YOUR LOGO GOES HERE

Cybersecurity & Data Protection Program (CDPP)

NIST SP 800-171 & CMMC Compliance Program

ACME Professional Services, LLC

CDPP

Cybersecurity & Data Protection Program

INTERNAL USE
Access Limited to Internal Use Only

IT IS PROHIBITED TO DISCLOSE THIS DOCUMENT TO THIRD-PARTIES WITHOUT AN EXECUTED NON-DISCLOSURE AGREEMENT (NDA)

Table of Contents

NOTICE

DOCUMENTATION STRUCTURE

The Cybersecurity & Data Protection Program (CDPP) leverages its structure the ComplianceForge Reference Model (Hierarchical Cybersecurity Governance Framework) for the structure of the policies, control objectives, standards and guidelines.[1] The controls objectives used in the CDPP are based on Secure Controls Framework (SCF) controls to provide crosswalk mapping to:[2]

- NIST SP 800-171 R2 (CUI & NFO controls);
- NIST SP 800-171A Assessment Objectives (AOs);
- Cybersecurity Maturity Model Certification (CMMC) 2.0 controls; and
- Other relevant laws, regulations and frameworks.

At the end of this document, **Appendix A** contains a crosswalk mapping between CDPP standards and:

- NIST SP 800-171 R2 (CUI & NFO controls);
- NIST SP 800-171A Assessment Objectives (AOs);
- Cybersecurity Maturity Model Certification (CMMC) 2.0 controls.

REFERENCED FRAMEWORKS & SUPPORTING PRACTICES

This document references numerous leading industry frameworks in an effort to provide a data-centric, holistic approach to securely designing, building and maintaining ACME Professional Services, LLC's (ACME)systems, applications and services. The following external content is a non-exhaustive list of frameworks that are referenced by or support ACME's NIST SP 800-171 Compliance Program (NCP):

- The National Institute of Standards and Technology (**NIST**): [3]
  - NIST SP 800-37: *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*
  - 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 800-64: *Security Considerations in Secure Development Life Cycle*
  - NIST SP 800-122: *Guide to Protecting the Confidentiality of Personal Information (PI)*
  - NIST SP 800-160: *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*
  - 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 IR 7298: *Glossary of Key Cybersecurity Terms*
  - NIST IR 8179: *Criticality Analysis Process Model: Prioritizing Systems and Components* [draft]
  - *NIST Framework for Improving Critical Cybersecurity* (Cybersecurity Framework)
- Other Frameworks:
  - Cloud Security Alliance Cloud Controls Matrix (**CSA CCM**)[4]
  - Center for Internet Security (**CIS**)[5]
  - Defense Information Systems Agency (**DISA**) Secure Technology Implementation Guides (**STIGs**)[6]
  - Cybersecurity Maturity Model Certification (**CMMC**)[7]
  - Secure Controls Framework (**SCF**)[8]

[1] Hierarchical Cybersecurity Governance Framework (HCGF) - https://content.complianceforge.com/Hierarchical_Cybersecurity_Governance_Framework.pdf
[2] Secure Controls Framework (SCF) - https://securecontrolsframework.com
[3] National Institute of Standards and Technology - http://csrc.nist.gov/publications/PubsSPs.html
[4] Cloud Security Alliance - https://cloudsecurityalliance.org/
[5] Center for Internet Security - https://www.cisecurity.org/
[6] Defense Information Systems Agency (DISA)- https://public.cyber.mil/
[7] DoD CIO - https://dodcio.defense.gov/CMMC
[8] Secure Controls Framework – https://www.securecontrolsframework.com

CYBERSECURITY PROGRAM STRUCTURE

MANAGEMENT DIRECTION FOR CYBERSECURITY

The objective of the CDPP is to provide management direction and support for cybersecurity in accordance with business requirements and relevant laws and regulations. [9] The CDPP represents an Information Security Management System (ISMS). This 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.

CONCEPT OF OPERATIONS (CONOPS) – ESTABLISHING & MAINTAINING SECURE PRACTICES

ACME's CDPP is focused on protecting regulated data (FCI/CUI). These policies and standards are directly influenced by ACME's strategic and operational planning processes to reflect strategic objectives and initiatives, where appropriate. The CDPP is designed to change, as necessary, to reflect corrective actions, changes in requirements or other improvements.

For NIST SP 800-171 and Cybersecurity Maturity Model Certification (CMMC) compliance, ACME utilizes the CDPP's policies and standards to define organization-specific requirements to:

- Satisfactorily applicable requirements; and
- Provide objective criteria for control operators to develop and implement procedures.

ACME's cybersecurity and data protection documentation is comprised of six (6) main parts:

(1) Core policy that establishes management's intent;
(2) Control objective that identifies leading practices;
(3) Standards that provides quantifiable requirements;
(4) Controls identify desired conditions that are expected to be met;
(5) Procedures / Control Activities establish how tasks are performed to meet the requirements established in standards and to meet controls; and
(6) Guidelines are recommended, but not mandatory.

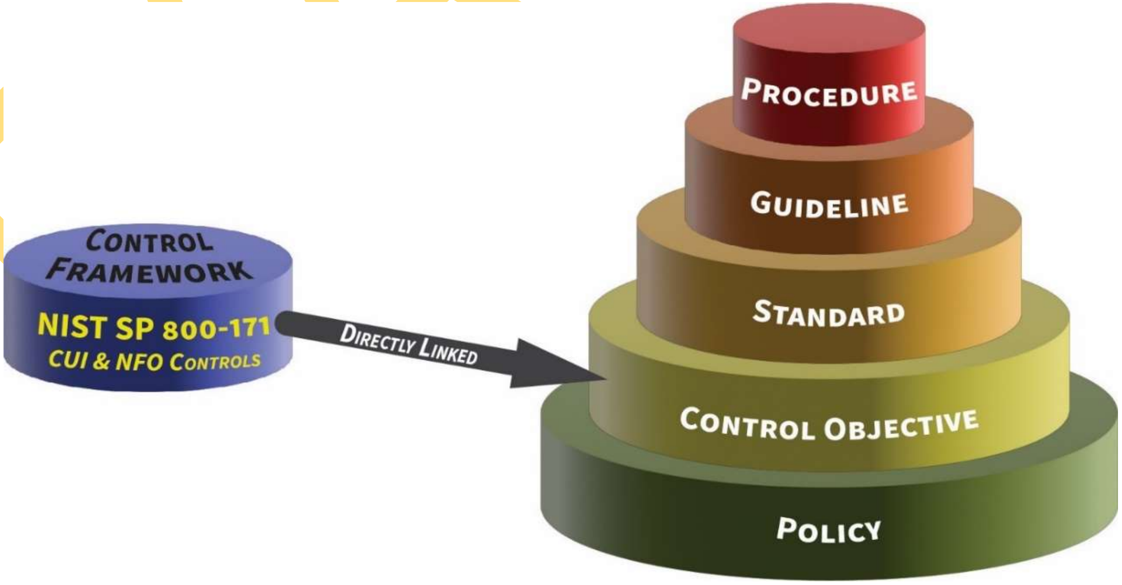


Figure 1: Cybersecurity Documentation Hierarchy

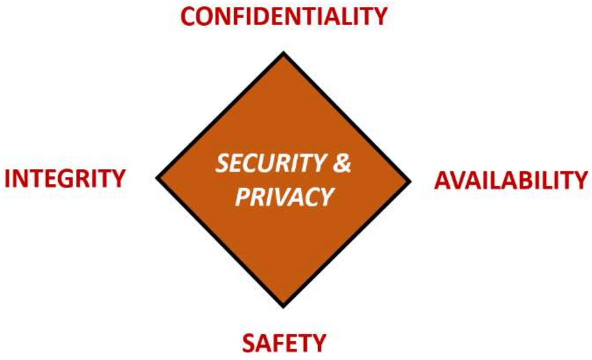
[9] ISO 27002 5.1

NIST SP 800-171 Compliance Program Overview

Introduction

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, cybersecurity 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** – This addresses preserving authorized restrictions on access and disclosure to authorized users and services, including means for protecting personal privacy and proprietary information.
- **INTEGRITY** – This addresses protecting against improper modification or destruction, including ensuring non-repudiation and authenticity.
- **AVAILABILITY** – This addresses timely, reliable access to data, systems and services for authorized users, services and processes.
- **SAFETY** – This addresses reducing risk associated with technologies that could fail or be manipulated by nefarious actors to cause death, injury, illness, damage to or loss of equipment.

Purpose

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

- Creating a leading practice-based cybersecurity program to address NIST SP 800-171 & CMMC requirements for:
  - Controlled Unclassified Information (CUI);
  - Non-Federal Organization (NFO);
  - Level 1 & 2 CMMC practices and processes (according to DoD guidance for CMMC v2.0).
- Protecting the confidentiality, integrity, availability and safety 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 control objectives, 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

The CDPP provides definitive information on the prescribed measures used to establish and enforce the NIST SP 800-171 & CMMC compliance program at ACME Professional Services, LLC (ACME).

These policies, standards and procedures 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; and
- Data, systems, activities and assets owned, leased, controlled or used by ACME, its agents, contractors or other business partners on behalf of ACME that are within scope of NIST SP 800-171 & CMMC through storing, processing or transmitting Federal Contract Information (FCI) and Controlled Unclassified Information (CUI).

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

These policies do not supersede any other applicable law or higher-level company directive or existing labor management agreement in effect as of the effective date of this policy.

ACME's cybersecurity roles & responsibilities provides a detailed description of ACME user roles and responsibilities, in regard to cybersecurity.

Policy Overview

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

ACME users are required to 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 controls will be tailored accordingly so that cost-effective controls can be applied commensurate with the risk and sensitivity of the data and system; and
- Security controls must be designed and maintained to ensure compliance with all legal requirements.

Violations

Any ACME user found to have violated any policy, standard or procedure may be 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

While every exception to a standard potentially weakens protection mechanisms for ACME systems and underlying data, occasionally exceptions will exist. When requesting an exception, users are required to submit a business justification for deviation from the standard in question.

Updates

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

Updates to the 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.

ASSET MANAGEMENT (AST) POLICY & STANDARDS

Management Intent: The purpose of the Asset Management (AST) policy is to ensure that technology assets are properly managed throughout the lifecycle of the asset, from procurement through disposal.

Policy: ACME shall implement and maintain appropriate IT Asset Management (ITAM) practices to strengthen the security and resilience of its technology infrastructure and data protection capabilities against both physical and cyber threats.

Supporting Documentation: This policy is supported by the following control objectives, standards and guidelines.

AST-01: ASSET GOVERNANCE

Control Objective: The organization facilitates an IT Asset Management (ITAM) program to implement and manage asset management controls.[16]

Standard: ACME's Chief Information Officer (CIO), or the CIO's designated representative(s), must establish and maintain an IT Asset Management (ITAM) program that includes, but is not limited to:

(a) Maintaining an accurate and current list of IT assets that includes but is not limited to:
   1. Make and model of the device;
   2. Location of device; and
   3. Device serial number or other methods of unique identification;

(b) A method to accurately and readily determine owner, contact information and purpose (e.g., labeling, coding and/or inventorying of devices); and

(c) A list of company-approved products.

Guidelines: It is also possible that the owner and custodian of the hardware, software and data are the same, but this needs to be identified and documented.

AST-02: ASSET INVENTORIES

Control Objective: The organization performs inventories of technology assets that: [17]

- Accurately reflects the current systems, applications and services in use;
- Identifies authorized software products, including business justification details;
- Is at the level of granularity deemed necessary for tracking and reporting;
- Includes organization-defined information deemed necessary to achieve effective property accountability; and
- Is available for review and audit by designated organizational personnel.

Standard: ACME's Chief Information Officer (CIO), or the CIO's designated representative(s), must establish and maintain an IT Asset Management (ITAM) program that inventories ACME's technology assets as follows:

(a) Hardware and software inventories, both:
   1. Internally-hosted assets; and
   2. Externally-hosted assets;

(b) A method to accurately and readily determine owner, contact information and purpose (e.g., labeling, coding and/or inventorying of devices);

(c) List of company-approved products;

(d) Updating the inventory as necessary; and

(e) Where technically feasible, a list of all personnel with access to assets.

Guidelines: The inventory should be updated as an integral part of component installations, removals and system updates. Without an inventory, some system components could be forgotten and be inadvertently excluded from applicable configuration standards. Inventory specifications include, for example, manufacturer, device type, model, serial number and physical location. Devices such

[16] ISO 27001-2013: 4.2 | ISO 27002-2022: 5.30, 5.31, 7.9 | NIST SP 800-53 R5: PM-5 | NIST CSF: ID.AM-1 | NIST SP 800-171 R2: 3.4.1

[17] ISO 27002-2022: 5.9 | NIST SP 800-53 R5: CM-8, PM-5 | NIST CSF: ID.AM-1, ID.AM-2, ID.AM-4 | NIST SP 800-171 R2: 3.4.1 | NIST SP 800-171A: 3.4.1[d], 3.4.1[e], 3.4.1[f]

CHANGE MANAGEMENT (CHG) POLICY & STANDARDS

Management Intent: The purpose of the Change Management (CHG) policy is for both technology and business leadership to proactively manage change. Without properly documented and implemented change controls, security features could be inadvertently or deliberately omitted or rendered inoperable, processing irregularities could occur or malicious code could be introduced. This includes the assessment, authorization and monitoring of technical changes across the enterprise.

Policy: ACME shall implement and maintain appropriate change management practices to reduce the risk associated with unauthorized or improper change. ACME requires active stakeholder involvement to ensure changes are appropriately tested, validated and documented before implementing any change on a production network.

Supporting Documentation: This policy is supported by the following control objectives, standards and guidelines.

CHG-01: CHANGE MANAGEMENT PROGRAM

Control Objective: The organization facilitates the implementation of change management controls.[23]

Standard: ACME's Change Management Program requires data/process owners and asset custodians to test, validate and document changes to systems before implementing the changes on the production network. Changes for any production system, application and/or service must:

(a) Be approved a ACME employee with the appropriate authority and knowledge to understand the impact of the change; and

(b) Sufficiently document the following criteria to enable independent review:

1. Reason for, and description of, the change;
2. Documentation of security impact;
3. Documented change approval by authorized parties;
4. Functionality testing to verify the change:
    - i. Did not adversely impact the security of the network; and
    - ii. Performs as expected;
5. For bespoke and custom software changes, all updates are tested for compliance with applicable statutory, regulatory and contractual obligations; and
6. Procedures to address failures and return to a secure state;

(c) Ensure all applicable statutory, regulatory and contractual requirements are confirmed to be in place on all new or changed systems and networks; and

(d) As applicable, update affected documentation to include the changes to prevent inconsistencies between network documentation and the actual configuration.

Guidelines: Change management processes are initiated when deficiencies in the design or operating effectiveness of controls are identified during system operation and are monitored to meet the entity's commitments and system requirements as they relate to security, availability, processing integrity, confidentiality or privacy or any combination thereof.

Due to the constantly changing state of pre- production environments, they are often less secure than the production environment. Organizations must clearly understand which environments are test environments or development environments and how these environments interact on the level of networks and applications.

Pre-production environments include development, testing, User Acceptance Testing (UAT), etc. Even where production infrastructure is used to facilitate testing or development, production environments still need to be separated (logically or physically) from pre- production functionality such that vulnerabilities introduced as a result of pre-production activities do not adversely affect production systems.

[23] ISO 27002-2022: 8.19, 8.32 | NIST SP 800-53 R5: CM-3 | NIST SP 800-171 R2: 3.4.3 | NIST CSF: PR.IP-3

CHG-02: Configuration Change Control

Control Objective: The organization governs the technical configuration change control processes.[24]

Standard: Data/process owners and asset custodians must follow ACME's change control processes and procedures for all changes to system components:

(a) Utilize separate environments for development/testing/staging and production;
(b) Utilize a separation of duties between development/testing/staging and production environments;
(c) Prohibit the use of production data (e.g., live PANs) for testing or development;
(d) Remove test data and accounts before production systems become active/goes into production; and
(e) Develop change control procedures for the implementation of security patches and software modifications, which includes, but is not limited to the following:
    1. Documentation of impact;
    2. Documented change approval by authorized parties; and
    3. Functionality testing to verify that the change does not adversely impact the security of the system;
(f) Back-out procedures; and
(g) Upon completion of significant change, all relevant compliance requirements must be implemented on all new or changed systems and networks and documentation updated as applicable.

Guidelines: Configuration change controls for organizational systems involve the systematic proposal, justification, implementation, testing, review and disposition of changes to the systems, including system upgrades and modifications. Configuration change control includes changes to baseline configurations for components and configuration items of systems, changes to configuration settings for information technology products (e.g., operating systems, applications, firewalls, routers and mobile devices), unscheduled/unauthorized changes and changes to remediate vulnerabilities.

CHG-02.2: Configuration Change Control | Test, Validate & Document Changes

Control Objective: The organization tests and documents proposed changes in a non-production environment before changes are implemented in a production environment.[25]

Standard: Where technically feasible, data/process owners and asset custodians must test and validate configuration changes in a test environment, prior to deploying the change in the production environment.

Guidelines: When operating platforms are changed, mission-critical (SC1) and business-critical (SC2) technology assets should be reviewed and tested to ensure there is no adverse impact on organizational operations or security. If it is not technically or logistically feasible to test a configuration change, compensating control should be identified and implemented in order to mitigate any negative impact to the production environment from an adverse change event. Compensating controls can include, but is not limited to:

- Images of systems;
- Backups of configurations;
- Viable back out plan;
- After-hours implementation; and
- Pilot/test group rollouts.

CHG-03: Security Impact Analysis for Changes

Control Objective: The organization analyzes proposed changes for potential security impacts, prior to the implementation of the change.[26]

Standard: Where technically feasible, from a test environment, data/process owners and asset custodians must test proposed changes specifically to assess the security functions of the system(s) to verify that those functions are:

(a) Implemented correctly;
(b) Operate as intended; and
(c) Meet the security requirements for the system.

[24] ISO 27002-2022: 8.19, 8.32 | NIST SP 800-53 R5: CM-3, SA-8(31) | NIST CSF: PR.IP-3 | NIST SP 800-171 R2: 3.4.3 | NIST SP 800-171A: 3.4.3[a], 3.4.3[b], 3.4.3[c], 3.4.3[d]

[25] ISO 27002-2022: 8.19, 8.32 | NIST SP 800-53 R5: CM-3(2), CM-3(7), SA-8(31) | NIST SP 800-171 R2: NFO - CM-3(2)

[26] NIST SP 800-53 R5: CM-4 | NIST SP 800-171 R2: 3.4.4 | NIST SP 800-171A: 3.4.4

CONFIGURATION MANAGEMENT (CFG) POLICY & STANDARDS

Management Intent: The purpose of the Configuration Management (CFG) policy is to establish and maintain the integrity of systems. Without properly documented and implemented configuration management controls, security features could be inadvertently or deliberately omitted or rendered inoperable, processing irregularities could occur or malicious code could be introduced.

Policy: ACME shall ensure all technology platforms used in support of its business operations adhere with industry-recognized secure configuration management practices. Current and accurate inventories of technology platforms shall be maintained so applicable secure configuration settings can be enforced on those technology platforms.

Supporting Documentation: This policy is supported by the following control objectives, standards and guidelines.

CFG-01: CONFIGURATION MANAGEMENT PROGRAM

Control Objective: The organization facilitates the implementation of configuration management controls.[38]

Standard: ACME's Chief Information Officer (CIO), or the CIO's designated representative(s), must document ACME's organization-wide configuration management controls that, at a minimum, include:

(a) A formal, documented configuration management program;
(b) Processes to facilitate the implementation of the configuration management program, including procedures and associated controls; and
(c) Where technically feasible, data/process owners and asset custodians must configure systems to include a description of groups, roles and responsibilities for the logical management of those devices.

Guidelines: As systems continue through the System Development Life Cycle (SDLC), new configuration items may be identified and some existing configuration items may no longer need to be under configuration control. Configuration management plans satisfy the requirements in organizational configuration management policies while being tailored to individual systems.

CFG-02: SYSTEM HARDENING THROUGH BASELINE CONFIGURATIONS

Control Objective: The organization develops, documents and maintains secure baseline configurations for technology platform that are consistent with industry-accepted system hardening standards.[39]

Standard: ACME's enabling technologies must be configured securely to support its operations as follows:

(a) Personnel responsible for configuration and/or administering systems, applications and/or services must be knowledgeable in the specific security parameters and settings that apply to that technology;
(b) Considerations must include secure settings for parameters used to access cloud portals and/or cloud-based services; and
(c) ACME's Chief Information Security Officer (CISO), or the CISO's designated representative(s), must develop and enforce baseline secure configuration requirements as follows:
    1. For all technology platforms used by ACME that includes but is not limited to:
        i. Server-class systems;
        ii. Workstation-class systems;
        iii. Network devices;
        iv. Mobile devices;
        v. Databases;
        vi. Major applications;
        vii. Minor applications;
        viii. Cloud-based services; and
        ix. Embedded technologies;
    2. Secure baseline configurations must be in accordance with applicable legal, statutory and regulatory compliance obligations and align with reasonably-expected, hardening practices:

[38] ISO 27002-2022: 8.3, 8.9, 8.12 | NIST SP 800-53 R5: CM-1, CM-9 | NIST CSF: PR.IP-1 | NIST SP 800-171 R2: NFO - CM-1, NFO - CM-9

[39] ISO 27002-2022: 8.3, 8.5, 8.9, 8.12, 8.25, 8.26 | NIST SP 800-53 R5: CM-2, CM-6, SA-8, PL-10, SA-15(5) | NIST CSF: PR.IP-1, PR.IP-3 | NIST SP 800-171 R2: 3.4.1, 3.4.2 | NIST SP 800-171A: 3.4.1[a], 3.4.1[b], 3.4.1[c], 3.4.2[a], 3.4.2[b]

   i. Center for Internet Security (CIS);[40]
   ii. Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs); [41] or
   iii. Original Equipment Manufacturer (OEM) security configuration guidance;

3. Each operating system must be hardened to provide only necessary ports, protocols and services to meet business needs and have in place supporting technical controls such as: antivirus, file integrity monitoring and logging as part of their baseline operating build standard or template;
4. Deviations from standard baseline configurations must be authorized following change management processes prior to deployment, provisioning or use;
5. Unless a technical or business reason exists, standardized images will be used to represent hardened versions of the underlying operating system and the applications installed on the system. These images must be validated and refreshed on a regular basis to update their security configuration in light of recent vulnerabilities and attack vectors; and
6. Data/process owners and asset custodians must develop configuration standards for all system components that are consistent with industry-accepted system hardening standards. This process of pre-production hardening systems includes, but is not limited to:
   i. Verifying that system configuration standards are:
      I. Updated as new vulnerability issues are identified;
      II. Applied when new systems are configured; and
      III. Consistent with industry-accepted hardening standards;
   ii. Implementing only one primary function per server to prevent functions that require different security levels from co-existing on the same server (e.g., web servers, database servers and DNS should be implemented on separate servers); and
   iii. Enforcing least functionality, which includes but is not limited to:
      I. Allowing only necessary and secure services, protocols and daemons;
      II. Removing all unnecessary functionality, which includes but is not limited to:
         a. Scripts;
         b. Drivers;
         c. Features;
         d. Subsystems;
         e. File systems; and
         f. Unnecessary web servers;
      III. Implementing security features for any required services, protocols or daemons that are considered to be insecure, which includes but is not limited to using secured technologies such as Secure Shell (SSH), Secure File Transfer Protocol (S-FTP), Transport Layer Security (TLS) or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet and FTP;
      IV. Verifying system security parameters are configured to prevent misuse; and
      V. Documenting the functionality present on systems.

Guidelines: There are known weaknesses with many operating systems, databases, network devices, software, applications, container images, and other devices used by an entity or within an entity's environment. There are also known ways to configure these system components to fix security vulnerabilities. Fixing security vulnerabilities reduces the opportunities available to an attacker. By developing standards, entities ensure their system components will be configured consistently and securely, and address the protection of devices for which full hardening may be more difficult.

Keeping up to date with current industry guidance will help the entity maintain secure configurations. The specific controls to be applied to a system will vary and should be appropriate for the type and function of the system. Numerous security organizations have established system-hardening guidelines and recommendations, which advise how to correct common, known weaknesses.

CFG-02.1: System Hardening Through Baseline Configurations | Reviews & Updates

Control Objective: The organization reviews and updates baseline configurations:[42]

- At least annually;
- When required due to so; or
- As part of system component installations and upgrades.

[40] CIS Benchmarks - https://www.cisecurity.org/cis-benchmarks/
[41] DISA STIGs official site - https://public.cyber.mil/stigs/
[42] ISO 27002-2022: 8.9 | NIST SP 800-53 R5: CM-2 | NIST SP 800-171 R2: NFO - CM-2(1)

Standard: Data/process owners and asset custodians must review and update baseline configurations for systems under their control:

(a) At least annually;
(b) When required due to so; or
(c) As part of system component installations and upgrades.

Guidelines: None

CFG-02.5: System Hardening Through Baseline Configurations | Configure Systems, Components or Devices for High-Risk Areas

Control Objective: The organization configures systems utilized in high-risk areas with more restrictive baseline configurations.[43]

Standard: Where technically feasible and justified by a valid business case, ACME's cybersecurity personnel must develop and use specialized configurations with enhanced security requirements for systems, components or devices deployed to "high-risk" areas (e.g., sensitive/regulated data enclaves).

Guidelines: When it is known that systems, system components or devices (e.g., notebook computers, mobile devices) will be located in high-risk areas, additional security controls may be implemented to counter the greater threat in such areas compared with the relative physical security to organizational-controlled areas. For example, organizational policies and procedures for notebook computers used by individuals departing on and returning from travel include, for example, determining which locations are of concern, defining required configurations for the devices, ensuring that the devices are configured as intended before travel is initiated and applying specific safeguards to the device after travel is completed. Specially configured notebook computers include, for example, computers with sanitized hard drives, limited applications and additional hardening (e.g., more stringent configuration settings). Specified safeguards applied to mobile devices upon return from travel include, for example, examining the device for signs of physical tampering and purging/reimaging the hard disk drive.

CFG-03: Least Functionality

Control Objective: The organization configures systems to provide only essential capabilities by specifically prohibiting or restricting the use of ports, protocols, and/or services.[44]

Standard: ACME utilizes the "principle of least functionality" which means that only the minimum access and functionality necessary to perform an operation should be granted and only for the minimum amount of time necessary. Data/process owners and asset custodians must:

(a) Identify and remove insecure services, protocols and ports;
(b) Enable only necessary and secure services, protocols and daemons, as required for the function of the system;
(c) Implement security features for any required services, protocols or daemons that are considered to be insecure (e.g., NetBIOS, Telnet, FTP, etc.);
(d) Verify services, protocols and ports are documented and properly implemented by examining firewall and router configuration settings; and
(e) Remove all unnecessary functionality, such as:
    1. Scripts;
    2. Drivers;
    3. Features;
    4. Subsystems;
    5. File systems; and
    6. Unnecessary web servers.

Guidelines: Asset custodians should review functions and services of systems, to determine which functions and services are candidates for elimination (e.g., Instant Messaging, SMS, auto-execute and file sharing). ACME may utilize network scanning tools, intrusion detection and prevention systems and endpoint protections such as firewalls and host-based intrusion detection systems to identify and prevent the use of prohibited functions, ports, protocols and services.

[43] ISO 27002-2022: 8.12 | NIST SP 800-53 R5: CM-2(7) | NIST SP 800-171 R2: NFO - CM-2(7)

[44] ISO 27002-2022: 8.3, 8.9, 8.12 | NIST SP 800-53 R5: CM-7 | NIST CSF: PR.PT-3 | NIST SP 800-171 R2: 3.4.6 | NIST SP 800-171A: 3.4.6[a], 3.4.6[b] | FAR: 52.204-21(b)(1)(ii)

[Company Name] 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 seven (7) sensitivity levels:

CUI-Restricted	CUI - RESTRICTED Access Limited to Authorized Personnel Controlled Unclassified Information (CUI)
Sensitive Personal Data (sPD)-Restricted	sPD - RESTRICTED Access Limited to Authorized Personnel
Personal Data (PD)-Restricted	PD - RESTRICTED Access Limited to Authorized Personnel
Restricted	RESTRICTED Access Limited to Authorized Personnel
Confidential	CONFIDENTIAL Access Limited to Authorized Personnel
Internal Use	INTERNAL USE Access Limited to Internal Use Only
Public	PUBLIC Public Release Authorized

Classification	Data Sensitivity Description	
Controlled Unclassified Information (CUI) - Restricted	**Definition**	CUI-Restricted information is U.S. Government regulated data that is highly-sensitive business information and the level of protection is dictated externally by both NIST SP 800-171 and Cybersecurity Maturity Model Certification (CMMC) requirements. CUI-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 CUI-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 statutory, regulatory and/or contractual requirements and damaging the company's reputation.
Sensitive Personal Data (sPD) Restricted	**Definition**	Sensitive Personal Data (sPD) is a subset of Personal Data (PD) that is highly-sensitive information about individuals (e.g., consumers, clients and/or employees) and the level of protection is dictated externally by statutory, regulatory and/or contractual requirements. sPD Restricted information must be limited to what is authorized in the Privacy Notice for how and where the sPD is authorized to be stored, processed and/or transmitted.
	Potential Impact of Loss	· **SIGNIFICANT DAMAGE** would occur if sPD 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 statutory, regulatory and/or contractual requirements, damaging the company's reputation and posing a risk to identified individuals (e.g., identity theft, stalking, harassment, etc.).
Personal Data (PD) Restricted	**Definition**	Personal Data (PD) Restricted that is information that can identify an individual (e.g., consumers, clients and/or employees) and the level of protection is dictated externally by statutory, regulatory and/or contractual requirements. The difference between sPD Restricted and PD Restricted is that PD Restricted information is publicly-available information (e.g., social media, news, court filings, etc.). PD Restricted information must be limited to what is authorized in the Privacy Notice for how and where the PD Restricted is authorized to be stored, processed and/or transmitted, unless it is publicly-available information.

	Potential Impact of Loss	**· MODERATE DAMAGE would occur if PD 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 statutory, regulatory and/or contractual requirements and damaging the company's reputation.**
Restricted	Definition	Restricted information is highly-valuable, highly-sensitive business information and the level of protection is generally dictated externally by statutory, regulatory 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 and violating contractual requirements.
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.

Data Handling Guidelines

Note: For U.S. Government regulated data, the following requirements supersede [Company Name] data handling guidelines:

- *For **Federal Contract Information (FCI)**, the following sources are authoritative for FCI data handing:*
  - *48 CFR § 52.204-21 (basic safeguarding for Covered Contractor Information Systems (CCIS))*
- *For **Controlled Unclassified Information (CUI)**, the following sources are authoritative for CUI data handing:*
  - *32 CFR § 2002*
  - *DoD Instruction 5200.48*
  - *NIST SP 800-171 rev2*

Handling Controls	CUI - RESTRICTED	sPD - RESTRICTED	PD - RESTRICTED	RESTRICTED	CONFIDENTIAL	INTERNAL USE	PUBLIC
Non-Disclosure Agreement (NDA)	▪ NDA is required prior to access by non-employees.	▪ NDA is required prior to access by non-employees.	▪ NDA is required prior to access by non-employees.	▪ NDA is required prior to access by non-employees.	▪ NDA is recommended prior to access by non-employees.	*No NDA requirements*	*No NDA requirements*
Internal Network Transmission (wired & wireless)	▪ Encryption is required ▪ Instant Messaging is prohibited ▪ FTP is prohibited ▪ Logical access must use multi-factor authentication	▪ Encryption is required ▪ Instant Messaging is prohibited ▪ FTP is prohibited	▪ Encryption is required ▪ Instant Messaging is prohibited ▪ FTP is prohibited	▪ Encryption is required ▪ Instant Messaging is prohibited ▪ FTP is prohibited	▪ Encryption is recommended ▪ Instant Messaging is prohibited ▪ FTP is prohibited	*No special requirements*	*No special requirements*
External Network Transmission (wired & wireless)	▪ Encryption is required ▪ Instant Messaging is prohibited ▪ FTP is prohibited ▪ Logical access must use multi-factor authentication ▪ Remote access must use multi-factor authentication	▪ Encryption is required ▪ Instant Messaging is prohibited ▪ FTP is prohibited ▪ Remote access should be used only when necessary and only with VPN and multi-factor authentication	▪ Encryption is required ▪ Instant Messaging is prohibited ▪ FTP is prohibited	▪ Encryption is required ▪ Instant Messaging is prohibited ▪ FTP is prohibited ▪ Remote access should be used only when necessary and only with VPN and multi-factor authentication	▪ Encryption is required ▪ Instant Messaging is prohibited ▪ FTP is prohibited	▪ Encryption is recommended	*No special requirements*
Data At Rest (file servers, databases, archives, etc.)	▪ Encryption is required ▪ Logical access controls are required to limit unauthorized use ▪ Physical access	▪ Encryption is required ▪ Logical access controls are required to limit unauthorized use ▪ Physical access	▪ Encryption is required ▪ Logical access controls are required to limit unauthorized use ▪ Physical access	▪ Encryption is required ▪ Logical access controls are required to limit unauthorized use ▪ Physical access	▪ Encryption is recommended ▪ Logical access controls are required to limit unauthorized use	▪ Encryption is recommended ▪ Logical access controls are required to limit unauthorized use	▪ Logical access controls are required to limit unauthorized use ▪ Physical access restricted

[Company Name] 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	PD - Restricted	sPD - Restricted	CUI - Restricted
Non-Public Consumer, Client or Employee Personal Data That Can Uniquely Identify An Individual	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	
	Geolocation Information (e.g., precise geographic location and/or history)						X	
	Race / Ethnicity						X	
	Religious Affiliation						X	
	Union Membership						X	
	Philosophical Beliefs						X	
	Private Communications (e.g., contents of private mail, emails and text messages)						X	
	Genetic Information						X	
	Biometrics						X	
	Health Information						X	
	Sexual Orientation						X	
	Birth Date						X	
	First & Last Name						X	
	Age						X	
	Phone Number						X	
	Home Address						X	
	Gender						X	
	Email Address						X	
Publicly Available Consumer, Client or Employee Personal Data That Can Uniquely Identify An Individual	Geolocation Information (e.g., precise geographic location and/or history)					X		
	Race / Ethnicity					X		
	Religious Affiliation					X		
	Union Membership					X		
	Philosophical Beliefs					X		
	Private Communications (e.g., contents of private mail, emails and text messages)					X		
	Health Information					X		
	Sexual Orientation					X		
	Birth Date					X		
	First & Last Name					X		
	Age					X		
	Phone Number					X		

[Company Name] 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)*.

Safety & Criticality

One component of assessing risk is to understand the criticality of systems and data. By having a clear understanding of the Safety & Criticality Level (SC) for an asset, system, application, service or data, determining potential impact will be more accurate.

There are four (4) SC levels:

1. Mission Critical (SC1);
2. Business Critical (SC2);
3. Non-Critical (SC3); and
4. Business Supporting (SC4).

Mission Critical (SC1)

Mission Critical (SC1) assets handle information that is determined to be vital to the operations or mission effectiveness of [Company Name].

The impact of a SC1 system, or its data, being unavailable includes, but is not limited to:

- Enterprise-wide business stoppage with significant revenue impact can be anything that creates a significant impact on [Company Name]'s ability to perform its mission;
- Public, wide-spread damage to [Company Name]'s reputation;
- Direct, negative & long-term impact on customer satisfaction; and
- Risk to human health or the environment.

Examples of SC1 systems include, but are not limited to:

- *Enterprise Resource Management (ERM) system (e.g., SAP)*
- *Active Directory (AD)*
- *Ability to process Point of Sale (PoS) or eCommerce payments*

Business Critical (SC2)

Business Critical (SC2) assets handle information that is important to the support of [Company Name]'s primary operations.

The impact of a SC2 system, or its data, being unavailable includes, but is not limited to:

- Enterprise-wide delay or degradation in providing important support services that may seriously impact mission effectiveness or the ability to operate;
- Department-level business stoppage with direct or indirect revenue impact; and
- Direct, negative & short-term impact on customer satisfaction.

Examples of SC2 systems include, but are not limited to:

- *Email (e.g., Exchange)*
- *Payroll systems*
- *Corporate website functionality*
- *Corporate mobile device application functionality*
- *HVAC systems*
- *Customer support / call center functionality*

Non-Critical (SC3)

Non-Critical (SC3) assets handle information that is necessary for the conduct of day-to-day business, but they are not mission critical in the short-term.

The impact of a SC3 system, or its data, being unavailable includes, but is not limited to:

- Widespread delays or degradation of services or routine activities;
- Widespread employee productivity degradation;

- Indirect revenue impact; and
- Indirect negative customer satisfaction.

Examples of SC3 systems include, but are not limited to:

- *Test / Development / Staging environment*
- *Security Incident Event Monitor (SIEM) / log collector*
- *Internal / Intranet web functionality*

Business Supporting (SC4)

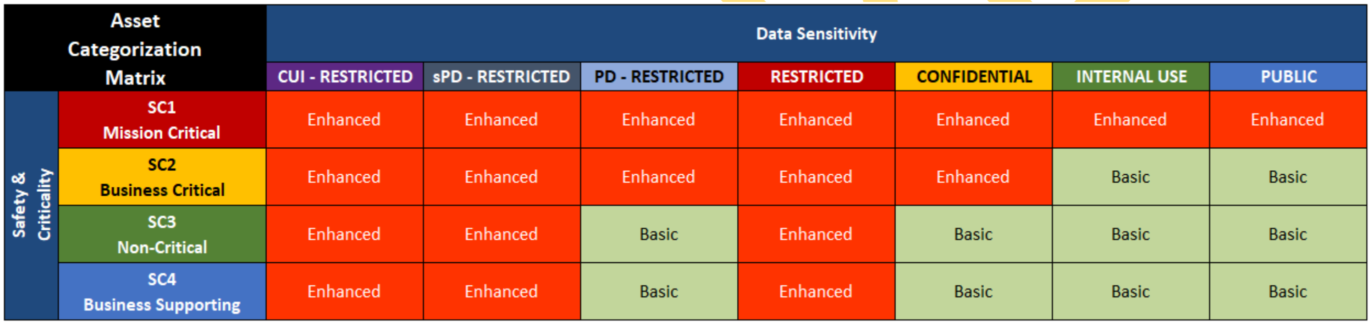
Business Supporting (SC4) assets are the least important category of systems and handle information that is used in the conduct of routine, day-to-day business. SC4 systems are not mission-critical in the short or long term.

The impact of a SC4 system, or its data, being unavailable includes, but is not limited to:

- Localized employee productivity degradation;
- Localized delays or degradation of services or routine activities;
- No revenue impact; and
- No impact on customer satisfaction.

Examples of SC4 systems include, but are not limited to:

- *Team-level metrics reporting*
- *Team-level productivity or reporting tools*



Asset Categorization Matrix		Data Sensitivity						
		CUI - RESTRICTED	sPD - RESTRICTED	PD - RESTRICTED	RESTRICTED	CONFIDENTIAL	INTERNAL USE	PUBLIC
Safety & Criticality	SC1 Mission Critical	Enhanced	Enhanced	Enhanced	Enhanced	Enhanced	Enhanced	Enhanced
	SC2 Business Critical	Enhanced	Enhanced	Enhanced	Enhanced	Enhanced	Basic	Basic
	SC3 Non-Critical	Enhanced	Enhanced	Basic	Enhanced	Basic	Basic	Basic
	SC4 Business Supporting	Enhanced	Enhanced	Basic	Enhanced	Basic	Basic	Basic

Figure 1: Asset Categorization Risk Matrix

Basic Assurance Requirements

Basic establishes the minimum level of control that would be "reasonably-expected" and is defined as industry-recognized secure practices (e.g., PCI DSS, NIST SP 800-53, ISO 27002, etc.). For security controls in Basic assurance projects or initiatives, the expectation for cybersecurity and privacy controls include:

- Controls are appropriately-scoped to address all applicable statutory, regulatory and contractual requirements;
- Technologies and processes are in-place with the expectation that no misconfigurations exist; and
- Flaw remediation processes correct any discovered flaws in a timely manner.

Enhanced Assurance Requirements

Enhanced establishes a more secure level of control that exceed minimum requirements and is defined as exceeding industry-recognized secure practices (e.g., DLP, FIM, DAM, etc.). These requirements are often "situationally required" per a statutory, regulatory or contractual obligation that is specific to a type of data or under a specific circumstance (e.g., personal data, cardholder data, electronic health protected information, etc.) where the expectation for cybersecurity and privacy controls include:

- Building upon Basic assurance requirements;
- Implementing robust preventative, detective and responsive capabilities exist that are commensurate with the value of the project to [Company Name]; and
- Stakeholders perform a greater role in maintaining situational awareness to ensure controls are properly executed and governed.