Your Logo
Will Be
Placed Here

SECURITY & PRIVACY BY DESIGN

ACME Business Consulting, LLC

SPBD
Security & Privacy By Design

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 cybersecurity 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:

- National Institute of Standards and Technology (**NIST**): [1]
    - NIST 800-37: *Guide for Applying the Risk Management Framework to Federal Information Systems*
    - NIST 800-39: *Managing Cybersecurity 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 800-128: *Guide for Security-Focused Configuration Management of Information Systems*
    - NIST 800-160: *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 8062: *An Introduction to Privacy Engineering and Risk Management in Federal Systems*
    - NIST IR 8179: *Criticality Analysis Process Model: Prioritizing Systems and Components* [draft]
    - NIST *Framework for Improving Critical Cybersecurity* (Cybersecurity Framework)
- International Organization for Standardization (**ISO**):[2]
    - ISO 15288: *Systems and Software Engineering -- System Life Cycle Processes*
    - ISO 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 Privacy Management Principles
- Organization for the Advancement of Structured Information Standards (**OASIS**): [4]
    - OASIS *Privacy Management Reference Model and Methodology (PMRM)*
- Open Web Application Security Project (**OWASP**)[5]
    - 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**)[6]
    - Center for Internet Security (**CIS**)[7]
    - Department of Defense Cybersecurity Agency (**DISA**) Secure Technology Implementation Guides (**STIGs**)[8]
    - Generally Accepted Privacy Practices (**GAPP**)[9]
    - Fair Information Practice Principles (**FIPP**)[10]
    - Privacy by Design (**PbD**) [11]
    - AuditScripts. *Open Threat Taxonomy*[12]
    - European Union Regulation 2016/279 (General Data Protection Regulation (**EU GDPR**))[13]
    - Payment Card Industry Data Security Standard (**PCI DSS**)[14]

[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] Open Web Application Security Project - https://www.owasp.org/index.php/Main_Page
[6] Cloud Security Alliance - https://cloudsecurityalliance.org/
[7] Center for Internet Security - https://www.cisecurity.org/
[8] DoD Information Security Agency - http://iase.disa.mil/stigs/Pages/index.aspx
[9] The American Institute of CPAs - http://www.aicpa.org
[10] Federal Trade Commission - https://www.ftc.gov
[11] Term and principles coined by Dr. Ann Cavoukian - https://www.owasp.org/index.php/Privacy_by_Design
[12] Open Threat Taxonomy - http://www.auditscripts.com/resources/open_threat_taxonomy_v1.1a.pdf
[13] EU General Data Protection Regulation - http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf
[14] Payment Card Industry Security Standards Council - https://www.pcisecuritystandards.org/

Table of Contents

Notice 2

Referenced Frameworks & Supporting Practices 2

Executive Summary 9

What Does It Mean To Perform Security and Privacy by Design? 9

Why Do We Need Security and Privacy by Design? 9

How To Use this Document 9

Target audience 10

Holistic Approach To Embedding Security & Privacy Practices Into Operations 11

Data-Centric Approach: Confidentiality, Integrity, Availability & Safety (CIAS) by Design 11

Mastering The Fundamentals: Building Block Approach To Security & Privacy 12

Secure Engineering for Success 12

Enterprise-Wide Scope: Holistic Coverage From Development To Production Environments 13

Utilize Linkages: Common Touch Points For Designing & Implementing Security & Privacy Principles 14

Leveraging The Risk Management Framework (RMF) To Organize Security & Privacy Tasks 14

Maintain A Fixed Target: Defining Security & Privacy Protection Needs 15

Understanding Protection Needs 16

Expected Controls For Security & Privacy 16

Implement A Culture of Security & Privacy 17

Building For Security & Privacy 17

Multi-Tiered Security & Privacy Risk Model 18

Tier 1: Organization-Level (Strategic Risk Considerations) 18

Tier 2: Business Process-Level (Operational Risk Considerations) 18

Tier 3: Information System & Data-Level (Tactical Risk Considerations) 19

Cybersecurity For Privacy by Design (C4P) 19

People 19

Process 19

Technology 21

Data Centric Security (DCS) Approach To Layered Defenses 21

Hierarchical Approach To Building A Security Culture 22

Security Culture-Enabling Processes (NIST 800-160) 22

Technical Management Processes 22

Secure Engineering Processes 23

Third-Party Management Processes 23

Operationalizing Security By Design 24

Understanding Security by Design (SbD) 24

Step 1: Align With Leading Security Frameworks 24

Step 2: Identify A Security & Privacy Capability Maturity Model (SP-CMM) Target State 25

Step 3: Determine Appropriate Scoping for Security Controls 25

Zone 1: Systems of Interest 26

Zone 2: Operating Environment 26

Zone 3: Influencing Systems 27

Step 4: Operationalize Security by Design (SbD) Principles 27

Step 5: Manage Threats To The Environment Through Threat Modeling 28

Defining Threats To The Environment 28

Threat Modeling Tool 29

STRIDE Model 29

Operationalizing Privacy By Design 31

Understanding Privacy by Design (PbD) 31

Step 1: Align With Leading Privacy Frameworks 32

Privacy Management Principles 32

Step 2: Identify A Security & Privacy Capability Maturity Model (SP-CMM) Target State 33

Step 3: Determine Appropriate Scoping for Privacy Controls 33

Phase 1: Application & Business Process Descriptions 34

Phase 2: Detailed Privacy Use Case Analysis 34

Phase 3: Services Supporting Privacy Controls 34

Step 4: Operationalize PbD Principles 34

Phase 2: Detailed Privacy Use Case Analysis 34

Step 5: Manage Changes To PD & Its Processing Environment 35

Phase 3: Services Supporting Privacy Controls 35

Appendices 36

Appendix A: Data Classification & Handling Guidelines 36

A-1: Data Classification 36

A-2: Determining the Safety & Criticality Rating 37

A-3: Defining Personal Data 38

Appendix B: Determining Mandatory and Discretionary Technology Controls 40

B-1: Baseline Security Categorization – Basic or Enhanced Assurance 40

B-2: Determining Mandatory and Discretionary Technology Controls 40

Appendix C: Safety Considerations With Embedded Technology 42

C-1: Mission Critical (SC-1) 42

C-2: Business Critical (SC-2) 42

C-3: Non-Critical (SC-3) 42

Appendix D: Secure Engineering Roles & Responsibilities 43

D-1: Cybersecurity Role Categories 43

D-2: Cybersecurity Specialty Areas (Roles) 44

D-3: Cybersecurity Work Roles & Responsibilities 47

Appendix E: Security & Privacy Capability Maturity Model (SP-CMM) 52

E-1: SP-CMM Overview 52

E-2: SP-CMM Categories 52

E-3: Summary of CCM vs Organization Size Considerations 55

E-4: Defining A Capability Maturity Target 56

Appendix F: EU General Data Protection Regulation (GDPR) Considerations 57

F-1: Security by Design (SbD) for EU GDPR 57

F-2: Privacy by Design (PbD) for EU GDPR 58

Glossary: Acronyms & Definitions 59

Acronyms 59

Definitions 59

Record of Changes 60

Annex 1: Risk Management Framework (RMF) – Secure Development Lifecycle (SDL) Tasks 61

RMF Phase 1 - Prepare 61

P-1: Risk Management Roles 61

P-2: Risk Management Strategy 62

P-3: Risk Assessment (Organization-Level) 62

P-4: Control Baselines & Cybersecurity Framework Profiles (Organization-Level) 63

P-5: Common Control Identification 63

P-6: Impact Level Prioritization 64

P-7: Continuous Monitoring Strategy (Organization-Level) 65

P-8: Mission or Business Focus 65

P-9: System Stakeholders 66

P-10: Asset Identification 66

P-11: Authorization Boundary 68

P-12: Information Types 68

P-13: Information Life Cycle 68

P-14: Risk Assessment (System) 69

P-15: Security & Privacy Requirements 70

P-16: Enterprise Architecture 71

P-17: Requirements Allocation 71

P-18: System Registration 72

RMF Phase 2- Categorize 72

C-1: System Description 72

C-2: Security Categorization 73

C-3: Security Categorization Review & Approval 73

RMF Phase 3 - Select 74

S-1: Control Selection *74*
S-2: Control Tailoring *74*
S-3: Control Allocation *75*
S-4: Documentation of Planned Control Implementations *77*
S-5: Continuous Monitoring Strategy (System) *77*
S-6: Plan Review & Approval *78*
RMF Phase 4 - Implement **78**
I-1: Control Implementation *78*
I-2: Update Control Implementation Information *79*
RMF Phase 5 - Assess **79**
A-1: Assessor Selection *79*
A-2: Assessment Plan *80*
A-3: Control Assessments *81*
A-4: Assessment Reports *82*
A-5: Remediation Actions *82*
A-6: Plan of Action & Milestones (POA&M) *83*
RMF Phase 6 - Authorize **84**
R-1: Authorization Package *84*
R-2: Risk Analysis & Determination *85*
R-3: Risk Response *85*
R-4: Authorization Decision *86*
R-5: Authorization Reporting *87*
RMF Phase 7 - Monitor **87**
M-1: System & Environment Changes *87*
M-2: Ongoing Assessments *88*
M-3: Ongoing Risk Response *89*
M-4: Authorization Package Updates *89*
M-5: Security & Privacy Reporting *90*
M-6: Ongoing Authorization *91*
M-7: System Disposal *91*

Annex 2: Security & Privacy by Design (S|P) Principles **92**
1. Security & Privacy Governance **92**
2. Asset Management **92**
3. Business Continuity & Disaster Recovery **92**
4. Capacity & Performance Planning **92**
5. Change Management **92**
6. Cloud Security **92**
7. Compliance **92**
8. Configuration Management **92**
9. Continuous Monitoring **92**
10. Cryptographic Protections **93**
11. Data Classification & Handling **93**
12. Embedded Technology **93**
13. Endpoint Security **93**
14. Human Resources Security **93**
15. Identification & Authentication **93**
16. Incident Response **93**
17. Information Assurance **93**
18. Maintenance **93**
19. Mobile Device Management **93**
20. Network Security **93**
21. Physical & Environmental Security **93**
22. Privacy **93**
23. Project & Resource Management **93**
24. Risk Management **94**
25. Secure Engineering & Architecture **94**
26. Security Operations **94**
27. Security Awareness & Training **94**

28. Technology Development & Acquisition 94
29. Third-Party Management 94
30. Threat Management 94
31. Vulnerability & Patch Management 94
32. Web Security 94

Annex 3: Privacy Management Principles 95
1.0 Privacy by Design. 95
1.1 Assigned Responsibilities. 95
1.2 Data Classification. 95
1.3 Registering Databases. 95
1.4 Resource Planning. 95
1.5 Inventory of PD. 95
1.6 Privacy Training. 95
2.0 Data Subject Participation. 95
2.1 Clear Choices. 95
2.2 Initial Consent. 95
2.3 Updated Consent. 95
2.4 Equal Service & Price. 96
2.5 Prohibit The Sale of Personal Data. 96
3.0 Limited Collection & Use. 96
3.1 Authority to Collect. 96
3.2 Data Minimization. 96
3.3 Internal Use. 96
4.0 Transparency. 96
4.1 Notice & Purpose Specification. 96
5.0 Data Lifecycle Management. 96
5.1 Processing Records. 96
5.2 Data Flow Mapping. 96
5.3 Data Custodians. 96
5.4 Retention of Personal Data. 97
5.5 Secure Destruction of Personal Data. 97
5.6 Geolocation Restrictions. 97
5.7 Data Portability. 97
5.8 Record of Disclosures. 97
5.9 Integrity Protections. 97
5.10 De-Identification . 97
5.11 Quality Management. 97
5.12 Secure Data Processing. 97
5.13 Data Lineage. 97
5.14 Updated Use Permissions. 97
5.15 Flaw Remediation with Personal Data. 97
5.16 Analytical Biases. 97
6.0 Data Subject Rights. 97
6.1 Inquiry Management. 97
6.2 Updating Personal Data. 98
6.3 Redress. 98
6.4 Notice of Correction or Amendment. 98
6.5 Appeal. 98
6.6 Right to Erasure. 98
7.0 Security by Design. 98
7.1 Cybersecurity Considerations. 98
7.2 Cryptographic Protections. 98
7.3 Physical Protections. 98
7.4 Embedded Technology. 98
7.5 Retire Outdated Systems. 98
7.6 Personnel Security. 98
7.7 Rules of Behavior. 98
7.8 Employee Sanctions. 98

7.9 Workforce Management. *98*

7.10 Professional Competency. *99*

8.0 Incident Response. **100**

8.1 Coordinated Response. *100*

8.2 Breach Notification. *100*

9.0 Risk Management. **100**

9.1 Evaluate Risks. *100*

9.2 Assess Supply Chain Risk. *100*

9.3 Risk Awareness. *100*

9.4 Risk Response. *100*

9.5 Data Protection Impact Assessment (DPIA). *100*

10.0 Third-Party Management. **100**

10.1 Supply Chain Protections. *100*

10.2 Secure Disclosure To Third-Parties. *100*

10.3 Contractual Obligations for Third-Parties. *100*

10.4 Third-Party Compliance. *100*

11.0 Business Environment. **101**

11.1 Privacy Protections Context. *101*

11.2 Policies, Standards & Procedures. *101*

11.3 Periodic Review. *101*

11.4 Oversight. *101*

11.5 Management Visibility. *101*

11.6 Compliance. *101*

11.7 Critical Business Functions. *101*

Annex 4: Cybersecurity & Privacy Control Selection – Minimum Security Requirements (MSR) **102**

Step 1: Download The Latest Version of the Secure Controls Framework (SCF) **102**

Step 2: Identify All Applicable Requirements **102**

Step 3: Filter Out Non-Applicable Requirements **102**

Step 4: Assign Controls To Stakeholders **103**

Annex 5: NIST 800-160 Secure Engineering Framework (SEF) **104**

Secure Engineering Framework (SEF) **104**

Phase 1: Identify The Problem *105*

Phase 2: Identify The Solution *105*

Phase 3: Ensure Trustworthiness *105*

Security Culture Enabling Processes **106**

Life Cycle Model Management (LM) *106*

Infrastructure Management (IF) *106*

Portfolio Management (PM) *106*

Human Resource Management (HR) *106*

Quality Management (QM) *107*

Knowledge Management (KM) *107*

Technical Management Processes **107**

Project Planning (PL) *107*

Project Assessment and Control (PA) *107*

Decision Management (DM) *108*

Risk Management (RM) *108*

Configuration Management (CM) *108*

Information Management (IM) *108*

Measurement (MS) *109*

Quality Assurance (QA) *109*

Security-Enabling Processes **109**

Business or Mission Analysis Process (BA) *109*

Stakeholder Needs and Requirements Definition Process (SN) *110*

System Requirements Definition Process (SR) *110*

System Analysis Process (SA) *110*

Architecture Definition Process (AR) *111*

Design Definition Process (DE) *111*

Implementation Process (IP) *111*

Integration Process (IN) 111
Verification Process (VE) 112
Transition Process (TR) 112
Validation Process (VA) 112
Operation Process (OP) 113
Maintenance Process (MA) 113
Disposal Process (DS) 113
Third-Party Management Processes **113**
Acquisition (AQ) 113
Supply Process (SP) 114

Annex 6: OASIS Privacy Management Reference Model & Methodology (PMRM) – Privacy Services **115**

Core Policy Services **115**
Agreement Service 115
Usage Service 115
Privacy Assurance Services **116**
Validation Service 116
Certification Service 116
Enforcement Service 116
Security Service 116
Presentation and Lifecycle Services **116**
Interaction Service 116
Access Service 116
OASIS PMRM Tasks by Phase **117**
Application & Business Process Descriptions (Phase 1) 117
Detailed Privacy Use Case Analysis (Phase 2) 118
Services Supporting Privacy Controls (Phase 3) 120

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.

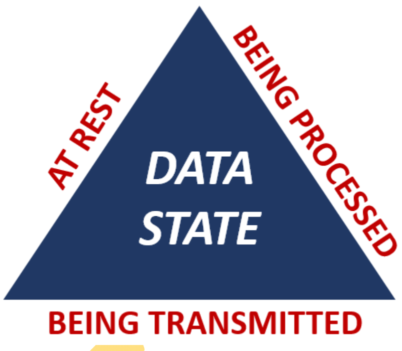


Figure 2. Data states.

Mastering The Fundamentals: Building Block Approach To Security & Privacy

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

Secure 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 secure 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.

Secure engineering 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.

Utilize Linkages: Common Touch Points For Designing & Implementing Security & Privacy Principles

All too often, when projects are commenced, involvement from key stakeholders is siloed, as compared to operating as a cohesive team. Specific to cybersecurity and privacy, ACME wants to avoid the following pitfalls:

- Project / application teams work in a vacuum, unaware of cybersecurity or privacy concerns;
- Privacy and security conduct their own assessments without any information sharing or collaboration; and
- Security involvement is viewed as a final hurdle to overcome, just prior to "go live" for the project.

As shown below, numerous touch points exist between security, privacy and the project teams throughout the lifecycle of a system, application or product. See Appendix E for more specific details on common security & privacy linkages that exist in the project lifecycle.

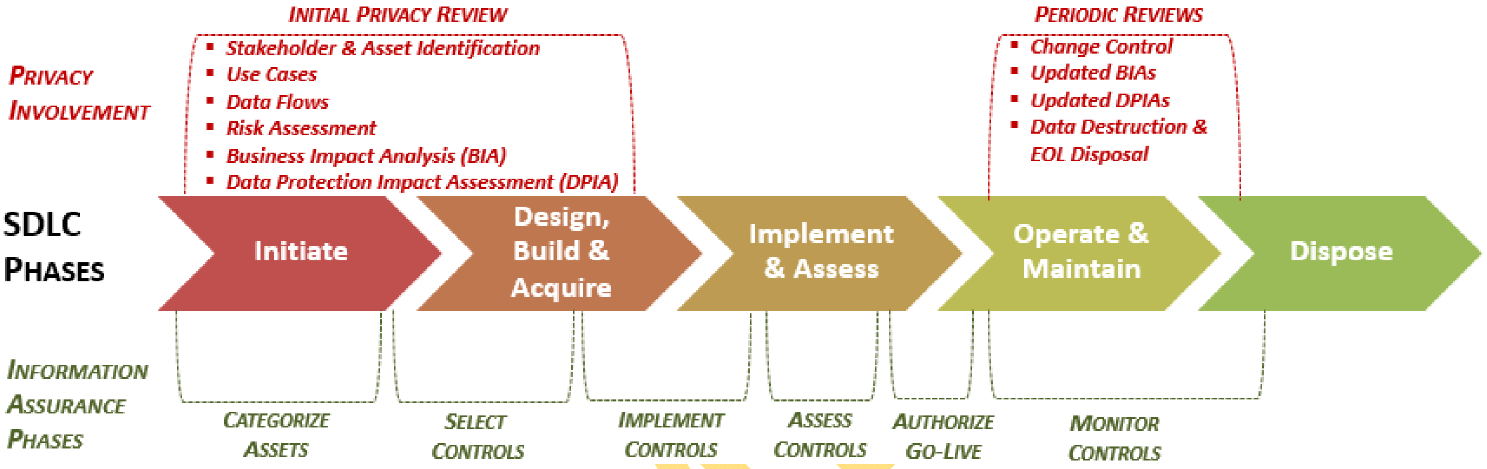
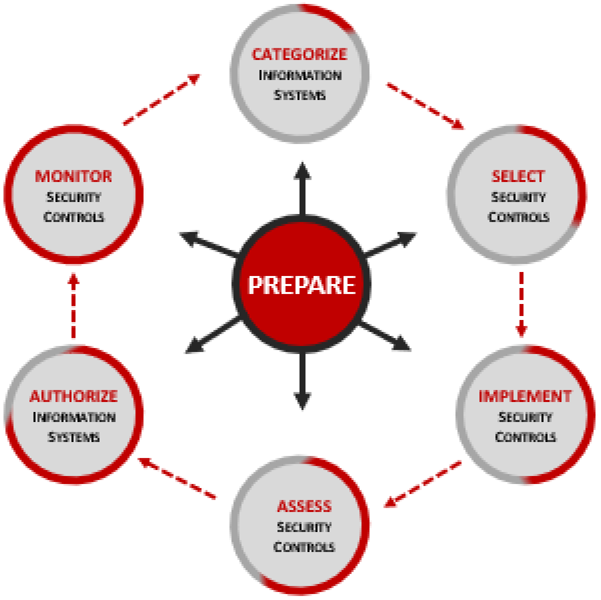


Figure 3. Secure development must involve coordinated cybersecurity and privacy operations.

Leveraging The Risk Management Framework (RMF) To Organize Security & Privacy Tasks

The goal of secure engineering is to deliver systems deemed "adequately secure" by stakeholders, since it is impossible to completely eliminate risk. The fundamental relationships among assets, an asset-dependent interpretation of loss and the corresponding loss consequences are central to any discussion of system security. This is where aligning ACME's Security by Design (SbD) and Privacy by Design (PbD) efforts with the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) is very beneficial, since the RMF provides a well-established format to securely engineer and maintain systems throughout the entire lifecycle of the asset.[15] See Annex 1 for RMF-specific secure engineering steps.



Categorize Information Systems
Select Security Controls
Implement Security Controls
Assess Security Controls
Authorize Information Systems
Monitor Security Controls
Prepare

Figure 4. Overview of Risk Management Framework (RMF) phases from NIST 800-37.

[15] NIST 800-37 rev2 - https://csrc.nist.gov/news/2018/rmf-update-nist-publishes-sp-800-37-rev-2

Multi-Tiered Security & Privacy Risk Model

Managing system-related security 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.

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 security and privacy risk at the organization level, the mission/business process level, and the information system level.[17] 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

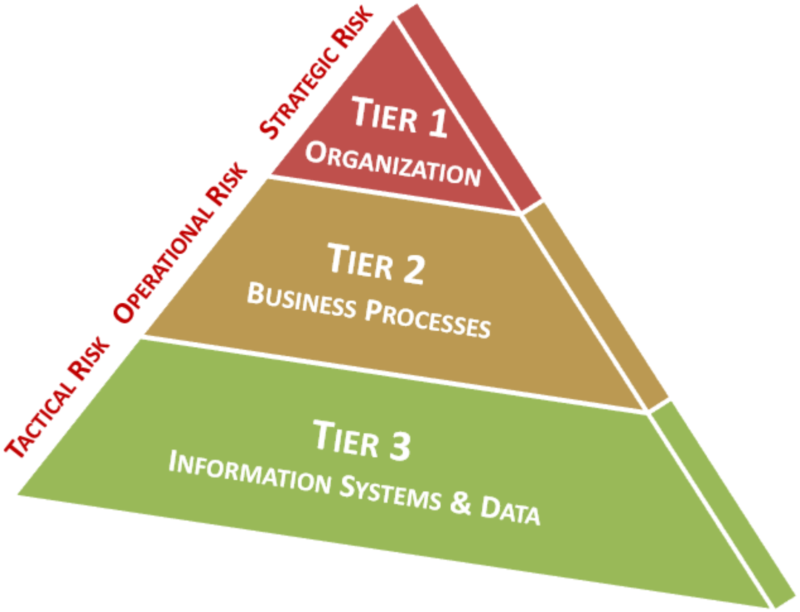


Figure 7. Multi-tiered cybersecurity & privacy risk model

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:

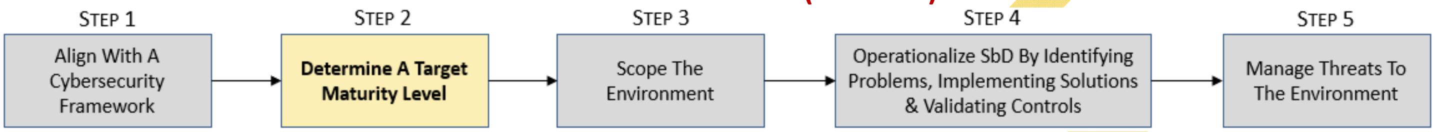
- Who?
  - Data Protection Officer (DPO) and their respective team(s); and
  - Chief Information Security Officer (CISO) and their respective team(s).
- How?
  - Resources for appropriate staffing and technology;
  - Senior leadership steering committees for company-wide buy-in for cybersecurity and privacy initiatives; and
  - Situational awareness through Key Performance Indicator (KPI) metrics reporting.

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

- ○ Secure Controls Framework (SCF)
- ○ Cloud Security Alliance Cloud Controls Matrix (**CSA CCM**)
- ○ Center for Internet Security (**CIS**) configuration benchmarks
- ○ Department of Defense Cybersecurity Agency (**DISA**) Secure Technology Implementation Guides (STIGs)
- ○ European Union Regulation 2016/279 (General Data Protection Regulation (**EU GDPR**))
- ○ Payment Card Industry Data Security Standard (**PCI DSS**)

Appropriate security controls will be selected from these frameworks, based on risk and applicability to the project / initiative. See Annex 4, *Cybersecurity & Privacy Control Selection*, for more details on identifying appropriate cybersecurity and privacy controls.

Step 2: Identify A Security & Privacy Capability Maturity Model (SP-CMM) Target State


Step 1
Align With A Cybersecurity Framework
Step 2
Determine A Target Maturity Level
Step 3
Scope The Environment
Step 4
Operationalize SbD By Identifying Problems, Implementing Solutions & Validating Controls
Step 5
Manage Threats To The Environment

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. Appendix E, *Security & Privacy Capability Maturity Model (SP-CMM)*, provides greater detail on this targeted maturity state.

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

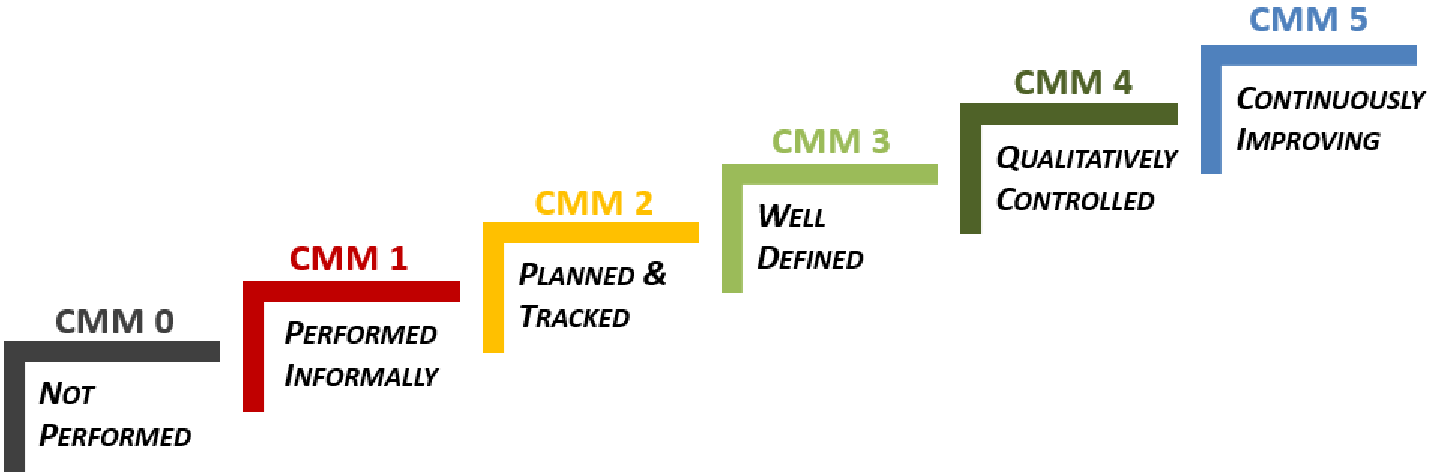
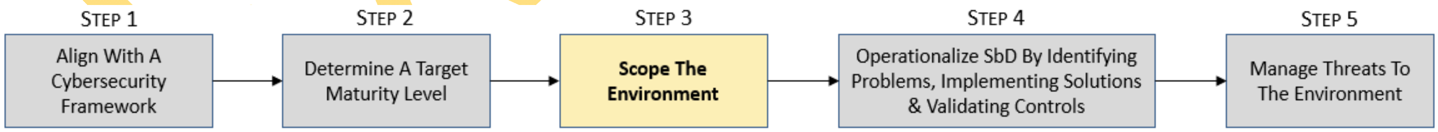


Figure 11. Security & Privacy Capability Maturity Model (SP-CMM) levels.

Step 3: Determine Appropriate Scoping for Security Controls


Step 1
Align With A Cybersecurity Framework
Step 2
Determine A Target Maturity Level
Step 3
Scope The Environment
Step 4
Operationalize SbD By Identifying Problems, Implementing Solutions & Validating Controls
Step 5
Manage Threats To The Environment

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, application or service that is in scope for the project or initiative;
- Zone 2 – The asset exists within the immediate operating environment that has a direct impact on the asset; or
- Zone 3 – The asset exists outside of the immediate operating environment but indirectly influences the asset.

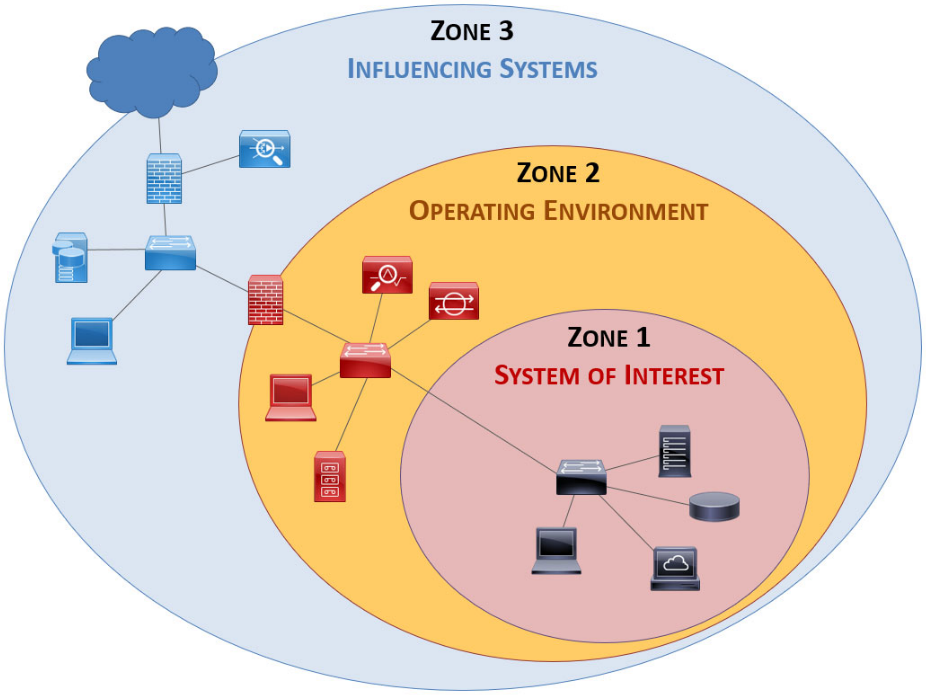


Figure 12. Zone-based approach to determining scoping efforts.

ZONE 1: SYSTEMS OF INTEREST

Zone 1 only contains systems of interest.

- Systems of Interest
  - These are systems that are the focus of the secure engineering effort.
- Examples include:
  - Project-related systems, applications & services

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
    - Centralized log management, antimalware, and other security mechanisms
    - General and special-purpose information systems
    - Command, control, and communication systems
    - Crypto modules
    - Central processing units and graphics processor boards
    - Industrial/process control systems
    - Weapons systems
    - Medical devices and treatment systems
    - Financial, banking, and merchandising transaction systems
    - Social networking systems
- System Elements
  - Member of a set of elements that constitute a system.
  - Examples include:
    - Hardware
    - Software
    - Firmware

OPERATIONALIZING PRIVACY BY DESIGN

Breaches involving Personal Data (PD) 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 PD, ACME uses a risk-based approach to guide protection requirements.

ACME cannot properly protect PD it does not know about. This document uses a broad definition of PD to identify as many potential sources of PD as possible (e.g., databases, shared network drives, backup tapes, contractor sites). PD 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 Personal Data / Personal Data can be referenced in Appendix A.

UNDERSTANDING PRIVACY BY DESIGN (PBD)

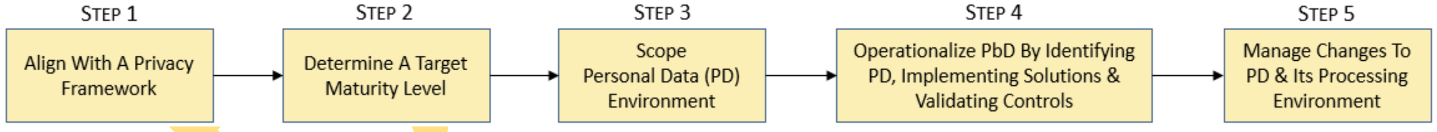
The term Privacy by Design (PbD) is commonly associated with several principles, but the term has evolved since it was first coined.[22] This original PbD framework contains the following seven (7), high-level privacy principles:

1. Privacy must be proactive, not reactive, and must anticipate privacy issues before they reach the user. Privacy must also be preventative, not remedial.
2. Privacy must be the default setting. The user should not have to take actions to secure their privacy, and consent for data sharing should not be assumed.
3. Privacy must be embedded into design. It must be a core function of the product or service, not an add-on.
4. Privacy must be positive sum and should avoid dichotomies. PbD sees an achievable balance between privacy and security, not a zero-sum game of privacy or security.
5. Privacy must offer end-to-end lifecycle protection of user data. This means engaging in proper data minimization, retention and deletion processes.
6. Privacy standards must be visible, transparent, open, documented and independently verifiable. ACME's processes must stand up to external scrutiny.
7. Privacy must be user-centric. This means giving users granular privacy options, maximized privacy defaults, detailed privacy information notices, user-friendly options and clear notification of changes.

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

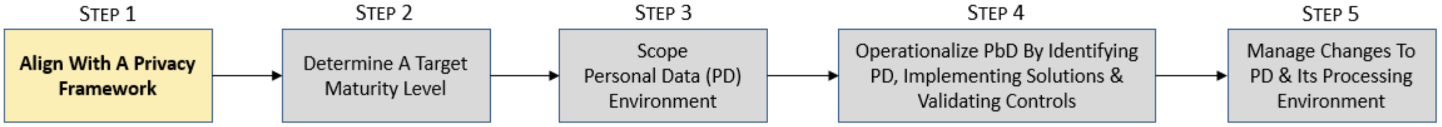
- Be properly and consistently applied throughout the PD lifecycle;
- Apply to all actors who have a connection with the information; and
- Apply to all systems/networks and jurisdictions where PD information is exposed.

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


STEP 1 – Align With A Privacy Framework
STEP 2 – Determine A Target Maturity Level
STEP 3 – Scope Personal Data (PD) Environment
STEP 4 – Operationalize PbD By Identifying PD, Implementing Solutions & Validating Controls
STEP 5 – Manage Changes To PD & Its Processing Environment

[22] The term Privacy by Design (PbD) is accredited to Ann Cavoukian, Ph.D., the Information & Privacy Commissioner, Ontario, Canada.

Step 1: Align With Leading Privacy Frameworks


Step 1
Align With A Privacy Framework
Step 2
Determine A Target Maturity Level
Step 3
Scope Personal Data (PD) Environment
Step 4
Operationalize PbD By Identifying PD, Implementing Solutions & Validating Controls
Step 5
Manage Changes To PD & Its Processing Environment

When defining "adequate level of data protection" and "data protection by design and by default" in terms of its alignment with leading privacy practices, ACME primarily aligns with the Secure Controls Framework (SCF) **Privacy Management Principles** since it consolidates several complex privacy frameworks into a single set of privacy management principles. [23]

The SCF Privacy Management Principles were developed to help organizations manage create an effective privacy program to addresses privacy risks and obligations, as well as business opportunities. These Privacy Management Principles establish a "Rosetta stone" approach to creating a baseline set of privacy principles from a myriad of industry-recognized privacy practices. When you tie the broader S|P in with these privacy management principles, you have an excellent foundation for building and maintaining secure systems, applications and services that address cybersecurity and privacy considerations by default and by design. ACME's use of the SCF Privacy Management Principles allows it to align with the following:

- AICPA Trust Services Criteria (SOC 2 privacy controls)
- Asia-Pacific Economic Cooperation (APEC) Privacy Framework
- California Consumer Privacy Act (CCPA)
- European Union General Data Protection Regulation (EU GDPR)
- Fair Information Practice Principles (FIPPs) (DHS & OMB versions)
- Generally Accepted Privacy Principles (GAPP)
- Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule
- ISO 27701
- ISO 29100
- Nevada SB820
- NIST 800-53 rev 4 (privacy controls)
- NIST Privacy Framework [draft]
- Organization for Economic Co-operation and Development (OECD) Privacy Guidelines
- Office of Manage and Budget (OMB) A-130
- Personal Information Protection and Electronic Documents Act (PIPEDA)

Privacy Management Principles

Annex 3 contains a complete listing of these Privacy Management Principles. These principles are grouped into the following eleven (11) categories:

1. **Privacy by Design**. Establish and maintain a comprehensive privacy program that ensures privacy considerations are addressed by design in the development of policies, standards, processes, systems, applications, projects and third-party contracts.
2. **Data Subject Participation**. Individuals are directly involved in the decision-making process regarding the fair and lawful processing of the individual's personal data and, to the extent practicable, directly-engaged to receive explicit permission to use their personal data.
3. **Limited Collection & Use**. Ensure that the design of data collection and use are consistent with the intended use of the information, and the need for new information is balanced against any privacy risks.
4. **Transparency**. Provide a transparent notice to the public about privacy practices through a clear and conspicuous notice on all organizational websites, mobile applications, and other digital services regarding the collection, creation, use, dissemination, maintenance, retention, and/or disclosure of the personal data.
5. **Data Lifecycle Management**. Limit the collection, creation, use, dissemination, maintenance, retention, and/or disclosure of personal data to that which is legally authorized, relevant, and deemed "reasonably necessary" for the proper performance of business functions.
6. **Data Subject Rights**. Provide individuals with appropriate access to their personal data.
7. **Security by Design**. Establish administrative, technical, and physical safeguards to protect sensitive data commensurate with the risk and magnitude of the harm that would result from its unauthorized access, use, modification, loss or dissemination. Selected practices are in accordance with industry-leading practices (e.g., ISO 27002, NIST 800-53, etc.).
8. **Incident Response**. Maintain adequate incident response plans, capabilities and training for employees and third-party stakeholders on how to report and respond to incidents.

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

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 800-171, etc.).

The chart below is intended to provide reasonable guidance for expectations to keep systems, applications and services secure. The specifics of technology controls are determined by the technology platform, since certain technologies are not possible to be installed on all technology platforms.

Assurance Level	BASIC	ENHANCED
Level of Effort	Meets industry-recognized secure practices	Greater than basic industry-recognized secure practices
MANDATORY Technology Controls	▪ Antimalware (host-based) ▪ Encryption in transit (e.g., SSL/TLS, SFTP, SSH, etc.) ▪ Log collection (forwarded to centralized log collector) ▪ Patch management ▪ Vulnerability scanning ▪ Identity & Access Management (IAM)	▪ Antimalware (host-based) ▪ Configuration management (automated) ▪ Encryption at rest (e.g., file, folder, table or whole drive) ▪ Encryption in transit (e.g., SSL/TLS, SFTP, SSH, etc.) ▪ File Integrity Monitoring (**FIM**) ▪ Host Intrusion Prevention System (**HIPS**) ▪ Log collection (forwarded to **SIEM**) ▪ Mobile Device Management (**MDM**) ▪ Multi-Factor Authentication (**MFA**) ▪ Network Intrusion Detection / Protection (**NIDS** / **NIPS**) ▪ Next Generation Firewall (**NGF**) ▪ Patch management
DISCRETIONARY Technology Controls	▪ Configuration management (automated) ▪ Encryption at rest (e.g., file, folder, table or whole drive) ▪ Host Intrusion Prevention System (**HIPS**) ▪ Mobile Device Management (**MDM**) ▪ Multi-Factor Authentication (**MFA**) ▪ Network Intrusion Detection / Protection (**NIDS** / **NIPS**) ▪ Next Generation Firewall (**NGF**) ▪ Privileged Identity & Account Management (**PIAM**) ▪ Security Incident Event Manager (**SIEM**)	▪ Database encryption ▪ Database Access Management (**DAM**) ▪ Data Loss Prevention (**DLP**) ▪ Dynamic / Static Application Security Testing (**DAST** / **SAST**) ▪ Network Access Control (**NAC**) ▪ Penetration test ▪ Privileged Identity & Account Management (**PIAM**) ▪ Session recording ▪ Web Application Firewall (**WAF**)

Figure B-2: Basic vs. Enhanced control expectations.

There will be cases where the Assurance Level may require a set of controls, but cybersecurity, privacy, technology or business teams feel additional controls are needed to address a specific risk. This is where discretionary controls come into play. Discretionary controls are at the discretion of stakeholders to implement that go above and beyond Mandatory controls.

Enhanced controls are "situationally required" and must be selected and implemented based on applicable statutory, regulatory or contractual requirements. In the absence of any such requirements, ACME may treat these controls or enhancements as discretionary technology controls.

to support the goal of being an industry leader.

E-3: 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 privacy program. ▪ [NEGLIGENT]		It is unlikely for a large organization to completely ignore cybersecurity and privacy 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 security / privacy 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 privacy program (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 privacy program (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.

methods, techniques, tools, and automation to support continuous monitoring and near real-time risk management; and are cost-effective.
- Establish expectations for the control assessments and the level of effort for the assessment.
- Help to ensure that appropriate resources are applied toward determining control effectiveness while providing the necessary level of assurance in making such determinations.

Potential Input(s):

- security and privacy plans
- Program management control information
- Common control documentation
- Organizational security and privacy program plans
- System design documentation
- Enterprise, security, and privacy architecture information
- Policies and procedures applicable to the system

A-3: Control Assessments

Task: Assess the controls in accordance with the assessment procedures described in assessment plans.

Expected Deliverable(s):

- Security and privacy assessment plans
- security and privacy plans
- External assessment or audit results (if applicable)

Task Guidance: Control assessments determine the extent to which the selected controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting security and privacy requirements for the system and the organization. The system owner, common control provider, and/or organization rely on the technical skills and expertise of assessors to assess implemented controls using the assessment procedures specified in assessment plans and provide recommendations on how to respond to control deficiencies to reduce or eliminate identified vulnerabilities or unacceptable risks. The senior manager for privacy serves as the control assessor for the privacy controls and is responsible for conducting an initial assessment of the privacy controls prior to system operation, and for assessing the controls periodically thereafter at a frequency sufficient to ensure compliance with privacy requirements and to manage privacy risks.

Controls implemented to achieve both security and privacy objectives may require a degree of collaboration between security and privacy control assessors. The assessor findings are a factual reporting of whether the controls are operating as intended and whether any deficiencies in the controls are discovered during the assessment. Control assessments occur as early as practicable in the SDLC/PDLC, preferably during the development phase. These types of assessments are referred to as developmental testing and evaluation and validate that the controls are implemented correctly and are consistent with the established cybersecurity and privacy architectures.

Developmental testing and evaluation activities include, for example, design and code reviews, regression testing, and application scanning. Deficiencies identified early in the SDLC/PDLC can be resolved in a more cost-effective manner. Assessments may be needed prior to source selection during the procurement process to assess potential suppliers or providers before the organization enters into agreements or contracts to begin the development phase. The results of control assessments conducted during the SDLC/PDLC can also be used (consistent with reuse criteria established by the organization) during the authorization process to avoid unnecessary delays or costly repetition of assessments. Organizations can maximize the use of automation to conduct control assessments to increase the speed, effectiveness, and efficiency of the assessments, and to support continuous monitoring of the security and privacy posture of organizational systems. Applying and assessing controls throughout the development process may be appropriate for iterative development processes. When iterative development processes (e.g., agile development) are employed, an iterative assessment may be conducted as each cycle is completed. A similar process is employed for assessing controls in commercial IT products that are used in the system.

Organizations may choose to begin assessing controls prior to the complete implementation of all controls in the security and privacy plans. This type of incremental assessment is appropriate if it is more efficient or cost-effective to do so. Assessor independence during the continuous monitoring process facilitates reuse of assessment results to support ongoing authorization and reauthorization.

Assessment results can be reused to support reciprocity. To make the risk management process more efficient and cost-effective, organizations may choose to establish reasonable and appropriate criteria for reusing assessment results as part of organization-wide assessment policy or in the security and privacy program plans. For example, a recent audit of a system may have produced information about the effectiveness of selected controls. If prior assessment results from the system developer or vendor are available, the control assessor, under appropriate circumstances, may incorporate those results into the assessment. In addition, if a control implementation was assessed during other forms of assessment at previous stages of the SDLC/PDLC (e.g., unit testing, functional testing, acceptance testing), organizations may consider potential reuse of those results to reduce duplication of efforts.

Potential Input(s):

- Security and privacy assessment plans
- security and privacy plans
- External assessment or audit results (if applicable)

A-4: Assessment Reports

Task: Prepare the assessment reports documenting the findings and recommendations from the control assessments.

Expected Deliverable(s):

- Completed security and privacy assessment reports detailing the assessor findings and recommendations

Task Guidance: The results of the security and privacy control assessments, including recommendations for correcting deficiencies in the implemented controls, are documented in the assessment reports by control assessors. Assessment reports are key documents in the system or common control authorization package that is developed for authorizing officials. Organizations may develop a single, integrated security and privacy assessment report.

The assessment reports include information based on assessor findings, necessary to determine the effectiveness of the controls implemented within or inherited by the system. Assessment reports are an important factor in a determining risk to organizational operations and assets, individuals and other organizations by the authorizing official. The format and the level of detail provided in assessment reports are appropriate for the type of control assessment conducted, for example:

- Developmental testing and evaluation;
- Independent verification and validation;
- Independent assessments supporting system or common control authorizations or reauthorizations;
- Self-assessments;
- Assessments after remediation actions;
- Independent evaluations or audits; and
- Assessments during continuous monitoring.

Potential Input(s):

- Completed control assessments82 and associated assessment evidence

A-5: Remediation Actions

Task: Conduct initial remediation actions on the controls and reassess remediated controls.

Expected Deliverable(s):

- Completed initial remediation actions based on the security and privacy assessment reports
- Changes to implementations reassessed by the assessment team
- Updated security and privacy assessment reports
- Updated security and privacy plans including changes to the control implementations

Task Guidance: The security and privacy assessment reports describe deficiencies in the controls implemented within the system or the common controls available for inheritance that could not be resolved during the development of the system or that are discovered post-development. Such control deficiencies may result in security, privacy, and supply chain risks. The findings generated during control assessments provide information that facilitates a disciplined and structured approach to responding to those risks in accordance with the organizational risk tolerance and priorities. The issue resolution process can also ensure that only substantive items are identified and transferred to the plan of actions and milestones.

Findings from a system-level control assessment may necessitate an update to the system risk assessment and the organizational risk assessment. The updated risk assessment and any inputs from the senior risk manager determines the initial remediation actions and the prioritization of those actions. System owners and common control providers may decide, based on a risk assessment, that certain

Annex 3: Privacy Management Principles

In support of the Security & Privacy by Design (S|P) principles from Annex 2, the **Privacy Management Principles** from the Secure Controls Framework (SCF) provides a "Rosetta stone" approach to aligning with industry-recognized privacy practices. When you tie the broader S|P in with these privacy management principles, you have an excellent foundation for building and maintaining secure systems, applications and services that address cybersecurity and privacy considerations by default and by design.[36]

1.0 Privacy by Design.

Establish and maintain a comprehensive privacy program that ensures privacy considerations are addressed by design in the development of policies, standards, processes, systems, applications, projects and third-party contracts.

1.1 Assigned Responsibilities.

Assign accountability through documented roles and responsibilities to qualified individuals, including key internal and external stakeholders, for maintaining compliance with all applicable privacy requirements that involves appropriately monitoring and documenting the privacy program.

1.2 Data Classification.

Classify data according to the sensitivity and type of personal data as defined by appropriate statutory, regulatory and contractual contexts.

1.3 Registering Databases.

Register applicable databases containing personal data with the appropriate Data Authority, when required.

1.4 Resource Planning.

Identify and plan for resources needed to operate a privacy program and include privacy requirements in solicitations for technology solutions and services.

1.5 Inventory of PD.

Maintain an inventory of both the type of personal data and specific data element, as well as the systems, applications and processes that collect, create, use, disseminate, maintain, and/or disclose that personal data.

1.6 Privacy Training.

Provide recurring privacy awareness and training for all employees and contractors.

2.0 Data Subject Participation.

Individuals are directly involved in the decision-making process regarding the fair and lawful processing of the individual's personal data and, to the extent practicable, directly-engaged to receive explicit permission to use their personal data.

2.1 Clear Choices.

Provide clear and conspicuous choices that enable an individual, or a person authorized by the individual, to permit or prohibit the collection, creation, use, dissemination, maintenance, retention, and/or disclosure of the individual's personal data. This is also referred to as the right to "opt out."

2.2 Initial Consent.

Prior to the collection, creation, use, dissemination, maintenance, retention, and/or disclosure of the individual's personal data, the knowledge and consent of the individual are required.

2.3 Updated Consent.

Based on changes to privacy practices that affect the parameters of an individual's initial consent, updated consent of the individual is required to continue the collection, creation, use, dissemination, maintenance, retention, and/or disclosure of the individual's personal data. This is also referred to as the right to "opt out" at any time after the initial consent was provided.

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