational agreements or contracts.

SR-6(1): Supplier Assessments & Reviews | Testing & Analysis

Control Objective: Employ organizational analysis, independent third-party analysis, organizational testing or independent third-party testing of organization-defined supply chain elements, processes, and actors associated with the system, system component, or system service.[143]

Standard: Where technically feasible and justified by a valid business case, ACME's data/process owners and asset custodians must utilize one of more methods to assess chain elements, processes and actors associated with ACME's systems, applications and services:

(1) Internal or independent, third-party analysis; or
(2) Internal testing or independent, third-party validation testing.

Guidelines: Relationships between entities and procedures within the supply chain, including development and delivery, are considered. Supply chain elements include organizations, entities, or tools that are used for the research and development, design, manufacturing, acquisition, delivery, integration, operations, maintenance, and disposal of systems, system components, or system services. Supply chain processes include supply chain risk management programs; SCRM strategies and implementation plans; personnel and physical security programs; hardware, software, and firmware development processes; configuration management tools, techniques, and measures to maintain provenance; shipping and handling procedures; and programs, processes, or procedures associated with the production and distribution of supply chain elements. Supply chain actors are individuals with specific roles and responsibilities in the supply chain. The evidence generated and collected during analyses and testing of supply chain elements, processes, and actors is documented and used to inform organizational risk management activities and decisions.

SR-8: Notification Agreements

Control Objective: Establish agreements and procedures with entities involved in the supply chain for the system, system component or system service for the:[144]

a. Notification of supply chain compromises;
b. Results of assessments or audits; and
c. Other information.

Standard: ACME's Chief Risk Officer (CRO), or the CRO's designated representative(s), must establish contractual agreements with entities involved in the supply chain for systems, applications and services for the:

(1) Notification of supply chain compromises;
(2) Sharing results of assessments or audits; and
(3) Other information that is pertinent to the security and/or privacy of ACME systems, applications and services.

Guidelines: The establishment of agreements and procedures facilitates communications among supply chain entities. Early notification of compromises and potential compromises in the supply chain that can potentially adversely affect or have adversely affected organizational systems or system components is essential for organizations to effectively respond to such incidents. The results of assessments or audits may include open-source information that contributed to a decision or result and could be used to help the supply chain entity resolve a concern or improve its processes.

SR-9: Tamper Resistance & Detection

Control Objective: Implement a tamper protection program for the system, system component or system service.[145]

[143] NIST SP 800-53 Rev 5 control SR-6(1)
[144] NIST SP 800-53 Rev 5 control SR-8
[145] NIST SP 800-53 Rev 5 control SR-9

Guidelines: Organizations recognize that incident response capabilities are dependent on the capabilities of organizational systems and the mission and business processes being supported by those systems. Organizations consider incident response as part of the definition, design and development of mission and business processes and systems. Incident-related information can be obtained from a variety of sources, including audit monitoring, physical access monitoring and network monitoring; user or administrator reports; and reported supply chain events. An effective incident handling capability includes coordination among many organizational entities (e.g., mission or business data/process owners, system data/process owners, authorizing officials, human resources offices, physical security offices, personnel security offices, legal departments, risk executive (function, operations personnel, procurement offices). Suspected security incidents include the receipt of suspicious email communications that can contain malicious code. Suspected supply chain incidents include the insertion of counterfeit hardware or malicious code into organizational systems or system components. For federal agencies, an incident that involves PII is considered a breach. A breach results in unauthorized disclosure, the loss of control, unauthorized acquisition, compromise or a similar occurrence where a person other than authorized user accesses or potentially accesses PII or an authorized user accesses or potentially accesses such information for other than authorized purposes.

IR-4(1): INCIDENT HANDLING | AUTOMATED INCIDENT HANDLING PROCESSES

Control Objective: Support the incident handling process using automated mechanisms.[209]

Standard: Where technically feasible and justified by a valid business case, ACME must implement automated mechanisms to support the incident handling process.

Guidelines: Automated mechanisms that support incident handling processes include online incident management systems and tools that support the collection of live response data, full network packet capture and forensic analysis.

IR-4(2): INCIDENT HANDLING | DYNAMIC RECONFIGURATION

Control Objective: Include organization-defined types of dynamic reconfiguration for organization-defined system components as part of the incident response capability.[210]

Standard: Where technically feasible and justified by a valid business case, ACME must implement automated mechanisms to enable dynamic reconfiguration of information systems as part of incident response remediation actions.

Guidelines: Dynamic reconfiguration includes changes to router rules, access control lists, intrusion detection or prevention system parameters and filter rules for guards or firewalls. Organizations may perform dynamic reconfiguration of systems to stop attacks, misdirect attackers and isolate components of systems, thus limiting the extent of the damage from breaches or compromises. Organizations include specific time frames for achieving the reconfiguration of systems in the definition of the reconfiguration capability, considering the potential need for rapid response to effectively address cyber threats.

IR-4(3): INCIDENT HANDLING | CONTINUITY OF OPERATIONS

Control Objective: Identify classes of incidents and take organization-defined actions in response to those incidents to ensure continuation of organizational mission and business functions.[211]

Standard: ACME's Integrated Incident Response Program (IIRP) addresses ten (10) categories of cybersecurity incidents. Each category has the potential to escalate and requires different handling procedures, per the IIRP:

#	Threat	Category	Category Description
0	**Training**	**Simulated Incident** (Training & Exercises)	This category is used during exercises and approved testing of internal/external network defenses or responses.
1	**Illegal Content or Activities**	**Illegal Content**	This category is used for any data that is illegal to have in possession. This includes illegal content such as child pornography or classified information on unclassified systems.

[209] NIST SP 800-53 Rev 5 control IR-4(1)
[210] NIST SP 800-53 Rev 5 control IR-4(2)
[211] NIST SP 800-53 Rev 5 control IR-4(3)

MEDIA PROTECTION (MP)

Media Protection Policy: ACME must protect system media, both hardcopy and digital, by limiting access to authorized users and sanitizing or destroying media so that unauthorized data recovery is technically infeasible.

Management Intent: The purpose of the Media Protection (MP) policy is to ensure that access to both paper and digital media is limited to authorized individuals.

Supporting Documentation: Media Protection (MP) control objectives, standards and guidelines directly support this policy.

MP-1: MEDIA PROTECTION POLICY & PROCEDURES

Control Objective:[232]

a. Develop, document and disseminate to organization-defined personnel or roles:
   1. Organization-level media protection policy that:
      (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities and compliance; and
      (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards and guidelines; and
   2. Procedures to facilitate the implementation of the media protection policy and the associated media protection controls;
b. Designate an organization-defined official to manage the development, documentation and dissemination of the media protection policy and procedures; and
c. Review and update the current media protection:
   1. Policy per an organization-defined frequency and following organization-defined events; and
   2. Procedures per an organization-defined frequency and following organization-defined events.

Standard: ACME's cybersecurity policies and standards must be consolidated in a single document, the Cybersecurity & Data Protection Program (CDPP). The CDPP:

(1) Documents ACME's security and privacy program and makes it available to authorized personnel that:
   (A) Identifies the requirements for ACME's security and privacy program, including Media Protection (MP)-related controls;
   (B) Identifies applicable statutory, regulatory and contractual obligations (see CDPP Applicability Matrix); and
   (C) Includes the identification and assignment of roles and responsibilities among stakeholders that reflects the coordination among the organizational entities responsible for security and privacy practices;
(2) Is approved by ACME's Chief Information Security Officer (CISO), who is ACME's designated official with the responsibility and accountability for security and privacy-related policies and standards;
(3) Establishes quantifiable requirements for people, processes and technologies to facilitate the development of procedures that are sufficient to document how ACME's policies and standards are implemented and enforced by stakeholders (e.g., data/process owners and asset custodians);
(4) Shall be reviewed annually, or as needed based on assessed need, by the CISO, or delegates who are qualified to perform review functions. Based on the review, any necessary updates to the CDPP will be implemented and distributed per ACME's established change management practices; and
(5) Must be protected from unauthorized disclosure and modification.

Guidelines: Media protection policy and procedures address the controls in the MP family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of media protection policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system SPPs or in one or more separate documents. Events that may precipitate an update to media protection policy and procedures include assessment or audit findings, security or privacy incidents or changes in applicable laws, executive orders, directives, regulations, policies, standards and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

[232] NIST SP 800-53 Rev 5 control MP-1

MP-2: Media Access

Control Objective: Restrict access to organization-defined types of digital and/or non-digital media to organization-defined personnel or roles.[233]

Standard: Data/process owners and asset custodians must restrict access to digital and non-digital media to authorized individuals, including:

(1) Assigning Role-Based Access Control (RBAC) to the specific data that is under their care or line of business to limit access to authorized personnel;
(2) Reviewing RBAC on a quarterly basis to verify only users with business justification have access; and
(3) Prohibiting ACME personnel, including ACME contractors/subcontractors, from releasing any information, regardless of medium (e.g., film, tape, document), pertaining to any part of a contract or any program related to a contract to anyone outside ACME. The only exceptions are if:
    (A) The project's contracting officer has given prior written approval; or
    (B) The information is otherwise in the public domain before the date of release.

Guidelines: System media includes digital and non-digital media. Digital media includes flash drives, diskettes, magnetic tapes, external or removable hard disk drives (e.g., solid state, magnetic), compact discs and digital versatile discs. Non-digital media includes paper and microfilm. Denying access to patient medical records in a community hospital unless the individuals seeking access to such records are authorized healthcare providers is an example of restricting access to non-digital media. Limiting access to the design specifications stored on compact discs in the media library to individuals on the system development team is an example of restricting access to digital media.

MP-3: Media Marking

Control Objective:[234]

a. Mark system media indicating the distribution limitations, handling caveats and applicable security markings (if any) of the information; and
b. Exempt organization-defined types of system media from marking if the media remain within organization-defined controlled areas.

Standard: ACME users must:

(1) Mark media in accordance with Annex 1: Data Classification & Handling Guidelines; and
(2) Configure systems to mark metadata in environments where Data Loss Prevention (DLP) and Network Access Control (NAC) technology is being used.

Guidelines: Security marking refers to the application or use of human-readable security attributes. Digital media includes diskettes, magnetic tapes, external or removable hard disk drives (e.g., solid state, magnetic), flash drives, compact discs and digital versatile discs. Non- digital media includes paper and microfilm. Control unclassified information is defined by the National Archives and Records Administration along with the appropriate safeguarding and dissemination requirements for such information and is codified in 32 CFR 2002. Security markings are generally not required for media that contains information determined by organizations to be in the public domain or to be publicly releasable. Some organizations may require markings for public information indicating that the information is publicly releasable.

System media marking reflects applicable laws, executive orders, directives, policies, regulations, standards and guidelines. The following labeling procedures should be followed to classify the sensitivity level of information contained within hard copy materials:

- Hard copy reports containing Confidential or Restricted information should be clearly marked on every page with an indication of the sensitivity level of the most sensitive information contained in the report and include page numbers;
- A cover page should be attached to all documents classified as Restricted, with the Information Owner's name, date and department; and
- Reports marked as containing Restricted information should be reviewed annually to ensure the marking is appropriate to the protection required for the information.

[233] NIST SP 800-53 Rev 5 control MP-2
[234] NIST SP 800-53 Rev 5 control MP-3

a. Users;
b. Devices; and
c. Encryption.

Standard: ACME personnel managers must ensure wireless networks use industry-recognized secure practices to implement strong encryption for authentication and transmission, commensurate with the sensitivity of the data being transmitted.

Guidelines: Wireless networking capabilities represent a significant potential vulnerability that can be exploited by adversaries. To protect systems with wireless access points, strong authentication of users and devices along with strong encryption can reduce susceptibility to threats by adversaries involving wireless technologies.

AC-18(3): Wireless Access | Disable Wireless Networking

Control Objective: Disable, when not intended for use, wireless networking capabilities embedded within system components prior to issuance and deployment.[348]

Standard: In sensitive environments, asset custodians must disable wireless networking capabilities in systems that do not have a legitimate need to have wireless network access.

Guidelines: Wireless networking capabilities that are embedded within system components represent a significant potential vulnerability that can be exploited by adversaries. Disabling wireless capabilities when not needed for essential organizational missions or functions can reduce susceptibility to threats by adversaries involving wireless technologies.

AC-18(4): Wireless Access | Restrict Configuration By Users

Control Objective: Identify and explicitly authorize users allowed to independently configure wireless networking capabilities.[349]

Standard: In sensitive environments, users are prohibited from independently configuring the wireless networking capabilities of their assigned systems.

Guidelines: Organizational authorizations to allow selected users to configure wireless networking capabilities are enforced, in part, by the access enforcement mechanisms employed within organizational systems.

AC-18(5): Wireless Access | Antennas & Transmission Power Levels

Control Objective: Select radio antennas and calibrate transmission power levels to reduce the probability that signals from wireless access points can be received outside of organization-controlled boundaries.[350]

Standard: Where technically feasible, data/process owners and asset custodians must confine the wireless transmission boundary to within the geographic confines of ACME's facilities through:
(1) Proper placement of Wireless Access Points (WAPs); and
(2) Limiting the output / transmission power of the WAPS.

Guidelines: Actions that may be taken to limit unauthorized use of wireless communications outside of organization-controlled boundaries include reducing the power of wireless transmissions so that the transmissions are less likely to emit a signal that can be captured outside of the physical perimeters of the organization, employing measures such as emissions security to control wireless emanations and using directional or beamforming antennas that reduce the likelihood that unintended receivers will be able to intercept signals. Prior to taking such mitigating actions, organizations can conduct periodic wireless surveys to understand the radio frequency profile of organizational systems as well as other systems that may be operating in the area.

AC-19: Access Control For Mobile Devices

Control Objective:[351]

a. Establish configuration requirements, connection requirements and implementation guidance for organization-controlled mobile devices, to include when such devices are outside of controlled areas; and
b. Authorize the connection of mobile devices to organizational systems.

[348] NIST SP 800-53 Rev 5 control AC-18(3)
[349] NIST SP 800-53 Rev 5 control AC-18(4)
[350] NIST SP 800-53 Rev 5 control AC-18(5)
[351] NIST SP 800-53 Rev 5 control AC-19

executive orders, directives, regulations, policies, standards and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

SC-2: Separation of System & User Functionality

Control Objective: Separate user functionality, including user interface services, from system management functionality.[483]

Standard: Where technically feasible, physically or logically separate user interfaces (e.g., public Web pages) must be implemented from storage and management services (e.g., administrative or database management). Separation may be accomplished through the use of one or more of the following:

(1) Network segmentation;
(2) Different computers;
(3) Different central processing units;
(4) Different instances of the operating system;
(5) Different network addresses; or
(6) Other methods as appropriate.

Guidelines: System management functionality includes functions that are necessary to administer databases, network components, workstations or servers. These functions typically require privileged user access. The separation of user functions from system management functions is physical or logical. Organizations may separate system management functions from user functions by using different computers, instances of operating systems, central processing units or network addresses; by employing virtualization techniques; or some combination of these or other methods. Separation of system management functions from user functions includes web administrative interfaces that employ separate authentication methods for users of any other system resources. Separation of system and user functions may include isolating administrative interfaces on different domains and with additional access controls. The separation of system and user functionality can be achieved by applying the systems security engineering design principles in SA-8, including SA-8(1), SA-8(3), SA-8(4), SA-8(10), SA-8(12), SA- 8(13), SA-8(14) and SA-8(18).

SC-3: Security Function Isolation

Control Objective: Isolate security functions from nonsecurity functions.[484]

Standard: Data/process owners and asset custodians must implement isolation techniques to prevent functions that require different security levels from co-existing on the same server. Isolation techniques include, but are not limited to:

(1) Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server;
(2) Firewall and router configurations need be configured to restrict connections between untrusted networks and any system components in ACME's trusted, internal network;
(3) Firewall need be installed at all connections from an internal to any other internal or external network;
(4) Demilitarized Zones (DMZs) need to be implemented to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols and ports;
(5) Servers which access external networks or are accessed from external networks need to be logically isolated from the private Intranet;
(6) Networks need to be segregated or divided into separate logical domains, so access between domains can be controlled by means of secure devices;
(7) Switched network technology need to be utilized, when possible, to prevent eavesdropping, session stealing or other exploits based on the accessibility of network traffic;
(8) Trust relationships should be strictly avoided between information resources with different risk profiles; and
(9) Information resources with higher protection requirements for confidentiality should not have a trusted relationship with a system that has lower protection requirements.
(10) If segmentation is used to isolate the sensitive networks from other networks, penetration tests must be performed at least annually and after any changes to segmentation controls/methods to verify that the segmentation methods are operational and effective and isolate all out-of-scope systems from in-scope systems.

Guidelines: Security functions are isolated from nonsecurity functions by means of an isolation boundary implemented within a system via partitions and domains. The isolation boundary controls access to and protects the integrity of the hardware, software

[483] NIST SP 800-53 Rev 5 control SC-2
[484] NIST SP 800-53 Rev 5 control SC-3

- SUPPLEMENTAL DOCUMENTATION -

CYBERSECURITY & DATA PROTECTION PROGRAM (CDPP)

ANNEXES, TEMPLATES & REFERENCES

Version 2021.1

CDPP
Cybersecurity & Data Protection Program

TABLE OF CONTENTS

ANNEX 1: DATA CLASSIFICATION & HANDLING GUIDELINES

DATA CLASSIFICATION

Information assets are assigned a sensitivity level based on the appropriate audience for the information. If the information has been previously classified by regulatory, legal, contractual, or company directive, then that classification will take precedence. The sensitivity level then guides the selection of protective measures to secure the information. All data are to be assigned one of the following four sensitivity levels:

CLASSIFICATION	DATA CLASSIFICATION DESCRIPTION	
RESTRICTED	Definition	Restricted information is highly valuable, highly sensitive business information and the level of protection is dictated externally by legal and/or contractual requirements. Restricted information must be limited to only authorized employees, contractors, and business partners with a specific business need.
	Potential Impact of Loss	· **SIGNIFICANT DAMAGE** would occur if Restricted information were to become available to unauthorized parties either internal or external to [Company Name].
		· Impact could include negatively affecting [Company Name]'s competitive position, violating regulatory requirements, damaging the company's reputation, violating contractual requirements, and posing an identity theft risk.
CONFIDENTIAL	Definition	Confidential information is highly valuable, sensitive business information and the level of protection is dictated internally by [Company Name]
	Potential Impact of Loss	· **MODERATE DAMAGE** would occur if Confidential information were to become available to unauthorized parties either internal or external to [Company Name].
		· Impact could include negatively affecting [Company Name]'s competitive position, damaging the company's reputation, violating contractual requirements, and exposing the geographic location of individuals.
INTERNAL USE	Definition	Internal Use information is information originated or owned by [Company Name], or entrusted to it by others. Internal Use information may be shared with authorized employees, contractors, and business partners who have a business need, but may not be released to the general public, due to the negative impact it might have on the company's business interests.
	Potential Impact of Loss	· **MINIMAL or NO DAMAGE** would occur if Internal Use information were to become available to unauthorized parties either internal or external to [Company Name].
		· Impact could include damaging the company's reputation and violating contractual requirements.
PUBLIC	Definition	Public information is information that has been approved for release to the general public and is freely shareable both internally and externally.
	Potential Impact of Loss	· **NO DAMAGE** would occur if Public information were to become available to parties either internal or external to [Company Name].
		· Impact would not be damaging or a risk to business operations.

ANNEX 2: DATA CLASSIFICATION EXAMPLES

The table below shows examples of common data instances that are already classified to simplify the process. This list is not inclusive of all types of data, but it establishes a baseline for what constitutes data sensitivity levels and will adjust to accommodate new types or changes to data sensitivity levels, when necessary.

IMPORTANT: You are instructed to classify data more sensitive than this guide, if you feel that is warranted by the content.

Data Class	Sensitive Data Elements	Public	Internal Use	Confidential	Restricted
Client or Employee Personal Data	Social Security Number (SSN)				X
	Employer Identification Number (EIN)				X
	Driver's License (DL) Number				X
	Financial Account Number				X
	Payment Card Number (credit or debit)				X
	Government-Issued Identification (e.g., passport, permanent resident card, etc.)				X
	Controlled Unclassified Information (CUI)				X
	Birth Date			X	
	First & Last Name		X		
	Age		X		
	Phone and/or Fax Number		X		
	Home Address		X		
	Gender		X		
	Ethnicity		X		
	Email Address		X		
Employee-Related Data	Compensation & Benefits Data				X
	Medical Data				X
	Workers Compensation Claim Data				X
	Education Data			X	
	Dependent or Beneficiary Data			X	
Sales & Marketing Data	Business Plan (including marketing strategy)			X	
	Financial Data Related to Revenue Generation			X	
	Marketing Promotions Development		X		
	Internet-Facing Websites (e.g., company website, social networks, blogs, promotions, etc.)	X			
	News Releases	X			
Networking & Infrastructure Data	Username & Password Pairs				X
	Public Key Infrastructure (PKI) Cryptographic Keys (public & private)				X
	Hardware or Software Tokens (multifactor authentication)				X
	System Configuration Settings			X	
	Regulatory Compliance Data			X	
	Internal IP Addresses			X	
	Privileged Account Usernames			X	
	Service Provider Account Numbers			X	
Strategic Financial Data	Corporate Tax Return Information			X	
	Legal Billings			X	
	Budget-Related Data			X	
	Unannounced Merger and Acquisition Information			X	
	Trade Secrets (e.g., design diagrams, competitive information, etc.)			X	
Operating Financial Data	Electronic Payment Information (Wire Payment / ACH)			X	
	Paychecks			X	
	Incentives or Bonuses (amounts or percentages)			X	
	Stock Dividend Information			X	
	Bank Account Information			X	

ANNEX 3: DATA RETENTION PERIODS

The following schedule highlights suggested retention periods* for some of the major categories of data:
** Retention periods are measured in years, after the event occurrence (e.g., termination, expiration, contract, filing, etc.)*

CATEGORY	TYPE OF RECORD	RETENTION PERIOD
Business Records	Amendments	Permanent
	Annual Reports	Permanent
	Articles of Incorporation	Permanent
	Board of Directors (elections, minutes, committees, etc.)	Permanent
	Bylaws	Permanent
	Capital stock & bond records	Permanent
	Charter	Permanent
	Contracts & agreements	Permanent
	Copyrights	Permanent
	Correspondence (General)	5
	Correspondence (Legal)	Permanent
	Partnership agreement	Permanent
	Patents	Permanent
	Service marks	Permanent
	Stock transfers	Permanent
	Trademarks	Permanent
CATEGORY	**TYPE OF RECORD**	**RETENTION PERIOD**
Financial Records	Audit report (external)	Permanent
	Audit report (internal)	3
	Balance sheets	Permanent
	Bank deposit slips, reconciliations & statements	7
	Bills of lading	3
	Budgets	3
	Cash disbursement & receipt record	7
	Checks (canceled)	3
	Credit memos	3
	Depreciation schedule	7
	Dividend register & canceled dividend checks	Permanent
	Employee expense reports	3
	Employee payroll records (W-2, W-4, annual earnings records, etc.)	7
	Financial statements (annual)	Permanent
	Freight bills	3
	General ledger	Permanent
	Internal reports (work orders, sales reports, production reports)	3
	Inventory lists	3
	Investments (sales & purchases)	Permanent
	Profit / Loss statements	Permanent
	Purchase and sales contracts	3
	Purchase order	3
	Subsidiary ledgers (accounts receivable, accounts payable, etc.)	Permanent
	Tax returns	Permanent
	Vendor Invoices	7
	Worthless securities	7

ANNEX 4: BASELINE SECURITY CATEGORIZATION GUIDELINES

Assets and services are categorized by two primary attributes: (a) the potential impact they pose from misuse and (b) the data classification level of the data processed, stored or transmitted by the asset or process. These two attributes combine to establish a basis for controls that should be assigned to that system or asset. *This basis is called an Assurance Level (AL).*

DATA SENSITIVITY

This is straightforward where the data sensitivity rating represents the highest data classification of the data processed, stored or transmitted by the asset or process

SAFETY & CRITICALITY

The Safety & Criticality (SC) rating reflects two aspects of the "importance" of the asset or process:

- On one hand, SC simply represents the importance of the asset relative to the achievement of the company's goals and objectives (e.g., business critical, mission critical, or non-critical).
- On the other hand, SC represents the potential for harm that misuse of the asset or service could cause to [Company Name], its clients, its partners, or the general public.

The three (3) SC ratings are:

- SC-1: Mission Critical. This category involves systems, services and data that is determined to be vital to the operations or mission effectiveness of [Company Name]:
  - Includes systems, services or data with the potential to significantly impact the brand, revenue or customers.
  - Any business interruption would have a significant impact on [Company Name]'s mission.
    - Cannot go down without having a significant impact on [Company Name]'s mission.
    - The consequences of loss of integrity or availability of a SC-1 system are unacceptable and could include the immediate and sustained loss of mission effectiveness.
  - *Requires the most stringent protection measures that exceed leading practices* to ensure adequate security.
  - Safety aspects of SC-1 systems, services and data could lead to:
    - Catastrophic hardware failure;
    - Unauthorized physical access to premises; and/or
    - Physical injury to users.
- SC-2: Business Critical. This category involves systems, services and data that are determined to be important to the support of [Company Name]'s business operations:
  - Includes systems, services or data with the potential to moderately impact the brand, revenue or customers.
  - Affected systems, services or data can go down for up to twenty-four (24) hours (e.g., one (1) business day) without having a significant impact on [Company Name]'s mission.
    - Loss of availability is difficult to deal with and can only be tolerated for a short time.
    - The consequences could include delay or degradation in providing important support services or commodities that may seriously impact mission effectiveness or the ability to operate.
    - The consequences of loss of integrity are unacceptable.
  - *Requires protection measures equal to or beyond leading practices* to ensure adequate security.
  - Safety aspects of SC-2 systems could lead to:
    - Loss of privacy; and/or
    - Unwanted harassment.
- SC-3: Non-Critical. This category involves systems, services and data that are necessary for the conduct of day-to-day operations, but are not business critical in the short-term:
  - Includes systems, services or data with little or potential to impact the brand, revenue or customers.
  - Affected systems, services or data can go down for up to seventy-two (72) hours (e.g., three (3) business days) without having a significant impact on [Company Name]'s mission.
    - The consequences of loss of integrity or availability can be tolerated or overcome without significant impacts on mission effectiveness.
    - The consequences could include the delay or degradation of services or routine activities.
  - *Requires protection measures that are commensurate with leading practices* to ensure adequate security.
  - Safety aspects of SC-3 systems could lead to:
    - Inconvenience;
    - Frustration; and/or
    - Embarrassment.

Where the data sensitivity and SC levels meet are considered the Assurance Levels (AL). The AL represents the "level of effort" that is needed to properly ensure the Confidentiality, Integrity, Availability and Safety (CIAS) of the asset or process.

Asset Categorization Matrix		Data Sensitivity			
		RESTRICTED	CONFIDENTIAL	INTERNAL USE	PUBLIC
Safety & Criticality	SC-1 Mission Critical	Enhanced	Enhanced	Enhanced	Enhanced
	SC-2 Business Critical	Enhanced	Enhanced	Basic	Basic
	SC-3 Non-Critical	Enhanced	Basic	Basic	Basic

Figure 1: Asset Categorization Risk Matrix

Basic Assurance Requirements

- The minimum level of controls is defined as industry-recognized leading practices (e.g., PCI DSS, NIST 800-53, ISO 27002, etc.).
- For security controls in Basic assurance projects or initiatives, the focus is on the digital security controls being in place with the expectation that no obvious errors exist and that as flaws are discovered they are addressed in a timely manner.

Enhanced Assurance Requirements

- The minimum level of controls is defined as exceeding industry-recognized leading practices (e.g., DLP, FIM, DAM, etc.).
- For security controls in Enhanced Assurance projects, it is essentially the Standard Assurance level that is expanded to require more robust Cybersecurity capabilities that are commensurate with the value of the project to [Company Name].