Your Logo
Will Be
Placed Here

SECURITY & PRIVACY BY DESIGN

ACME Business Consulting, Inc.

SPBD
Security & Privacy By Design

INTERNAL USE
Access Limited to Internal Use Only

NOTICE

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 security and privacy concepts being incorporated in all stages of the system development lifecycle. The following external content is referenced by or supports this Security & Privacy By Design (SPBD) document:

- The National Institute of Standards and Technology (**NIST**): [1]
  - NIST 800-37: *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*
  - NIST 800-39: *Managing Information Security Risk: Organization, Mission and Information System View*
  - NIST 800-53: *Security and Privacy Controls for Federal Information Systems and Organizations*
  - NIST 800-64: *Security Considerations in System Development Lifecycle*
  - NIST 800-122: *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*
  - NIST 800-160: *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*
  - NIST 800-161: *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*
  - NIST 800-171: *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*
  - NIST IR 7298: *Glossary of Key Information Security Terms*
  - NIST IR 8062: *An Introduction to Privacy Engineering and Risk Management in Federal Systems*
  - NIST IR 8179: *Criticality Analysis Process Model: Prioritizing Systems and Components* [draft]
  - NIST *Framework for Improving Critical Cybersecurity* (Cybersecurity Framework)
- The 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 Information Security Controls*
  - ISO 27018: *Information Technology -- Security Techniques -- Code of Practice for Protection of Personally Identifiable Information (PII) in Public Clouds Acting as PII Processors*
- Organization for the Advancement of Structured Information Standards (**OASIS**): [3]
  - OASIS *Privacy Management Reference Model and Methodology (PMRM)*
- Open Web Application Security Project (**OWASP**)[4]
  - OWASP Top 10 Most Critical Web Application Security Risks
  - OWASP Application Security Verification Standard Project (ASVS)
- Other Frameworks:
  - Cloud Security Alliance Cloud Controls Matrix (**CSA CCM**)[5]
  - Center for Internet Security (**CIS**)[6]
  - Department of Defense Information Security Agency (**DISA**) Secure Technology Implementation Guides (**STIGs**)[7]
  - Generally Accepted Privacy Practices (**GAPP**)[8]
  - Fair Information Practice Principles (**FIPP**)[9]
  - AuditScripts. *Open Threat Taxonomy*[10]
  - European Union Regulation 2016/279 (General Data Protection Regulation (**EU GDPR**))[11]
  - Payment Card Industry Data Security Standard (**PCI DSS**)[12]

[1] National Institute of Standards and Technology - http://csrc.nist.gov/publications/PubsSPs.html
[2] International Organization for Standardization - https://www.iso.org
[3] Privacy Management Reference Model and Methodology (PMRM) Version 1.0. 26 March 2012. OASIS Committee Specification Draft 01. http://docs.oasisopen.org/pmrm/PMRM/v1.0/csd01/PMRM-v1.0-csd01.html.
[4] Open Web Application Security Project - https://www.owasp.org/index.php/Main_Page
[5] Cloud Security Alliance - https://cloudsecurityalliance.org/
[6] Center for Internet Security - https://www.cisecurity.org/
[7] DoD Information Security Agency - http://iase.disa.mil/stigs/Pages/index.aspx
[8] The American Institute of CPAs - http://www.aicpa.org
[9] Federal Trade Commission - https://www.ftc.gov
[10] Open Threat Taxonomy - http://www.auditscripts.com/resources/open_threat_taxonomy_v1.1a.pdf
[11] EU General Data Protection Regulation - http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf
[12] Payment Card Industry Security Standards Council - https://www.pcisecuritystandards.org/

TABLE OF CONTENTS

EXECUTIVE SUMMARY

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 we are entrusted with. The Security & Privacy By Design (SPBD) document:

- Focuses on putting security and privacy principles into practice;
- Supports ACME's existing requirements (e.g., policies and standards); and
- Is intended to influence the development of procedures at the department and team levels.

WHAT DOES IT MEAN TO PERFORM SECURITY AND PRIVACY BY DESIGN?

Implementing both Security by Design (SbD) and Privacy by Design (PbD) principles is a systematic way to find and address weaknesses, flaws and risks to ACME. It is focused on helping us:

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

WHY DO WE NEED SECURITY AND PRIVACY BY DESIGN?

ACME wants to develop quality systems, applications and processes. We are entrusted with the security and privacy of information on behalf of employees and customers. Additionally, the constantly evolving statutory and regulatory landscapes now require that ACME implement both security and privacy by design. This is primarily driven by the following:

- European Union General Data Protection Regulation (EU GDPR)[13]; and
- Payment Card Industry Data Security Standard (PCI DSS).[14]

HOW TO USE THIS DOCUMENT

The SPBD is a two-part document:

- Word Document - This is the core document that provides program-level guidance on implementing both security and privacy by design; and
- Excel Spreadsheet -This is a multi-tabbed spreadsheet that contains checklists to enable a "paint by numbers" approach to conducting both security and privacy assessments.

It is recommended to begin with reviewing the table of contents of this document to understand the overall scope of the material contained in the SPBD and then read through the document. Take your time to understand the terminology as it applies to security and privacy management. Please note there are references at the end of the document to help with acronyms. When you finish reading this document, you should understand what actions are needed from you and your team to support ACME's objectives to implement both security and privacy by design.

Thoroughly review this document at least once a year, since change is a constant and changes will impact how security and privacy are managed at ACME. Stakeholders in the program, like yourself, can continually improve this program by revisiting topics, discussing protection measures, and updating the program.

TARGET AUDIENCE

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

- Security 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.

[13] European Union. http://ec.europa.eu/justice/data-protection/index_en.htm
[14] Payment Card Industry Security Standards Council. https://www.pcisecuritystandards.org

HOLISTIC APPROACH TO EMBEDDING SECURITY & PRIVACY PRACTICES INTO OPERATIONS

ACME Business Consulting, Inc. (ACME) is committed to protecting its employees, partners, clients and ACME from damaging acts that are intentional or unintentional. Effective security and privacy is a team effort involving the participation and support of every ACME user who interacts with data and systems. Therefore, it is the responsibility of every user to understand security and privacy principles and to conduct their activities accordingly.

ACME's endorses a moderate risk appetite for matters related to new projects or significant change to current operations. The risks and rewards of such opportunities are to be weighed by ACME against both short and long term strategic and operational priorities, as well as ACME's financial position. However, ACME endorses a low risk appetite for matters relating to:

- Security; and
- Privacy.

There are a number of specific risks for which ACME has zero tolerance, and those risks will be considered totally unacceptable. These are outlined below:

- Any action that causes, or may cause, imminent and serious risk to the health and safety of a person that could result in serious injuries to staff, contractors, or customers;
- Any deliberate violation of an applicable statutory, regulatory or regulatory requirement; and
- Any actions that cause, or may cause, imminent and serious risk to the reputation, viability or long-term profitability of ACME.

DATA-CENTRIC APPROACH: CONFIDENTIALITY, INTEGRITY, AVAILABILITY & SAFETY (CIAS) BY DESIGN

A data-centric approach refers to a mindset that recognizes data as a central and permanent asset, where applications and services are transitory, with finite lifecycles. In simple terms, applications and services come and go, but data remains.

Since every application is developed to use a specific data model, it is extremely difficult to change the data model of an implemented application system due to code dependencies. In Data Centric Architecture (DCA), the data model must precede the implementation of an application or service so that the data model drives system development and not the inverse. Data Centric Security (DCS) recognizes that privacy is an essential element in the protection of data.

The Security & Privacy By Design (SPBD) document provides prescribed measures used to design, implement and maintain systems, applications and processes at ACME. The main objective of SPBD is to implement security and privacy principles to reduce both the likelihood and impact of possible incidents that affect the confidentiality, integrity, availability or safety of the solution.

Security and privacy are a byproduct of Confidentiality, Integrity, Availability and Safety (CIAS) measures:

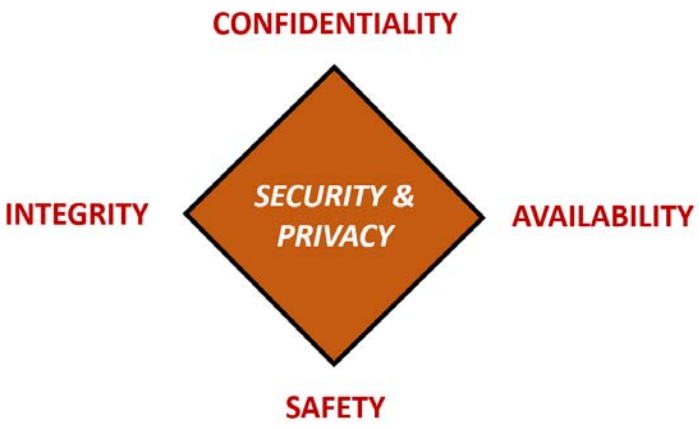


Figure 1. CIAS model.

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

Commensurate with risk, CIAS measures must be implemented to guard against unauthorized access to, alteration, disclosure or destruction of data and systems. This also includes protection against accidental loss or destruction, regardless of what state data is in.

Data can be viewed as being in only one (1) of the following states at any given time:

- Data is at rest;
- Data is being processed; or
- Data is being transmitted.

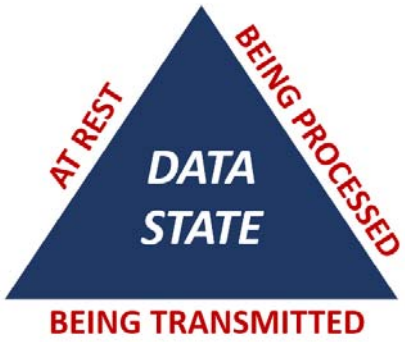


Figure 2. Data states.

MASTERING THE FUNDAMENTALS: BUILDING BLOCK APPROACH TO SECURITY & PRIVACY

Building an organization that routinely incorporates security and privacy practices into daily operations requires a mastery of the fundamentals of both security and privacy principles.

A useful analogy is with the children's' toy, LEGO®. With LEGO® you can build nearly anything you want—either through following directions or using your own creativity. However, it first requires an understanding of how various LEGO® shapes either snap together or are incompatible.

- Once you master the fundamentals with LEGO®, it is easy to keep building and become immensely creative since you know how everything interacts. However, when the fundamentals are ignored, the LEGO® structure will be weak and include systemic flaws.
- Security and privacy really are not much different, since those disciplines are made up of numerous building blocks that all come together to build secure systems and processes. The lack of critical building blocks will lead to insecure and poorly architected solutions.
- When envisioned that each component that make up a security or privacy "best practice" is a LEGO® block, it is possible to visualize how certain requirements are the foundation that form the basis for others components to attach to. Only when the all the building blocks come together and take shape do you get a functional security / privacy program.

ENGINEERING FOR SUCCESS

ACME encourages its employees not to focus on what is likely to happen, but instead, to focus on what can happen so that ACME is prepared. Fundamentally, that is what systems security engineering means, since it embraces proactive planning and design to:

- Prevent the loss of an asset that ACME is not willing to accept;
- Be in a position to minimize the consequences should such a loss occur; and
- Be in an informed position to reactively recover from the loss when it does happen.

Engineering for success necessitates appropriate protection capabilities.

PROTECTION CAPABILITIES

A protection capability represents the "many things that come together" in a planned manner to produce the emergent system security property. Similar to the LEGO® analogy listed above, protections must fit together properly in order to ensure the protections operate as intended. There are two (2) forms of protection capability:

- Active Protection
  - Active protection includes security functions of the system that have functional and performance attributes.
  - Examples include: antimalware, Intrusion Prevention Systems (IPS), Network Access Control (NAC), etc.
- Passive Protection
  - Passive protection includes architecture, design, and the rules that govern behavior, interaction, and utilization.
  - Examples include: end user awareness training, personnel background screening, logon banners, etc.

IMPLEMENT A CULTURE OF SECURITY & PRIVACY

Within an organization, a "security culture" is a pattern of behaviors, beliefs, assumptions, attitudes and ways of doing things.[15] Regardless of the size or industry, a security culture exists in every organization and it is comprised of a pattern of behaviors, beliefs, assumptions, attitudes and ways of doing things that constitute a corporate culture. The same holds true for the concept of a privacy culture.

At ACME, it is management's intent to have a strong and proactive culture of security, since ACME wants to reduce both risk and operational expenses that are attributed to weak security practices. This security culture forms the foundation for secure engineering, privacy and vendor management.

BUILDING FOR SECURITY & PRIVACY

As ACME's SPBD program matures, it will become increasingly efficient and streamlined. Correspondingly, the quantity and severity of discovered vulnerabilities, deficiencies and incidents should decrease. Essentially, the overall resiliency of ACME's technology infrastructure is strengthened by a mature SPBD.

At the heart of the matter, SPBD assists in eliminating assumptions across the lifecycle of projects, programs and general operations. The SPBD addresses the "Who, What, When, Why & How" that is necessary to ensure successful tactical, operational and strategic goals are accomplished.

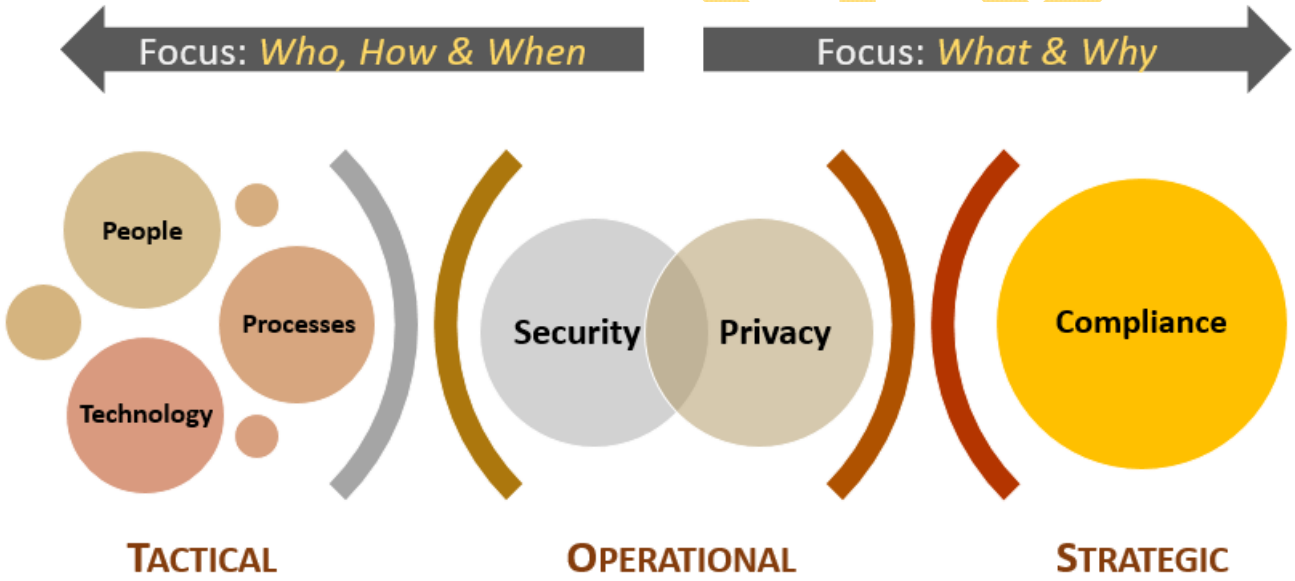


Figure 6. Overview of focus at the tactical, operational and strategic levels.

STRATEGIC 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.

[15] ISACA, The Business Model for Information Security (BMIS), USA, 2010

Operational Considerations

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

- Who?
  - Data Protection Officer (DPO) and their respective team(s); 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 security and privacy initiatives; and
  - Situational awareness through Key Performance Indicator (KPI) 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.

Tactical 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.

Cybersecurity For Privacy by Design (C4P)

Surprising to many people, privacy protections overlay most existing security protection mechanisms. In a Cybersecurity For Privacy by Design (C4P) model, focuses on People, Processes and Technology (PPT) to:

- Enable privacy;
- Preset security configuration settings so that they are secure by default;
- "Bakes in" security mechanisms, as compared to "bolting on" protections as an afterthought;
- Value keeping things simple to save resources and avoid negatively affecting users;
- Integrate throughout the lifecycle of projects / applications / systems.
- Support a common method to "trust but verify" projects / applications / systems.
- Set security up to be seen as an enabler through educating users, managing expectations, and supporting change.

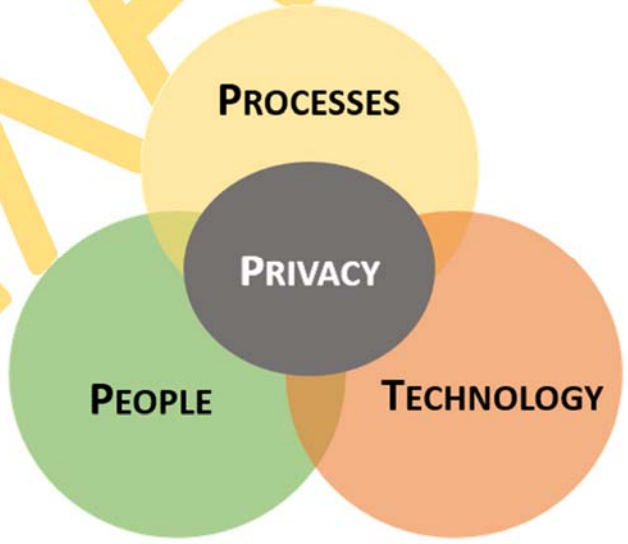
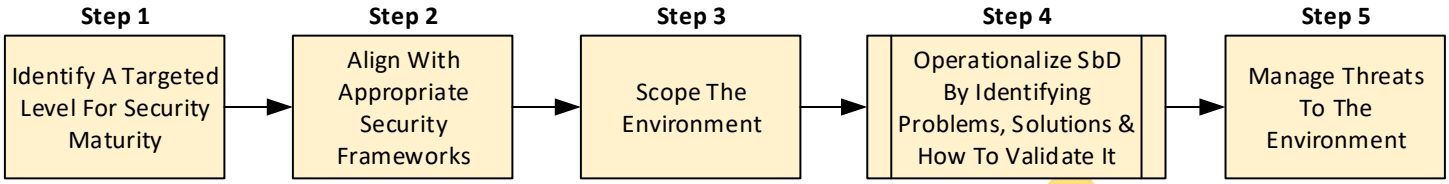


Figure 7. People, Processes & Technology (PPT)

OPERATIONALIZING SECURITY BY DESIGN (O-SBD)

ACME's Security by Design (SbD) principles can be implemented in a five (5) step process that is applicable to any project or initiative:

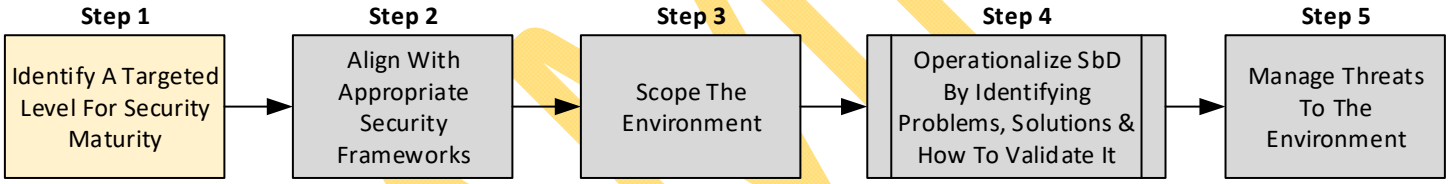


Security design principles and concepts serve as the foundation for engineering trustworthy secure systems, including their constituent subsystems and components. The principles and concepts are intended to be universally applicable across this broad range of systems, as well as new systems as they emerge and mature.

Systems security engineering ultimately performs security analyses with the appropriate fidelity and rigor to produce the evidence to substantiate claims that the system is adequately secure. The evidence spans the entire system life cycle and for all system life cycle concepts in terms of the following three roles:

- Engineering the security functions that provide system security capability;
- Engineering the security-driven constraints for all system functions; and
- Engineering and advising for the protection of data, information, technology, methods, and assets associated with the system throughout its life cycle.

STEP 1: IDENTIFY A SECURITY MATURITY MODEL (SMM) TARGET STATE



Since every organization is unique in its compliance requirements and available resources to address those needs, it is important to identify a target level of maturity that makes sense for ACME. The NIST Cybersecurity Framework's Security Maturity Model (SMM) [17] and it incorporates five (5) distinct maturity levels.

As part of ACME's multi-year strategy to reduce cybersecurity-related risk, the target is to achieve at least a Tier 3 (Repeatable) maturity level.

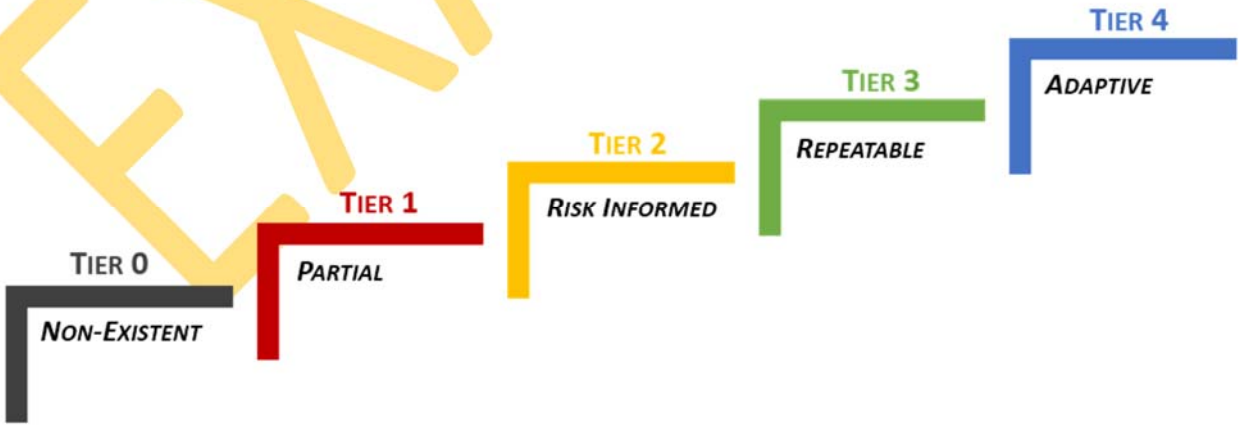


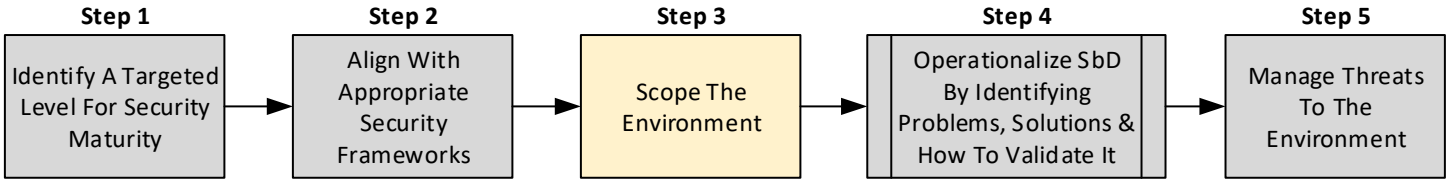
Figure 10. Security maturity levels.

SMM TIER 0: NON-EXISTENT

- Risk Management Process

[17] National Institute of Standards and Technology (NIST) *Framework for Improving Critical Cybersecurity* (Cybersecurity Framework)

STEP 3: DETERMINE APPROPRIATE SCOPING



From a secure engineering and architecture perspective, leveraging practices from NIST 800-160, it is worthwhile to take a zone-based approach to scoping an environment for secure systems engineering. This effort is meant to focus on particular systems of interest, while taking into account the systems elements and enabling systems that compose the system of interest.

System elements of other systems may place constraints on the system of interest and, therefore ACME must be cognizant of other impacting systems, regardless of the primary focus on the system of interest. Figure 11 illustrates the systems engineering view of the system of interest.

Assets can be logically grouped into three (3) overlapping zones:

- Zone 1 – The asset is a system of interest;
- Zone 2 – The asset exists within the immediate operating environment of a system of interest; or
- Zone 3 – The asset exists outside of the operating environment but influences the system of interest.

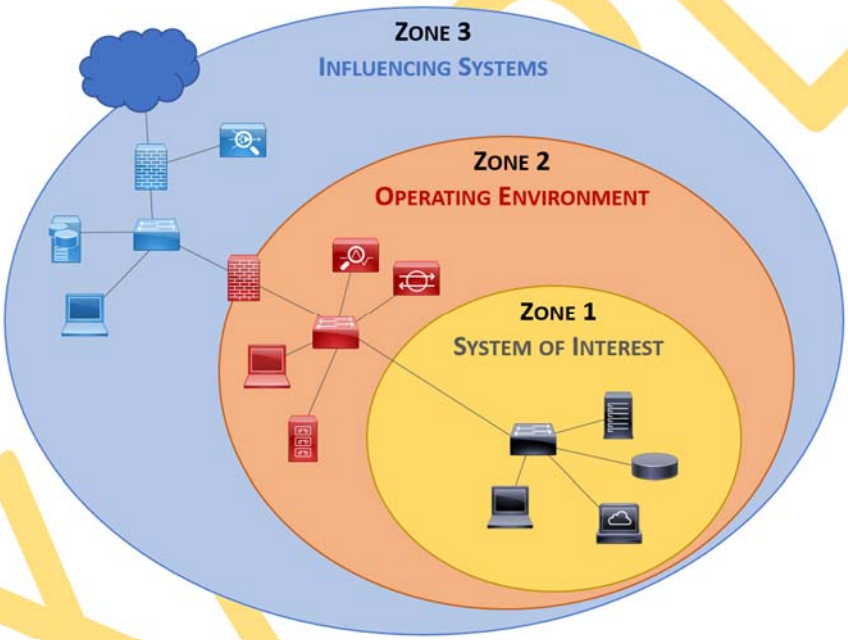


Figure 11. Zone-based approach to determining scoping efforts.

ZONE 1: SYSTEMS OF INTEREST

Zone 1 only contains systems of interest.

- Systems of Interest
  - These are systems that are the focus of the systems engineering effort.
- Examples include:
  - Project initiative
  - Product offering
  - Service offering

ZONE 2: OPERATING ENVIRONMENT

Zone 2 is the operating environment for the systems of interest. In addition to containing the systems of interest, it contains Systems and System Elements:

- Systems
  - Combination of interacting elements organized to achieve one or more stated purposes.
  - Examples include:
    - Active Directory (AD) (directory services)
    - Shared computing resources and network infrastructure

PHASE 2: IDENTIFY THE SOLUTION

The solution context transforms the stakeholder security requirements into design requirements for the system; addresses all security architecture, design, and related aspects necessary to realize a system that satisfies those requirements; and produces sufficient evidence to demonstrate that those requirements have been satisfied. The solution context is based on a balanced proactive and reactive system security protection strategy that exercises control over events, conditions, asset loss, and the consequence of asset loss to the degree possible, practicable, and acceptable to stakeholders. The solution context includes:

- Defining the security aspects of the solution;
- Realizing the security aspects of the solution; and
- Producing evidence for the security aspects of the solution.

Reference Appendix E for details on steps to take during this phase. This is part of the **Architectural Definition Process (AR)** for selecting candidate architecture (Step # 2-52).

LAYERED DEFENSES APPROACH TO IDENTIFYING SOLUTIONS

SbD solutions should rely on layered defenses to help address both technical and non-technical weaknesses that exist in any project or initiative:

- Technical
  - Lack of security hardening (e.g., unnecessary services running, missing patches, etc.);
  - Incorrectly configured systems (e.g., access permissions, password policy, user rights, encryption, etc.); and
  - Lack of situational awareness (e.g., centralized log reviews, alert notifications, etc.).
- Non-Technical
  - Weak physical access control to buildings or areas housing key IT infrastructure;
  - Untrained or poorly trained IT / cybersecurity personnel; and
  - Lack of formalized program documentation.

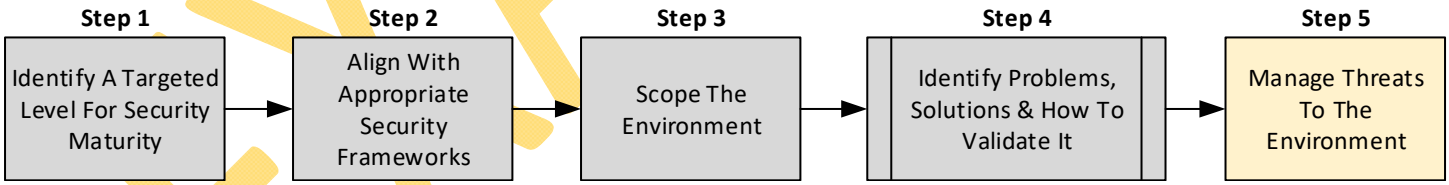
PHASE 3: ENSURE TRUSTWORTHINESS

The trustworthiness context is a decision-making context that provides an evidence-based demonstration, through reasoning, that the system-of-interest is deemed trustworthy based upon a set of claims derived from security objectives. The trustworthiness context consists of:

- Developing and maintaining the assurance case; and
- Demonstrating that the assurance case is satisfied.

Reference Appendix E for details on steps to take during this phase. This is part of the **Verification Process (VE)** for preparing for the security aspects of verification (Step # 4-1).

STEP 5: MANAGE THREATS TO THE ENVIRONMENT THROUGH THREAT MODELING



When assessing threats, there are a number of different components to consider, including:

- Threat sources or agents;
- Threat actions;
- Threat targets;
- Threat consequences; and
- Available countermeasures to reduce risk.

A threat source will most often perform a threat action against a threat target, which leads to threat consequences.

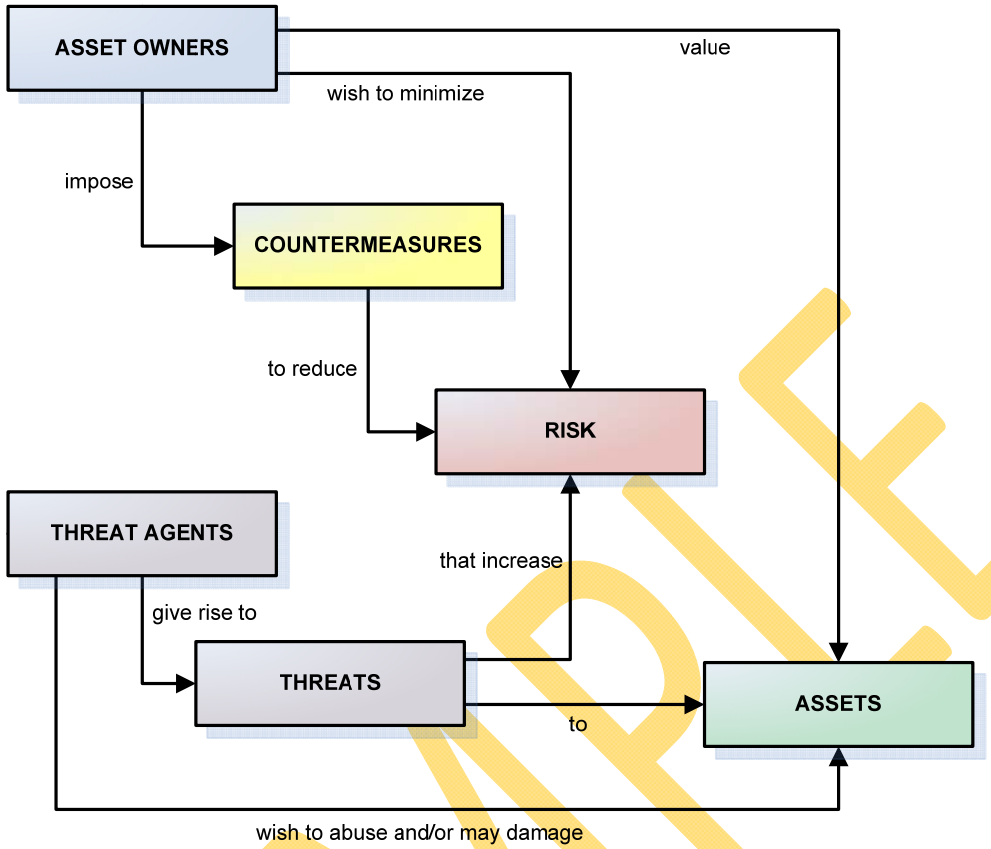


Figure 13. Threat management model.

DEFINING THREATS TO THE ENVIRONMENT

To aide in defining threats, ACME uses the to Open Threat Taxonomy (OTT) provide a baseline of reasonable threats to information systems. [19] The OTT is comprised of four (4) categories of threats, which includes:

- Physical Threats
- Resource Threats
- Personnel Threats
- Technical Threats

PHYSICAL THREATS

- This includes threats to the confidentiality, integrity, or availability of information systems that are physical in nature.
- These threats generally describe actions that could lead to the theft, harm, or destruction of information systems.

RESOURCE THREATS

- This includes threats to the confidentiality, integrity, or availability of information systems that are the result of a lack of resources required by the information system.
- These threats often cause failures of information systems through a disruption of resources required for operations.

PERSONNEL THREATS

- This includes threats to the confidentiality, integrity, or availability of information systems that are the result of failures or actions performed by an organization's personnel.
- These threats can be the result of deliberate or accidental actions that cause harm to information systems.

[19] Open Threat Taxonomy - http://www.auditscripts.com/resources/open_threat_taxonomy_v1.1a.pdf

OPERATIONALIZING PRIVACY BY DESIGN (O-PBD)

Breaches involving Personal Information (PI) are hazardous to both individuals and ACME. Harm to individuals may include identity theft, embarrassment, or blackmail. Harm to ACME may include a loss of public trust, legal liability, and remediation costs. To appropriately protect the confidentiality of PI, ACME uses a risk-based approach to guide protection requirements.

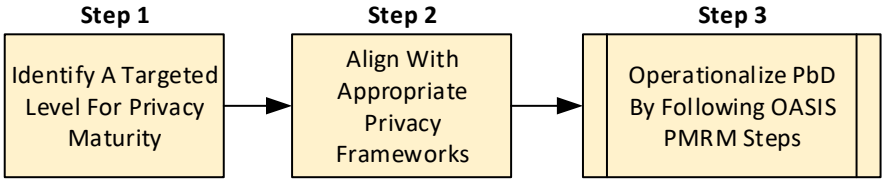
ACME cannot properly protect PI it does not know about. This document uses a broad definition of PI to identify as many potential sources of PI as possible (e.g., databases, shared network drives, backup tapes, contractor sites). PI is any information about an individual maintained by ACME including any information that:

- Can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and
- Is linked or linkable to an individual, such as medical, educational, financial, and employment information.

Examples of PI include, but are not limited to:

- Name
  - Full name;
  - Maiden name;
  - Mother's maiden name; and
  - Alias(es);
- Personal Identification Numbers
  - Social Security Number (SSN);
  - Passport number;
  - Driver's license number;
  - Taxpayer Identification Number (TIN), and
  - Financial account or credit card number;
- Address Information
  - Home address; and
  - Personal email address;
- Personal Characteristics
  - Photographic image (especially of the face or other identifying characteristics, such as scars or tattoos);
  - Fingerprints;
  - Handwriting, and
  - Other biometric data:
    - Retina scan;
    - Voice signature; and
    - Facial geometry; and
- Linkable Information
  - Date of birth;
  - Place of birth
  - Race;
  - Religion;
  - Weight;
  - Social / recreational activities or hobbies;
  - Geographical indicators (e.g., geolocation information);
  - Employment information;
  - Medical information;
  - Education information; and
  - Financial information.

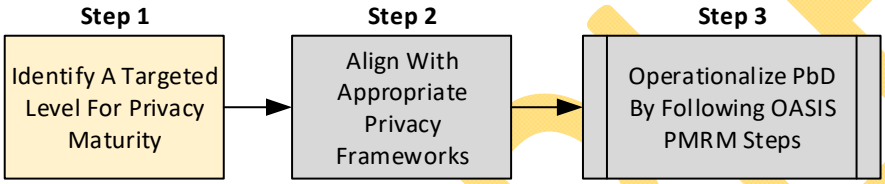
ACME's Privacy by Design (PbD) principles can be implemented in a three (3) step process that is applicable to any project or initiative:



From an operational perspective, privacy management equates to the assured, proper, and consistent collection, processing, communication, use and disposition of personal information (PI) throughout its lifecycle. Privacy management must:

- Be properly and consistently applied throughout the PI lifecycle;
- Apply to all actors who have a connection with the information; and
- Apply to all systems/networks and jurisdictions where PI information is exposed.

STEP 1: IDENTIFY A PRIVACY MATURITY MODEL (PMM) TARGET STATE



Similar to right-sizing mechanisms to align with a targeted security maturity state, it is crucial for ACME to identify its targeted maturity state for its privacy program. The AICPA / CISA Privacy Maturity Model (PMM) [21] is based on the Generally Accepted Privacy Principles (GAPP) and supports ACME's alignment with GAPP.

There are six (6) distinct maturity levels and as part of ACME's multi-year strategy to reduce privacy-related risk, the target is to achieve at least a Tier 4 (Managed) maturity level.

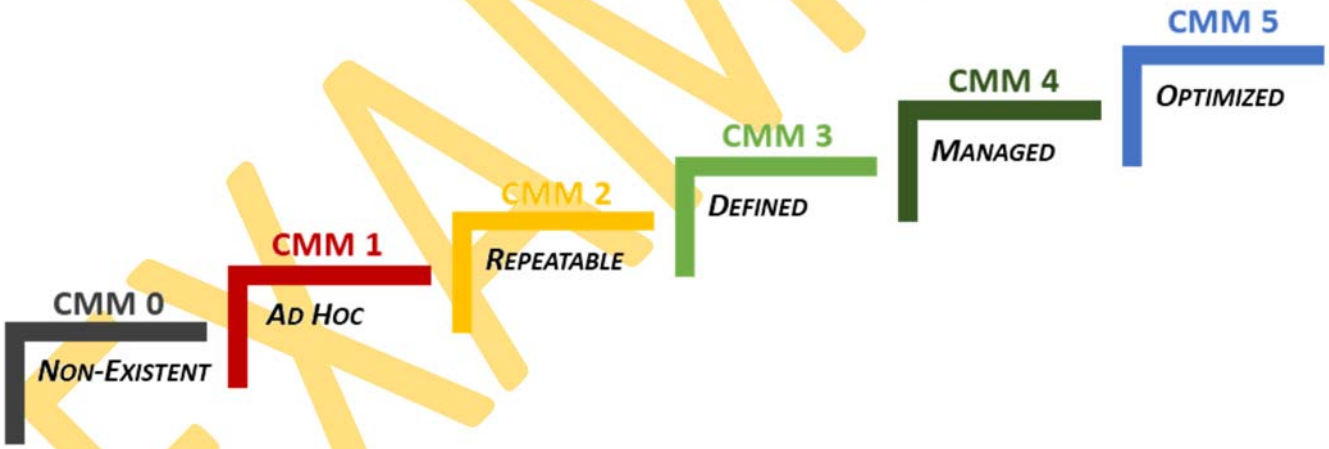


Figure 15. Privacy maturity levels.

PMM TIER 0: NON-EXISTENT

Procedures or processes do not exist.

PMM TIER 1: AD HOC

Procedures or processes are generally informal, incomplete, and inconsistently applied.

PMM TIER 2: REPEATABLE

Procedures or processes exist; however, they are not fully documented and do not cover all relevant aspects.

PMM TIER 3: DEFINED

Procedures and processes are fully documented and implemented, and cover all relevant aspects.

[21] AICPA / CICA Privacy Maturity Model (PMM). March 2011

APPENDICES

APPENDIX A – DATA CLASSIFICATION & HANDLING GUIDELINES

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 four sensitivity levels:

Classification	Data Classification Description	
Restricted	**Definition**	Restricted information is highly valuable, highly sensitive business information, and the level of protection is dictated externally by legal and/or contractual requirements. Restricted information must be limited to 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, violating contractual requirements, and exposing the geographic location of individuals.
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.
	Potential Impact of Loss	· **NO DAMAGE** would occur if Public information were to become available to parties either internal or external to ACME. · Impact would not be damaging or a risk to business operations.

Figure A-1. Data Classification Matrix

Where the data sensitivity and SC levels meet 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.

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

Figure B-1. Asset Categorization Risk Matrix

B-3: Basic Assurance Requirements

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

B-4: Enhanced Assurance Requirements

- The minimum level of controls is defined as exceeding industry-recognized leading practices (e.g., specialized hardening requirements, DLP, FIM, DAM, etc.).
- For security controls in Enhanced Assurance projects, it is essentially the Basic Assurance level that is expanded to require more robust IT security capabilities that are commensurate with the value of the project to ACME.

APPENDIX E – ALIGNING SECURITY & PRIVACY PRINCIPLES WITH THE RISK MANAGEMENT FRAMEWORK (RMF)

The SPBD's corresponding Excel spreadsheet, Tab "Checklist 1 – Security," creates a "paint by numbers" approach to implementing the following SbD principles, where security engineering processes are overlaid onto the RMF phases.

The first step is to identify if the project / initiative should have a BASIC or ENHANCED baseline set of controls. This can be determined by referencing Appendix B for guidance.

PHASE 1: CATEGORIZE INFORMATION SYSTEMS

This phase focuses on categorizing the information systems and the information processed, stored, and transmitted by those systems based on an impact analysis. The pertinent control families from NIST 800-160 include: [25]

- Business or Mission Analysis Process (BA)
- Stakeholder Needs and Requirements Definition Process (SN)

PHASE 2: SELECT SECURITY CONTROLS

This phase focuses on selecting an initial set of baseline security controls for the information systems based on the security categorization step. Tailoring and supplementing the initial security control baseline will occur as needed, based on follow-on assessments of risk and local conditions. The pertinent control families from NIST 800-160 include: [26]

- System Analysis Process (SA)
- System Requirements Definition Process (SR)
- Architecture Definition Process (AR)
- Design Definition Process (DE)

PHASE 3: IMPLEMENT SECURITY CONTROLS

This phase focuses on implementing the security controls and describe how the controls are employed within information systems and the operating environment. The pertinent control families from NIST 800-160 include: [27]

- Implementation Process (IP)
- Integration Process (IN)

PHASE 4: ASSESS SECURITY CONTROLS

This phase focuses on assessing the security controls using appropriate assessment procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for systems. The pertinent control families from NIST 800-160 include: [28]

- Verification Process (VE)
- Transition Process (TR)

PHASE 5: AUTHORIZE INFORMATION SYSTEMS

This phase focuses on authorizing information system operations based on a determination of the risk to organizational operations and assets, individuals, other organizations, resulting from the operation of the information systems and the decision that this risk is acceptable. The pertinent control families from NIST 800-160 include: [29]

- Validation Process (VA)

PHASE 6: MONITOR SECURITY CONTROLS

This phase focuses on monitoring the security controls on an ongoing basis, including assessing control effectiveness, documenting changes to systems or its operating environment, conducting security impact analyses of the associated changes, and reporting the security state to designated organizational officials. The pertinent control families from NIST 800-160 include: [30]

- Operation Process (OP)
- Maintenance Process (MA)
- Disposal Process (DS)

[25] NIST 800-160 - http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160.pdf
[26] NIST 800-160 - http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160.pdf
[27] NIST 800-160 - http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160.pdf
[28] NIST 800-160 - http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160.pdf
[29] NIST 800-160 - http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160.pdf
[30] NIST 800-160 - http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160.pdf

APPENDIX G – OASIS PRIVACY MANAGEMENT REFERENCE MODEL & METHODOLOGY (PMRM) – CHECKLIST

The power and the value of the OASIS Privacy Management Reference Model and Methodology (PMRM) to each stakeholder, whether privacy officer, business owner, developer, regulator, or data subject, lies in executing a series of specific tasks that move from initially establishing high-level descriptions (and boundaries) of a particular use case, to exposing greater levels of specificity, including personal information, data flows, domains and domain owners, privacy controls and their supporting services, functionality, and mechanisms. The PMRM incorporates iterative risk analysis that focuses on the expected and actual operation of the functionality put in place to make privacy delivery a reality. The outcome of this final step is a Privacy Management Analysis (PMA) that links together the policies, personal information, controls, and procedural and technical service delivery functionality.

G-1: APPLICATION & BUSINESS PROCESS DESCRIPTIONS (PHASE 1)

Phase 1 contains the following tasks:

- Task 1: Use Case Description
- Task 2: Use Case Inventory
- Task 3: Privacy Policy Conformance Criteria
- Task 4: Assessment Preparation

Task #	Privacy Management Task	Privacy Task Objective	Context
1	Use Case Description	Provide a general description of the use case.	The first step in applying the **OASIS Privacy Management Reference Model and Methodology (PMRM)** requires the scoping of the application(s) or business service(s) in which Personal Information (PI) is associated. The intent is to identify the complete environment where privacy and data protection requirements are applicable.
2	Use Case Inventory	Provide an inventory of the capabilities, applications and policy environment under review at the level of granularity appropriate for the analysis covered by the PMRM and define a high-level use case which will guide subsequent analysis.	The inventory can include applications and business processes; products; policy environment; legal and regulatory jurisdictions; systems supporting the capabilities and applications; data; time; and other factors Impacting the collection, communication, processing, storage and disposition of PI. The inventory should also include the types of data subjects covered by the use case together with individual user privacy options (such as policy preferences, privacy settings, etc. if these are formally expressed). In order to facilitate the analysis described in the Detailed Privacy use case Analysis, the components of the use case Inventory should align as closely as possible with the components that will be analyzed in the corresponding detailed use case analysis.

APPENDIX I – TECHNICAL MANAGEMENT PROCESSES

This section contains the eight ISO/IEC/IEEE 15288 "technical management processes" with extensions for systems security engineering. The processes are:

- Project Planning (PL);
- Project Assessment and Control (PA);
- Decision Management (DM);
- Risk Management (RM);
- Configuration Management (CM);
- Information Management (IM);
- Measurement (MS); and
- Quality Assurance (QA).

I-1: PROJECT PLANNING (PL)

The purpose of the Project Planning process is to produce and coordinate effective and workable plans. [37]

Anticipated Security Engineering Outcomes:

- Security objectives and the security aspects of project plans are defined.
- Systems security engineering roles, responsibilities, accountabilities, and authorities are defined.
- Resources and services necessary to achieve the security objectives of the project are formally requested and committed.
- Plans for the execution of the security aspects of the project are activated.

I-2: PROJECT ASSESSMENT AND CONTROL (PA)

The purpose of the Project Assessment and Control process is to assess if the plans are aligned and feasible; determine the status of the project, technical and process performance; and direct execution to help ensure that the performance is according to plans and schedules, within projected budgets, to satisfy technical objectives. [38]

Anticipated Security Engineering Outcomes:

- The security aspects of performance measures or assessment results are available.
- The adequacy of security-relevant roles, responsibilities, accountabilities, and authorities is assessed.
- The adequacy of resources allocated to the security aspects of the project is assessed.
- The security aspects of technical progress reviews are performed.
- Deviations in the security aspects of project performance from plans are investigated and analyzed.
- Lessons learned are recorded to help inform and guide future projects and activities within projects.
- Affected stakeholders are informed of the security aspects of project status.
- Corrective action is defined and directed, when the security aspects of project achievement are not meeting targets.
- The security aspects of project re-planning are initiated, as necessary.
- The security aspects of project action to progress (or not) from one scheduled milestone or event to the next is authorized.
- Project security objectives are achieved.

I-3: DECISION MANAGEMENT (DM)

The purpose of the Decision Management process is to provide a structured, analytical framework for objectively identifying, characterizing and evaluating a set of alternatives for a decision at any point in the life cycle and select the most beneficial course of action. [39]

Anticipated Security Engineering Outcomes:

- The security aspects of the decision management strategy are established.
- The security aspects of decisions requiring alternative analysis are identified.
- Security-based decisions requiring alternative analysis are identified.
- The security aspects of alternative courses of action are identified and evaluated.
- A preferred course of action informed by or driven by security considerations is selected.
- The security aspects of a resolution, of the decision rationale, and of the assumptions are identified.

[37] Definition from ISO/IEC/IEEE 15288-2015 via NIST 800-160.
[38] Definition from ISO/IEC/IEEE 15288-2015 via NIST 800-160.
[39] Definition from ISO/IEC/IEEE 15288-2015 via NIST 800-160.

APPENDIX L – EU GENERAL DATA PROTECTION REGULATION (GDPR) CONSIDERATIONS

Within the European Union Regulation 2016/279 (General Data Protection Regulation (**EU GDPR**)), Articles 5, 25 and 35 have shared responsibilities between cybersecurity and privacy teams. [61]

L-1: SECURITY BY DESIGN (SBD) FOR EU GDPR

The following sections are the key articles from the EU GDPR that pertain to cybersecurity:

- Article 5 - Principles relating to processing of personal data
  - ACME must protect personal data in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.
- Article 25 – Data protection by design and by default
  - ACME must implement "appropriate technical and organizational measures" to implement data-protection principles and ensure that, by default, only personal data which are necessary for each specific purpose of the processing are processed.
- Article 28 - Processor:
  - ACME must only use processors providing sufficient guarantees to implement appropriate technical and organizational security and privacy measures.
- Article 32 - Security of processing:
  - ACME must implement “appropriate technical and organizational measures” to ensure a level of security appropriate to the risk of data being processed.
- Article 33 - Notification of a personal data breach to the supervisory authority:
  - Without undue delay and, where feasible, not later than 72 hours after having become aware of it, ACME must notify the personal data breach to the supervisory authority
- Article 35 - Data protection impact assessment:
  - In an effort to assess the impact of envisioned processing operations, ACME must perform a Data Protection Impact Assessment (DPIA) prior to the processing of data.
- Article 45 - Transfers on the basis of an adequacy decision:
  - ACME must limit the transfer of personal data to third countries or international organizations that the Commission has decided ensures an adequate level of protection.
- Article 46 - Transfers subject to appropriate safeguards
  - In the absence of a decision for Article 45, ACME must have at least one (1) of the following in place:
    - A legally binding and enforceable instrument between public authorities or bodies;
    - Binding corporate rules in accordance with Article 47;
    - Standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2);
    - Standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 93(2);
    - An approved code of conduct pursuant to Article 40 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or
    - An approved certification mechanism pursuant to Article 42 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.

In terms of the EU GDPR, the company defines “adequate level of data protection” and “appropriate technical or organizational measures” in terms of its alignment with leading security practices. Therefore, ACME adopts a “best in class” approach to implementing security frameworks, since each has its own unique strengths and weaknesses:

- International Organization for Standardization (ISO) 27000-series guidance;
- National Institute of Standards and Technology (NIST) 800-series guidance;
- NIST Cybersecurity Framework;
- Open Web Application Security Project (OWASP) Application Security Verification Standard (ASVS);
- Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM);
- Center for Internet Security (CIS) configuration benchmarks; and
- Department of Defense Information Security Agency (DISA) Secure Technology Implementation Guides (STIGs).

[61] EU General Data Protection Regulation - http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf