YOUR LOGO GOES HERE

DATA PRIVACY PROGRAM

EXAMPLE

ACME Worldwide Consulting, LLP

DPP
Data Privacy Program

INTERNAL USE
Access Limited to Internal Use Only

NOTICE

This document is intended for the following data subjects and teams with the assigned responsibilities:

- Cybersecurity governance, risk management, and oversight responsibilities;
- Privacy governance and oversight responsibilities;
- Systems and application engineering, architecture, design, development, and integration responsibilities;
- Independent security verification, validation, testing, auditing, assessment, and monitoring responsibilities; and
- Acquisition, budgeting, and project management and oversight responsibilities.

REFERENCED FRAMEWORKS & SUPPORTING PRACTICES

This document references numerous leading industry frameworks in an effort to provide a comprehensive and holistic approach to designing systems, applications and processes with both cybersecurity and privacy concepts being incorporated in all stages of the system development lifecycle. The following external content is referenced by or supports this Data Privacy Program (DPP) 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 800-64: *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 800-161: *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*
  - 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 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*
- Secure Controls Framework (SCF) [3]
  - SCF Security & Privacy Capability Maturity Model (SP-CMM)
  - SCF Security & Privacy Risk Management Model (SP-RMM)
  - SCF Privacy Management Principles
- Organization for the Advancement of Structured Information Standards (OASIS): [4]
  - OASIS *Privacy Management Reference Model and Methodology (PMRM)*
- Other Frameworks:
  - Cloud Security Alliance Cloud Controls Matrix (CSA CCM)[5]
  - Center for Internet Security (CIS)[6]
  - Department of Defense Cybersecurity Agency (DISA) Secure Technology Implementation Guides (STIGs)[7]
  - Generally Accepted Privacy Practices (GAPP)[8]
  - Fair Information Practice Principles (FIPP)[9]
  - Privacy by Design (PbD) [10]
  - European Union Regulation 2016/279 (General Data Protection Regulation (EU GDPR))[11]

EXAMPLE

[1] National Institute of Standards and Technology - http://csrc.nist.gov/publications/PubsSPs.html
[2] International Organization for Standardization - https://www.iso.org
[3] Secure Controls Framework - https://www.securecontrolsframework.com
[4] Privacy Management Reference Model and Methodology (PMRM) Version 1.0. http://docs.oasisopen.org/pmrm/PMRM/v1.0/csd01/PMRM-v1.0-csd01.html.
[5] Cloud Security Alliance - https://cloudsecurityalliance.org/
[6] Center for Internet Security - https://www.cisecurity.org/
[7] DoD Information Security Agency - https://public.cyber.mil/stigs/
[8] The American Institute of CPAs - http://www.aicpa.org
[9] Federal Trade Commission - https://www.ftc.gov
[10] Term and principles coined by Dr. Ann Cavoukian - https://www.owasp.org/index.php/Privacy_by_Design
[11] EU General Data Protection Regulation - https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_en

Table of Contents

EXAMPLE

EXAMPLE

EXAMPLE

CAPABILITY NEED

ACME's Privacy Program exists to ensure that data protection-related controls are adequately identified and implemented across its systems, applications, services, processes and other initiatives, including third-party service providers. ACME's privacy personnel are tasked to advise privacy stakeholders on Privacy by Design (PbD) matters, while providing oversight to ACME's executive management to hold the Line of Business (LOB) and other key stakeholders accountable for their associated data privacy practices.

The Data Privacy Program (DPP) prescribes a comprehensive framework for the collection, creation, use, dissemination, maintenance, retention, and/or disclosure of Personal Data / sensitive Personal Data (PD / sPD) at ACME. The privacy principles that are documented in the DPP apply to all ACME systems, applications and services that are owned, leased, controlled or used by ACME, its agents, contractors or other business partners on behalf of ACME.

PRIVACY PROGRAM DESCRIPTION

ACME's privacy department is made up of [insert #] teams, each with a functional area that provides its own unique set of services to ACME. Each team focuses on a specific area to support the Data Privacy Program's overall mission:

[edit the names and description of the teams your company has – the following teams are just common examples]

- Privacy Governance Function
  - Specialists in managing governance, risk and compliance operations.
  - Identifies applicable privacy laws, regulations and industry frameworks that ACME must comply with.
  - Governs ACME's privacy-related policies, standards and controls, in accordance with applicable laws, regulations and contractual obligations.
  - Assigns data protection controls to appropriate stakeholders and provides an oversight function for control execution.
  - Evaluates the effectiveness of proposed compensating data protection controls.
  - Assists in pre-production testing (e.g., control validation testing) to ensure privacy control implementation is appropriate.
  - Provides privacy-related consulting services to internal technology teams and business units.
- Data Protection Officer (DPO) Function
  - Collaborates with Business Process Owners (BPOs) to ensure the PD / sPD of data subjects (e.g., ACME's staff, customers and other parties) is stored, processed and/or transmitted in compliance with applicable data protection requirements.
  - Assists BPOs in performing Data Protection Impact Assessments (DPIAs).
  - Conducts recurring assessments of ACME's data handling practices.
  - Trains personnel with access to PD / sPD on secure and compliant data handling processes.
- Incident Response (IR) Function
  - Specialists in evaluating "data breach" incidents for privacy implications.

STATUTORY, REGULATORY & CONTRACTUAL OBLIGATIONS FOR DATA PROTECTION / PRIVACY

To properly scope ACME's Data Privacy Program, the DPP addresses requirements for the following compliance requirements:

[fill-in applicable statutory, regulatory and contractual requirements]

STATUTORY REQUIREMENTS

Example statutory requirements include:

- *Cable Communications Policy Act (CCPA)*
- *Children's Internet Protection Act (CIPA)*
- *Children's Online Privacy Protection Act (COPPA)*
- *Computer Fraud and Abuse Act (CFAA)*
- *Consumer Credit Reporting Reform Act (CCRRA)*
- *Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM)*
- *Electronic Communications Privacy Act (ECPA)*

EXAMPLE

OPERATIONALIZING THE DATA PRIVACY PROGRAM

ACME aligns its overall Data Privacy Program with the Secure Controls Framework Privacy Management Principles (SCF PMP) and may adopt other specialized privacy practices to enhance ACME's data protection controls for sensitive initiatives and critical business needs.[12] The SCF PMP is a "Rosetta Stone" of privacy management principles that maps to the following privacy practices:

1. AICPA's Trust Services Criteria (TSC) (2017)[13]
2. Asia-Pacific Economic Cooperation (APEC) [14]
3. California Privacy Rights Act (CPRA) [15]
4. European Union General Data Protection Regulation (EU GDPR) [16]
5. Fair Information Practice Principles (FIPPs) - Department of Homeland Security (DHS) [17]
6. Fair Information Practice Principles (FIPPs) - Office of Management and Budget (OMB) [18]
7. Generally Accepted Privacy Principles (GAPP) [19]
8. HIPAA Privacy Rule[20]
9. ISO/IEC 27701:2019[21]
10. ISO/IEC 29100:2011[22]
11. Nevada SB820[23]
12. NIST SP 800-53 R4[24]
13. NIST SP 800-53 R5[25]
14. NIST Privacy Framework v1.0[26]
15. OASIS Privacy Management Reference Model (PMRM) [27]
16. Organization for Economic Co-operation and Development (OECD) [28]
17. Office of Management and Budget (OMB) - Circular A-130[29]
18. Personal Information Protection and Electronic Documents Act (PIPEDA) [30]
19. Privacy by Design (PbD) – The 7 Foundational Principles [31]

The overall Data Privacy Program maturity target is to establish and maintain standardized, secure and compliant privacy practices across ACME. Given the nature of cybersecurity and privacy operations, it is arguable that CMM2 (Planned & Tracked) is the most reasonable maturity level for the Data Privacy Program to target for 2023, with the goal of CMM3 (Well-Defined) is the most reasonable maturity level for the Data Privacy Program to target for 2024.

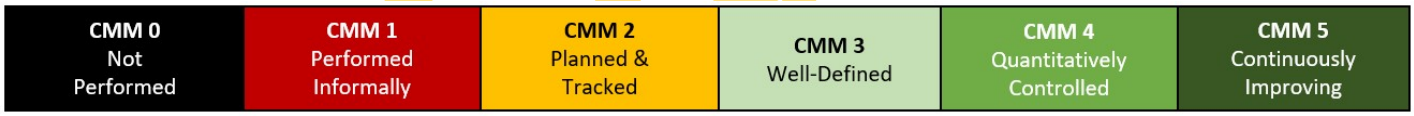


Figure 1. Security & Privacy Capability Maturity Model (SP-CMM)

These process maturation efforts will evolve ACME's Data Privacy Program from a reactive service delivery model to a proactive, consultative service delivery model. The underlying concept is forming a strategic alignment with the technology-related and privacy functions with the goal of embedding privacy-enabled practices in the development and maintenance of systems, applications and services that reduce risk to ACME.

[12] SCF PMP - https://securecontrolsframework.com/privacy-management-principles/
[13] AICPA TSC 2017 - https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpasoc2report.html
[14] APEC Privacy Framework - http://publications.apec.org/-/media/APEC/Publications/2005/12/APEC-Privacy-Framework/05_ecsg_privacyframewk.pdf
[15] CPRA Nov 2022 - https://cppa.ca.gov/regulations/pdf/20221102_mod_text.pdf
[16] EU GDPR - http://ec.europa.eu/justice/data-protection/reform/index_en.htm
[17] DHS FIPPs - https://www.dhs.gov/publication/fair-information-practice-principles-fipps
[18] OMB FIPPs - https://a130.cio.gov//Proposed%20A-130%20for%20Public%20Comment.pdf
[19] AICPA / CICA Privacy Maturity Model (GAPP) - https://www.kscpa.org/writable/files/AICPADocuments/10-229_aicpa_cica_privacy_maturity_model_finalebook.pdf
[20] HIPAA Privacy Rule - https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf
[21] ISO/IEC 27701:2019 - https://www.iso.org/standard/71670.html
[22] ISO/IEC 29100:2011 - https://www.iso.org/standard/45123.html
[23] Nevada SB220 - https://www.leg.state.nv.us/App/NELIS/REL/80th2019/Bill/6365/Text
[24] NIST SP 800-53 rev4 - https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final
[25] NIST SP 800-53 rev5 - https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final
[26] NIST Privacy Framework v1.0 - https://www.nist.gov/privacy-framework
[27] OASIS Privacy Management Reference Model (PMRM) - https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=pmrm
[28] OECD Privacy Principles - http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf#page=14
[29] OMB Circular A-130 - https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf
[30] PIPEDA - https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/
[31] Privacy by Design (PbD) - https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf

EXAMPLE

CONCEPT OF OPERATIONS (CONOPS)

To address the identified deficiency of standardized cybersecurity and privacy practices across ACME, establishing a Center of Excellence (CoE) within the Data Privacy Program is a step to provide ACME's business process owners and asset custodians and with "best practices" guidance, support and training so they both understand and utilize a uniform set of standards and practices though generations of products and employee changes. The CoE will serve as the source for standards and procedures when ACME employees have questions concerning privacy practices and data protection controls for systems, applications and/or services.

ACME is committed to establishing an organizational culture that ensures Security by Design / Privacy by Design (SpD / PbD) principles are an integral part of all activities. ACME shall use a multi-year strategy to address its incorporation of SpD / PbD principles to support ACME's overall business strategy. ACME will achieve this through:

- Controlling how PD / sPD is collected, created, used, disseminated, maintained, retained and disclosed.
- Developing a comprehensive strategy to holistically manage System Development Lifecycle (SDLC) processes that apply to:
  - Line of Business (LOB) operations and technology assets;
  - ACME's clients; and
  - Third-party organizations associated with the operation and use of ACME's systems, applications and/or services;
- Implementing the SDLC management strategy consistently across the entire organization; and
- Proactively reviewing and updating the SDLC management strategy to address both organizational changes and the evolving threat landscape.

Implementing SpD / PbD principles is a systematic way to find and address weaknesses, flaws and risks to ACME. The DPP is focused on helping ACME:

- Adopt repeatable, methodical processes to seek out privacy risks to reduce the chance of surprises;
- Address privacy issues in an orderly manner that gives ACME better assurance that gaps are closed properly and as quickly as possible; and
- Incorporate privacy considerations into all parts of the SDLC to reduce the costs of risk remediation.

ACME's existing policies and standards require that precautions are taken to ensure the security of systems and data, as well as the privacy of the data that ACME is entrusted with. The DPP:

- Supports ACME's existing policies and standards;
- Is intended to influence the development of secure and compliant processes at the department and team levels; and
- Focuses on putting privacy principles into practice.

IDENTIFYING "MUST HAVE" VS "NICE TO HAVE" REQUIREMENTS

For SpD / PbD, it is necessary to develop a catalog of data protection controls that addresses ACME's applicable statutory, regulatory and contractual obligations. Ideally, the controls are weighted since not all security & data protection controls are equal, in terms of impact or consequence. To assist in this process, it is helpful for ACME to categorize its applicable controls according to "must have" vs "nice to have" requirements:[32]

- Minimum Compliance Criteria (MCC) are the absolute minimum requirements that must be addressed to comply with applicable laws, regulations and contracts.
- Discretionary Security Requirements (DSR) are tied to the organization's risk appetite since DSR are "above and beyond" MCC, where the organization self-identifies additional cybersecurity and data protection controls to address voluntary industry practices or internal requirements, such as findings from internal audits or risk assessments.

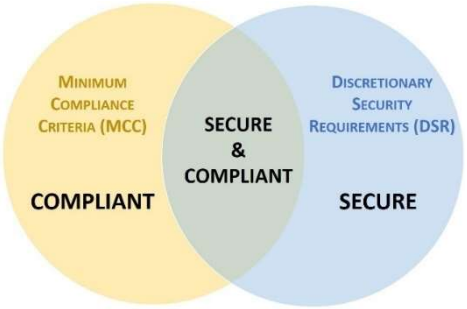


Figure 2. MCC vs DSR

Secure and compliant operations exist when both MCC and DSR are implemented and properly governed:

- MCC are primarily externally-influenced, based on industry, government, state and local regulations. MCC should never imply adequacy for secure practices and data protection, since they are merely compliance-related.
- DSR are primarily internally-influenced, based on the organization's respective industry and risk tolerance. While MCC establish the foundational floor that must be adhered to, DSR are where organizations often achieve improved efficiency, automation and enhanced security.

[32] Integrated Controls Management (ICM) model - http://integrated-controls-management.com/

EXAMPLE

Managing system-related cybersecurity and privacy risk is a complex undertaking that requires the involvement of the entire organization—from senior leaders providing the strategic vision and top-level goals and objectives for the organization, to mid-level leaders planning, executing, and managing projects, to individuals developing, implementing, operating, and maintaining the systems supporting the organization's missions and business functions.

DATA CENTRIC SECURITY (DCS) APPROACH TO LAYERED DEFENSES

Data, or information, is ACME's most valuable asset. Therefore, being data-centric is how ACME approach its defense-in-depth concept. When envisioned as a set of concentric boundaries, at the center is ACME's data.

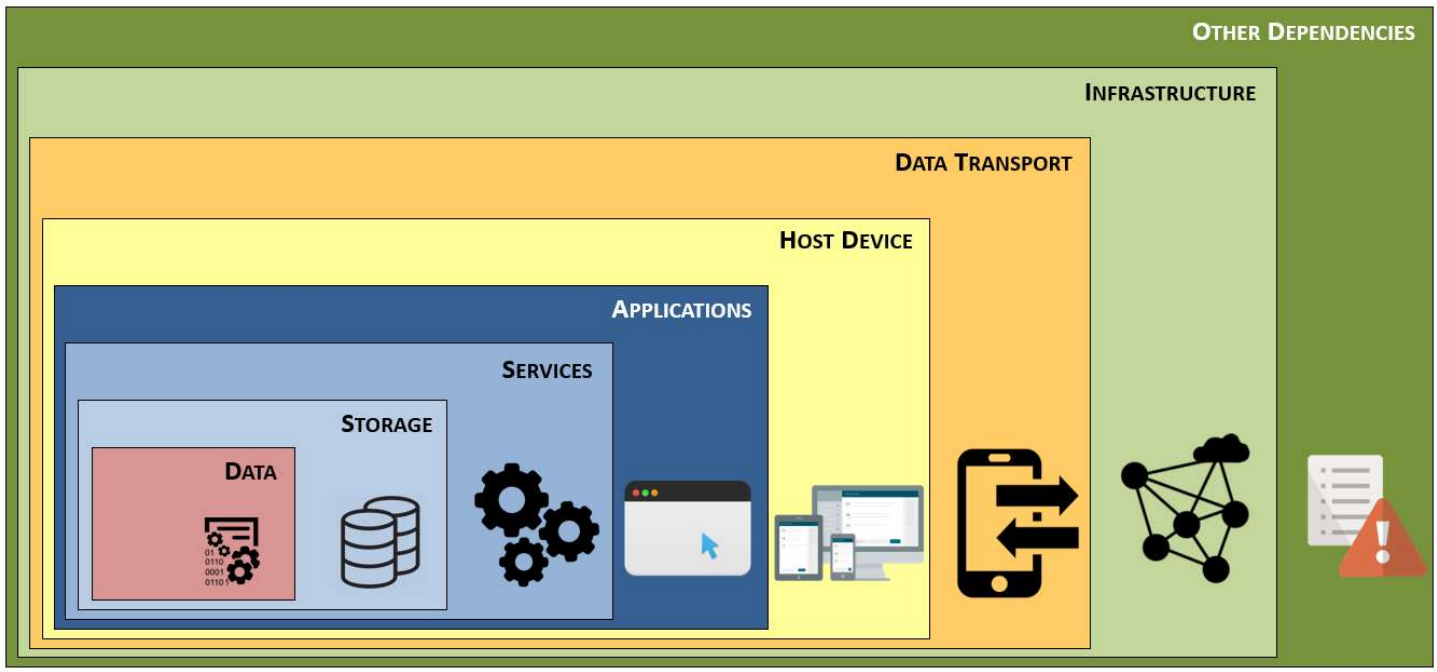


Figure 6. Data-Centric Security (DCS) approach to understanding dependencies.

This core concept of the data being the heart of protection measures will help built successive layers of protection. However, data centric security first starts with an awareness of both what our data is and where it is located. By improperly tracking data, ACME may not apply the correct levels of protection to sensitive or it could waste resources protecting data of minimal value.

MULTI-TIERED CYBERSECURITY & PRIVACY RISK MODEL

The image below illustrates a multi-level approach to risk management described in **NIST SP 800-39**, ***Managing Information Security Risk: Organization, Mission and Information System View***, that addresses cybersecurity and privacy risk at the organization level, the mission/business process level, and the information system level.[34] Communication and reporting are bi-directional information flows across the three levels to ensure that risk is addressed throughout the organization:

- Tier 1 – Organization
- Tier 2 – Business process
- Tier 3 – Information & systems

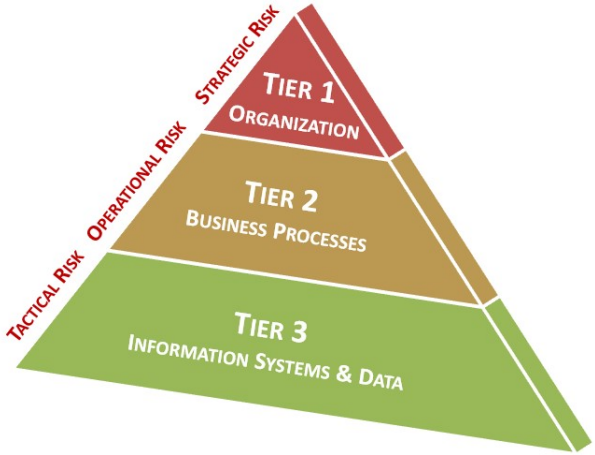


Figure 7. Multi-tiered cybersecurity & privacy risk model

[34] NIST SP 800-39 - https://csrc.nist.gov/publications/detail/sp/800-39/final

TIER 1: ORGANIZATION-LEVEL (STRATEGIC RISK CONSIDERATIONS)

Broadly address the "What and Why?" questions:

- What?
  - Statutory, regulatory and contractual obligations (e.g., European Union Data Protection Regulation (EU GDPR)).
- Why?
  - Corporate obligation to do what is expected; and
  - Avoid negative ramifications of non-compliance:
    - Breach of contract;
    - Fines; and
    - Criminal / civil actions.

TIER 2: BUSINESS PROCESS-LEVEL (OPERATIONAL RISK CONSIDERATIONS)

Assign governance and oversight to the "Who, How and When?" questions:

- Who?
  - Chief Privacy Officer (CPO);
  - Data Protection Officer (DPO); and
  - Chief Information Security Officer (CISO) and their respective team(s).
- How?
  - Resources for appropriate staffing and technology;
  - Senior leadership steering committees for company-wide buy-in for cybersecurity and privacy initiatives; and
  - Situational awareness through metrics reporting.
- When?
  - Timelines are established by multi-year, department-level business plans; and
  - Targeted maturity levels are identified and are supported by business planning timelines.

TIER 3: INFORMATION SYSTEM & DATA-LEVEL (TACTICAL RISK CONSIDERATIONS)

Address the specific details of "Who, How and When?" questions:

- Who?
  - Individuals / Teams / Groups (e.g., Security Operations Center (SOC), Information Risk Management (IRM), etc.)
- How?
  - Standardized Operating Procedures (SOPs)
- When?
  - In accordance with:
    - SOPs; and
    - Milestones established to meet the established, multi-year, department-level business plan.

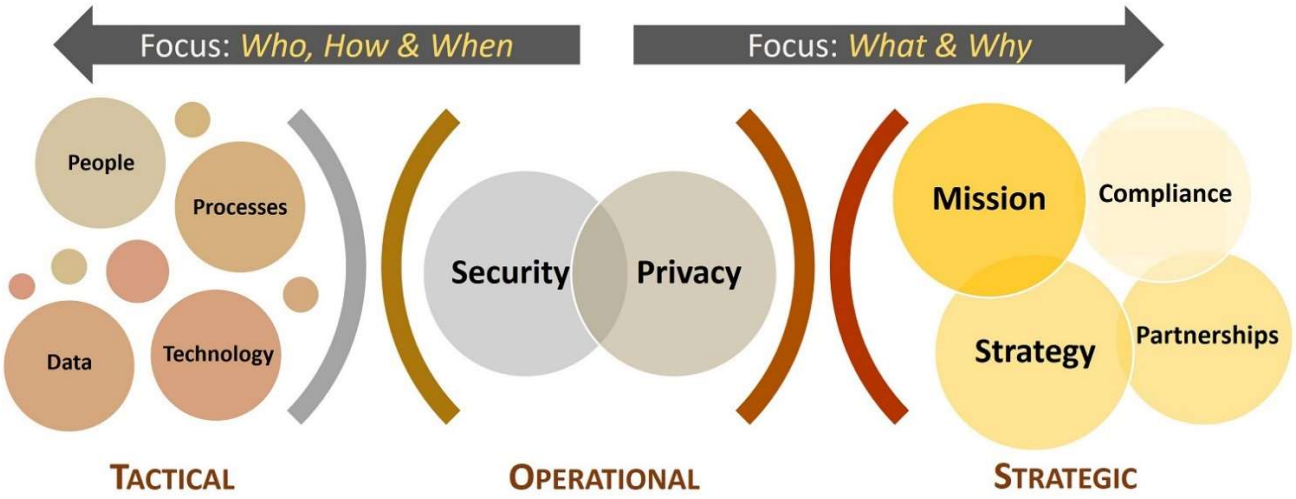


Figure 8. Who, What, When, Why & How Focus

SAMPLE

The Secure Controls Framework Privacy Management Principles (SCF PMP) provides a "Rosetta stone" approach to aligning with industry-recognized privacy practices.[35] ACME adopts the metaframework concept of the SCF PMP as a way to address applicable data protection requirements across multiple, disparate privacy laws, regulations and frameworks.

1.0 PRIVACY BY DESIGN.

Principle: Establish and maintain a comprehensive Data Privacy Program that ensures data protection considerations are addressed by design in the development of policies, standards, processes, systems, applications, projects and third-party contracts.

ACME-Specific Interpretation: The Data Privacy Program (DPP) serves as ACME's comprehensive Data Privacy Program. Leveraging the SCF PMP helps ACME ensures its applicable privacy considerations are addressed by design in the development of policies, standards, processes, systems, applications, projects and third-party contracts.

1.1 ASSIGNED RESPONSIBILITIES.

Principle: Assign accountability through documented roles and responsibilities to qualified personnel, including key internal and external stakeholders, for maintaining compliance with all applicable data protection requirements that involves appropriately monitoring and documenting the Data Privacy Program.

ACME-Specific Interpretation: The assignment of Data Privacy Program responsibilities is multifaceted:

- ACME's Human Resources (HR) department assigns qualified, screened data subjects to dedicated Data Privacy Program roles.
- The Chief Executive Officer (CEO) empowers the Chief Privacy Officer (CPO) to:
  - Staff the Data Privacy Program; and
  - Set organization-wide data protection requirements that are necessary to comply with applicable statutory, regulatory and/or contractual obligations.
- The CPO defines role-specific responsibilities for:
  - Personnel assigned to the Data Privacy Program;
  - Major stakeholders (e.g., CRO, CIO, CTO, CISO, etc.); and
  - Minor stakeholders (e.g., PMO and business process owners).

1.2 DATA CLASSIFICATION.

Principle: Classify data according to the sensitivity and type of PD / sPD, as defined by appropriate statutory, regulatory and contractual contexts.

ACME-Specific Interpretation: ACME's Data Classification & Handling Guidelines (Appendix A) is the authoritative source for ACME personnel to classify data according to the sensitivity and type of PD / sPD.

1.3 REGISTERING DATABASES.

Principle: Register applicable databases containing PD / sPD with the appropriate Data Authority, when required.

ACME-Specific Interpretation: The CPO, or a designated representative, will:

- Perform a legal review of the applicable statutory or regulatory requirement to register a ACME database containing PD / sPD.
- Document the results of the registration requirements review.
- Where technically feasible, register the database with a distribution list email so that appropriate personnel can be notified of any relevant information pertaining to the registered database.

1.4 RESOURCE PLANNING.

Principle: Identify and plan for resources needed to operate a Data Privacy Program and include data protection requirements in solicitations for technology solutions and services.

ACME-Specific Interpretation: The Chief Executive Officer (CEO):

- Provides adequate resources for ACME to operate a Data Privacy Program; and
- Empowers the Chief Privacy Officer (CPO) to embed data protection requirements for PD / sPD, regardless of where or how it is collected, created, used, disseminated, maintained, retained and/or disclosed, including third-parties.

[35] SCF Privacy Management Principles - https://www.securecontrolsframework.com/privacy-management-principles

EXAMPLE

1.5 Inventory of Personal Data.

Principle: Maintain an accurate inventory of:

- Types of PD / sPD;
- Specific data element(s); and
- Systems, applications and processes that collect, create, use, disseminate, maintain, and/or disclose that PD / sPD.

ACME-Specific Interpretation: The inventorying of PD / sPD is a multifaceted endeavor:

- The Data Privacy Program will maintain a Single Source of Truth (SSOT) for PD / sPD inventories that is either manual or automated.
- The Program Management Office (PMO) will use Data Protection Impact Assessments (DPIAs) as a project gate, where projects/initiatives are prohibited from being promoted into a production environment without a completed DPIA.
- DPOs will examine DPIAs to further the inventory of all instances where ACME is collecting, using, maintaining, or sharing PD / sPD, including:
    - Projects/initiatives;
    - Systems;
    - Applications;
    - Services; and
    - Third-parties.
- Where technically feasible, ACME will use an automated tool to scan structured and unstructured data sources for PD / sPD on a recurring basis.
- CPO, in conjunction with DPOs, will use this information collected from DPIAs to maintain an accurate inventory of:
    - Types of PD / sPD;
    - Specific data element(s); and
    - Systems, applications and processes that collect, create, use, disseminate, maintain, and/or disclose that PD / sPD.

1.6 Privacy Training.

Principle: Provide recurring data privacy awareness and training for all employees and contractors.

ACME-Specific Interpretation: The training of users on privacy-related matters requires coordination between the Data Privacy Program and HR:

- HR is required to identify roles that interact with PD / sPD:
    - New employees / contractors will be provided with data privacy-specific training as part of new hire orientation; and
    - Staffing changes that require data privacy-specific training will be managed to ensure training is conducted.
- The Data Privacy Program will develop and maintain data privacy-specific training material that is focused on:
    - New hires; and
    - Annual refresher training.
- HR will maintain evidence of employee training and share the results with the Data Privacy Program.
- The CPO will encourage Data Privacy Program staff to attain and maintain one, or more, of the following privacy-related certifications from the International Association of Privacy Professionals (IAPP):
    - Certified Information Privacy Manager (CIPM);
    - Certified Information Privacy Professional (CIPP); and/or
    - Certified Information Privacy Technologist (CIPT).

1.7 Personal Data Categories.

Principle: Define and implement data handling and protection requirements for specific categories of PD / sPD.

ACME-Specific Interpretation: For PD / sPD categories:

- CPO, in conjunction with DPOs, define data handling and protection requirements for each category of PD / sPD at ACME.
- BPOs, in conjunction with technology stakeholders, are required to configure applicable systems, applications and services to implement data handling and protection requirements each specific category of applicable PD / sPD.

1.8 Data Subject Communications.

Principle: Craft disclosures and communications to data subjects so the material is readily accessible and written in a manner that is concise, unambiguous and understandable by a reasonable person.

ACME-Specific Interpretation: BPOs, in conjunction with DPOs, are required to craft disclosures and communications to data subjects so that:

EXAMPLE

APPENDIX A: DATA CLASSIFICATION & HANDLING GUIDELINES

General data sensitivity guidelines include:

- Any information created or received by ACME employees in the performance of their jobs at is Internal Use, by default, unless the information requires greater confidentiality or is approved for release to the general public.
- Treat information that is not assigned a classification level as "Internal Use" at a minimum and use corresponding controls.
- When combining information with different sensitivity levels into a single application or database, assign the most restrictive classification of the combined asset. For example, if an application contains Internal Use and Confidential information, the entire application is Confidential.
- Restricted, Confidential and Internal Use information must never be released to the general public but may be shared with third-parties, such as government agencies, business partners or consultants, when there is a business need to do so and the appropriate security controls are in place according to the level of classification (e.g., Non-Disclosure Agreement).
- Personnel may not change the format or media of information if the new format or media used does not have the same level of security controls in place. For example, users may not export Restricted information from a secured database to an unprotected Microsoft Excel spreadsheet.
- Personal data (e.g., Personally Identifiable Information (PII), etc.) definitions widely vary. The applicable statutory, regulatory or contractual obligation will govern the specific definition of PD for a project.
- Information assets must be assigned a data 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 sensitivity level will take precedence. The sensitivity level then guides the selection of minimum protective measures to secure the information.

A-1: 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

Sensitive Personal Data (sPD)-Restricted

Personal Data (PD)-Restricted

Restricted

Confidential

Internal Use

Public

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 ACME. · Impact could include negatively affecting ACME's competitive position, violating statutory, regulatory and/or contractual requirements and damaging the company's reputation.

EXAMPLE

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 ACME. · Impact could include negatively affecting ACME'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 a data subject (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 ACME.** **· Impact could include negatively affecting ACME'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 ACME. · Impact could include negatively affecting ACME'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 ACME.
	Potential Impact of Loss	· **MODERATE DAMAGE** would occur if Confidential information were to become available to unauthorized parties either internal or external to ACME. · Impact could include negatively affecting ACME's competitive position, damaging the company's reputation and violating contractual requirements.
Internal Use	**Definition**	Internal Use information is information originated or owned by ACME 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 ACME. · 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.

APPENDIX B: DETERMINING MANDATORY AND DISCRETIONARY TECHNOLOGY CONTROLS

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).*

B-1: BASELINE SECURITY CATEGORIZATION – BASIC OR ENHANCED ASSURANCE

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.

Where the data sensitivity intersect with Safety & Criticality (SC) levels, it is 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. *It is important to note that SCs and data sensitivity ratings are independent characteristics.*

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 B-1. Asset categorization matrix.

BASIC ASSURANCE

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 data protection 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

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 data protection 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 ACME; and
- Stakeholders perform a greater role in maintaining situational awareness to ensure controls are properly executed and governed.

B-2: DETERMINING MANDATORY AND DISCRETIONARY TECHNOLOGY CONTROLS

What sets the Basic and Enhanced requirements apart comes down to the technology controls in place, where Enhanced will have more protection in place than Basic. The expectation is that Basic contains "reasonably-expected protections" that would withstand scrutiny by an outside auditor or regulator, based on following industry-recognized practices to design, build and maintain secure systems, applications and services. In terms of "basic security," this consists of having antimalware protections, protecting sensitive data, maintain systems and reviewing security logs (see the chart below for more details).

TECHNOLOGY CONTROLS BY ASSURANCE LEVEL

When it is necessary to increase security requirements, additional controls will be needed. These Discretionary controls go above and beyond Mandatory controls to meet specific data protection needs that would withstand scrutiny by an outside auditor or regulator (see the chart below for specific examples of enhanced controls). The assignment of Enhanced controls is often required to meet a statutory, regulatory or contractual obligation (e.g., PCI DSS, EU GDPR, NIST SP 800-171, etc.).

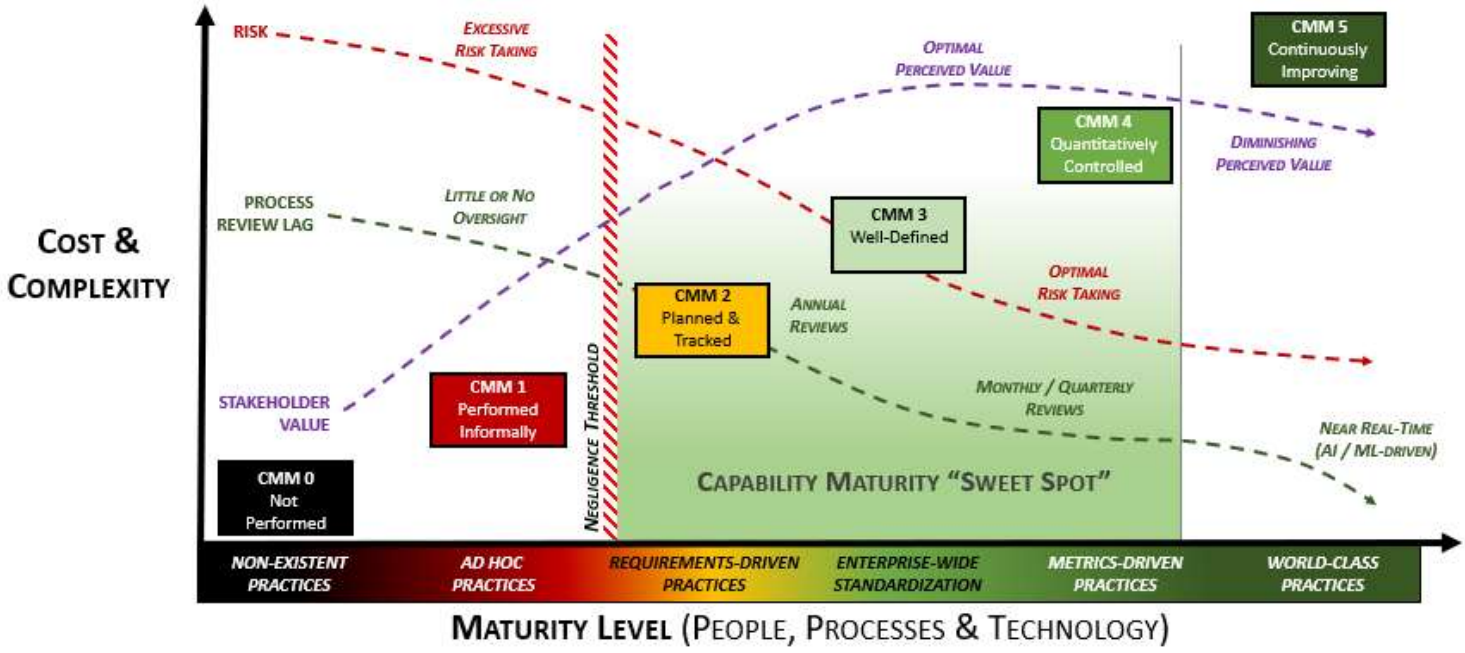
EXAMPLE

APPENDIX C: CAPABILITY MATURITY MODEL (CMM) DEFINITIONS

The six (6) Security & Privacy Capability Maturity Model (SP-CMM) levels are:

- CMM 0 – Not Performed
- CMM 1 – Performed Informally
- CMM 2 – Planned & Tracked
- CMM 3 – Well-Defined
- CMM 4 – Quantitatively Controlled
- CMM 5 – Continuously Improving

For most organizations, the "sweet spot" for maturity targets is between CMM 2 and 4 levels. ACME's Data Privacy Program strives for a baseline CMM3, but may dictate certain functions require a higher level of maturity, based on specific risks.



Negligence Considerations

Without the ability to demonstrate evidence of both due care and due diligence, an organization may be found negligent. In practical terms, the "negligence threshold" is between CMM 1 and CMM 2. The reason for this is at CMM 2, practices are formalized to the point that documented evidence exists to demonstrate reasonable steps were taken to operate a control.

Risk Considerations

Risk associated with the control in question decreases with maturity, but noticeable risk reductions are harder to attain above CMM 3. Oversight and process automation can decrease risk, but generally not as noticeably as steps taken to attain CMM 3.

Process Review Lag Considerations

Process improvements increase with maturity, based on shorter review cycles and increased process oversight. What might have been an annual review cycle to evaluate and tweak a process can be near real-time with Artificial Intelligence (AI) and Machine Learning (ML).

Stakeholder Value Considerations

The perceived value of security controls increases with maturity. However, perceived value tends to decrease after CMM 3 since the value of the additional cost and complexity becomes harder to justify to business stakeholders. Companies that are genuinely focused on being industry leaders are ideal candidates for CMM 5 targets to support their aggressive business model needs.

EXAMPLE

SUMMARY OF CCM VS ORGANIZATION SIZE CONSIDERATIONS

The following table summarizes the high-level expectations for small/medium/large organizations to meet each level of maturity.

Maturity Level	Small Organizations	Medium Organizations	Large Organizations
SP-CMM 0	▪ Lack of processes would be considered negligent behavior. This is generally due to a lack of a cybersecurity and data privacy. ▪ [NEGLIGENT]		It is unlikely for a large organization to completely ignore cybersecurity and data protection requirements.
SP-CMM 1	▪ IT support focuses on reactionary "break / fix" activities and are ad hoc in nature. ▪ IT support is likely outsourced with a limited support contract. ▪ [LIKELY NEGLIGENT]	▪ Internal IT staff exists, but there is no management support to spend time or budget on cybersecurity / data protection controls that leads to ad hoc control implementation. ▪ Focus is on general IT operations without clear standards that implement secure systems and processes. ▪ [LIKELY NEGLIGENT]	
SP-CMM 2	▪ Internal IT role(s) has clear requirements and is supported to meet applicable cybersecurity / privacy compliance obligations; or ▪ The outsourced IT provider is properly scoped in its support contract to address applicable compliance obligations.	▪ IT staff have clear requirements to meet applicable compliance obligations. ▪ There is most likely a dedicated cybersecurity role or a small cybersecurity team.	
SP-CMM 3	▪ There is a small IT staff that has clear requirements to meet applicable compliance obligations. ▪ There is likely a very competent leader (e.g., security manager / director) with solid cybersecurity experience who has the authority to direct resources to enact secure practices across the organization.	▪ IT staff have clear requirements to meet applicable compliance obligations. ▪ In addition to the existence of a dedicated cybersecurity team, there are specialists (e.g., engineers, SOC analysts, GRC analysts, privacy, etc.). ▪ There is a very competent leader (e.g., CISO) with solid cybersecurity experience who has the authority to direct resources to enact secure practices across the organization.	
SP-CMM 4	It is unrealistic for a small organization to attain this level of maturity.	▪ IT staff have clear requirements to meet applicable compliance obligations. ▪ In addition to the existence of a dedicated cybersecurity team, there are specialists (e.g., engineers, SOC analysts, GRC analysts, privacy, etc.). ▪ There is a very competent leader (e.g., CISO) with solid cybersecurity experience who has the authority to direct resources to enact secure practices across the organization. ▪ Business stakeholders are made aware of the status of the cybersecurity and data privacy (e.g., quarterly business reviews to the CIO/CEO/board of directors). Situational awareness is made possible through detailed metrics.	
SP-CMM 5	It is unrealistic for a small or medium organization to attain this level of maturity.		▪ IT staff have clear requirements to meet applicable compliance obligations. ▪ In addition to the existence of a dedicated cybersecurity team, there are specialists (e.g., engineers, SOC analysts, GRC analysts, privacy, etc.). ▪ There is a very competent leader (e.g., CISO) with solid cybersecurity experience who has the authority to direct resources to enact secure practices across the organization. ▪ Business stakeholders are made aware of the status of the cybersecurity and data privacy (e.g., quarterly business reviews to the CIO/CEO/board of directors). Situational awareness is made possible through detailed metrics. ▪ The organization has a very aggressive business model that requires not only IT, but its cybersecurity and privacy practices, to be innovative to the point of leading the industry in how its products and services are designed, built or delivered. ▪ The organization invests heavily into developing AI/ML technologies to made near real-time process improvements to support the goal of being an industry leader.

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)

ACRONYMS

AD. Active Directory
APT. Advanced Persistent Threat
BCP. Business Continuity Plan
BPO. Business Process Owner
CEO. Chief Executive Officer
CERT. Computer Emergency Response Team
CIO. Chief Information Officer
CIRT. Computer Incident Response Team
CISO. Chief Information Security Officer
CM. Change Management
COE. Center of Excellence
COOP. Continuity of Operations Plan
CPO. Chief Privacy Officer
CRO. Chief Risk Officer
C-SCRM. Cybersecurity Supply Chain Risk Management
CTI. Controlled Technical Information [38]
CUI. Controlled Unclassified Information [39]
DAC. Discretionary Access Control
DISA. Defense Information Security Agency
DLP. Data Loss Prevention
DPIA. Data Protection Impact Assessment
DPP. Data Privacy Program
DRP. Disaster Recovery Plan
DSR. Discretionary Security Requirements
EAP. Extensible Authentication Protocol
EPHI. Electronic Protected Health Information
FIM. File Integrity Monitor
GDPR. General Data Protection Regulation
HIPAA. Health Insurance Portability and Accountability Act
IAM. Identity and Access Management
IAP. Information Assurance Program
IRP. Incident Response Plan
ISIRT. Integrated Security Incident Response Team
ISMS. Information Security Management System
ISO. International Organization for Standardization
ITAM. Information Technology Asset Management
KSA. Knowledge, Skills and Abilities
LOB. Line of Business
MCC. Minimum Compliance Criteria
MDM. Mobile Device Management
NIST. National Institute of Standards and Technology
PbD. Privacy by Design
PD / sPD. Personal Data / sensitive Personal Data
PDCA. Plan-Do-Check-Act
PM. Project Management
PMO. Program Management Office
RBAC. Role-Based Access Control
RMP. Risk Management Program
RoPA. Record of Processing Activities
SbD. Security by Design
SCF PMP. Secure Controls Framework Privacy Management Principles
SCRM. Supply Chain Risk Management
SDLC. System Development Lifecycle
SME. Subject Matter Expert
SOP. Standard Operating Procedures
SSDP. Secure Software Development Practices
SSOT. Single Source of Truth

DEFINITIONS

ACME recognizes two sources for authoritative definitions:

- The National Institute of Standards and Technology (NIST) IR 7298, *Glossary of Key Cybersecurity Terms*, is the approved reference document used to define common digital security terms;[40] and
- NIST Glossary.[41]

Security Requirements and Controls

The term control can be applied to a variety of contexts and can serve multiple purposes. When used in the security context, a security control can be a mechanism (e.g., a safeguard or countermeasure) designed to address protection needs that are specified by a set of security requirements.

- Controls are defined as the power to make decisions about how something is managed or how something is done; the ability to direct the actions of someone or something; an action, method or law that limits; or a device or mechanism used to regulate or guide the operation of a machine, apparatus or system.
- Requirements are defined as statements that translate or express a need and its associated constraints and conditions.[42]

[38] CUI Registry - https://www.archives.gov/cui/registry/category-detail/controlled-technical-info.html
[39] CUI Registry - https://www.archives.gov/cui/registry/category-list
[40] NIST IR 7298 - https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.7298r3.pdf
[41] NIST Glossary - https://csrc.nist.gov/glossary
[42] ISO/IEC/IEEE 29148

EXAMPLE