Security & Privacy by Design Principles (S|P)

The S|P establishes 32 common-sense principles to guide the development and oversight of a modern security and privacy program. The S|P is sourced from the Secure Controls Framework (SCF), which is a free resource for businesses. The SCF's comprehensive listing of over 1,000 cybersecurity and privacy controls is categorized into 32 domains that are mapped to over 100 statutory, regulatory and contractual frameworks. Those applicable SCF controls can operationalize the S|P principles to help an organization ensure that secure practices are implemented by design and by default. Those 32 S|P principles are listed below:

1. Security & Privacy Governance

Execute a documented, risk-based program that supports business objectives while encompassing appropriate security and privacy principles that addresses applicable statutory, regulatory and contractual obligations.

2. Asset Management

Manage all technology assets from purchase through disposition, both physical and virtual, to ensure secured use, regardless of the asset's location.

3. Business Continuity & Disaster Recovery

Maintain a resilient capability to sustain business-critical functions while successfully responding to and recovering from incidents through well-documented and exercised processes.

4. Capacity & Performance Planning

Govern the current and future capacities and performance of technology assets.

5. Change Management

Manage change in a sustainable and ongoing manner that involves active participation from both technology and business stakeholders to ensure that only authorized changes occur.

6. Cloud Security

Govern cloud instances as an extension of on-premise technologies with equal or greater security protections than the organization's own internal cybersecurity and privacy controls.

7. Compliance

Oversee the execution of cybersecurity and privacy controls to ensure appropriate evidence required due care and due diligence exists to meet compliance with applicable statutory, regulatory and contractual obligations.

8. Configuration Management

Enforce secure configurations for systems, applications and services according to vendor-recommended and industry-recognized secure practices.

9. Continuous Monitoring

Maintain situational awareness of security-related events through the centralized collection and analysis of event logs from systems, applications and services.

10. Cryptographic Protections

Utilize appropriate cryptographic solutions and industry-recognized key management practices to protect the confidentiality and integrity of sensitive data both at rest and in transit.

11. Data Classification & Handling

Enforce a standardized data classification methodology to objectively determine the sensitivity and criticality of all data and technology assets so that proper handling and disposal requirements can
be followed.

12. Embedded Technology

Provide additional scrutiny to reduce the risks associated with embedded technology, based on the potential damages posed from malicious use of the technology.

13. Endpoint Security

Harden endpoint devices to protect against reasonable threats to those devices and the data those devices store, transmit and process.

14. Human Resources Security

Execute sound hiring practices and ongoing personnel management to cultivate a security and privacy-minded workforce.

15. Identification & Authentication

Enforce the concept of "least privilege" consistently across all systems, applications and services for individual, group and service accounts through a documented and standardized Identity and Access Management (IAM) capability.

16. Incident Response

Maintain a viable incident response capability that trains personnel on how to recognize and report suspicious activities so that trained incident responders can take the appropriate steps to handle incidents, in accordance with a documented Incident Response Plan (IRP).

17. Assurance

Execute an impartial assessment process to validate the existence and functionality of appropriate cybersecurity and privacy controls, prior to a system, application or service being used in a production environment.

18. Maintenance

Proactively maintain technology assets, according to current vendor recommendations for configurations and updates, including those supported or hosted by third-parties.

19. Mobile Device Management

Implement measures to restrict mobile device connectivity with critical infrastructure and sensitive data that limit the attack surface and potential data exposure from mobile device usage.

20. Network Security

Architect and implement a secure and resilient defense-in-depth methodology that enforces the concept of "least functionality" through restricting network access to systems, applications and services.

21. Physical & Environmental Security

Protect physical environments through layers of physical security and environmental controls that work together to protect both physical and digital assets from theft and damage.

22. Privacy

Align privacy practices with industry-recognized privacy principles to implement appropriate administrative, technical and physical controls to protect regulated personal data throughout the lifecycle of systems, applications and services.

SCF SECURE CONTROLS FRAMEWORK

version 2022.1

23. Project & Resource Management

Operationalize a viable strategy to achieve cybersecurity & privacy objectives that establishes cybersecurity as a key stakeholder within project management practices to ensure the delivery of resilient and secure solutions.

24. Risk Management

Proactively identify, assess, prioritize and remediate risk through alignment with industry-recognized risk management principles to ensure risk decisions adhere to the organization's risk threshold.

25. Secure Engineering & Architecture

Utilize industry-recognized secure engineering and architecture principles to deliver secure and resilient systems, applications and services.

26. Security Operations

Execute the delivery of security and privacy operations to provide quality services and secure systems, applications and services that meet the organization's business needs.

27. Security Awareness & Training

Foster a security and privacy-minded workforce through ongoing user education about evolving threats, compliance obligations and secure workplace practices.

28. Technology Development & Acquisition

Develop and test systems, applications or services according to a Secure Software Development Framework (SSDF) to reduce the potential impact of undetected or unaddressed vulnerabilities and design weaknesses.

29. Third-Party Management

Execute Supply Chain Risk Management (SCRM) practices so that only trustworthy third-parties are used for products and/or service delivery.

30. Threat Management

Leverage industry-recognized Attack Surface Management (ASM) practices to strengthen the security and resilience systems, applications and services against evolving and sophisticated attack vectors.

31. Vulnerability & Patch Management

Utilize a risk-based approach to vulnerability and patch management practices that minimizes the attack surface of systems, applications and services.

32. Web Security

Ensure the security and resilience of Internet-facing technologies through secure configuration management practices and monitoring for anomalous activity.

Security & Privacy Capability Maturity Model (SP-CMM)

CMM 0 Not Performed	CMM 1 Performed Informally	CMM 2 Planned & Tracked	CMM 3 Well Defined	CMM 4 Quantitatively Controlled	CMM 5 Continuously Improving
NEGLIGENT PRACTICES	*AD HOC PRACTICES*	*REQUIREMENTS-DRIVEN PRACTICES*	*ENTERPRISE-WIDE STANDARDIZATION*	*METRICS-DRIVEN PRACTICES*	*WORLD-CLASS PRACTICES*

The SP-CMM enables organizations using the S|P and associated SCF controls to identify objective expectations for each control, based on the targeted maturity level.

Based on the criteria provided by each of the SP-CMM's maturity levels, this allows the SCF to assess maturity across multiple statutory, regulatory or contractual requirement, since it is written to be objective and the maturity is focused at the control level. The SP-CMM is a free resource for businesses and is included as part of the SCF.

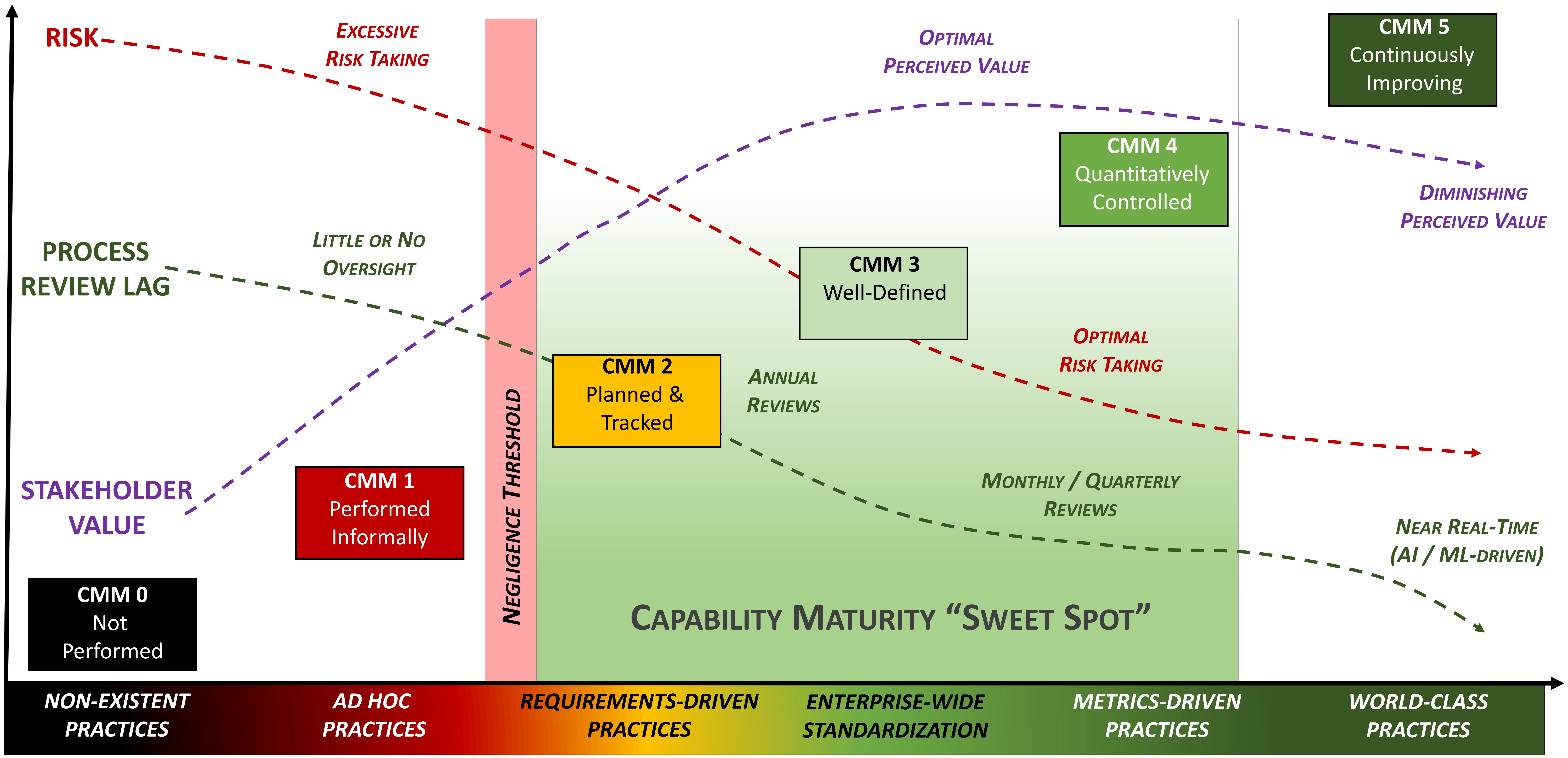
Security & Privacy Capability Maturity Model (SP-CMM)

The SP-CMM a Capability Maturity Model (CMM) that was designed to help solve the problem of objectivity in both establishing and evaluating cybersecurity and privacy control, so maturity criteria can exist to defend decisio

There are three main objectives for the SP-CMM:

1. Provide CISO/CPOs/CIOs with objective criteria that can be used to establish expectations for a cybersecurity & privacy program;
2. Provide objective criteria for project teams so that secure practices are appropriately planned and budgeted for; and
3. Provide minimum criteria that can be used to evaluate third-party service provider controls.

SECURE CONTROLS FRAMEWORK



RISK

EXCESSIVE RISK TAKING

OPTIMAL PERCEIVED VALUE

CMM 5 Continuously Improving

CMM 4 Quantitatively Controlled

DIMINISHING PERCEIVED VALUE

PROCESS REVIEW LAG

LITTLE OR NO OVERSIGHT

CMM 3 Well-Defined

OPTIMAL RISK TAKING

CMM 2 Planned & Tracked

ANNUAL REVIEWS

STAKEHOLDER VALUE

CMM 1 Performed Informally

MONTHLY / QUARTERLY REVIEWS

NEAR REAL-TIME (AI / ML-DRIVEN)

NEGLIGENCE THRESHOLD

CMM 0 Not Performed

CAPABILITY MATURITY "SWEET SPOT"

NON-EXISTENT PRACTICES

AD HOC PRACTICES

REQUIREMENTS-DRIVEN PRACTICES

ENTERPRISE-WIDE STANDARDIZATION

METRICS-DRIVEN PRACTICES

WORLD-CLASS PRACTICES

MATURITY LEVEL (PEOPLE, PROCESSES, TECHNOLOGY & DATA) = INCREASING COST & COMPLEXITY

RISK : Risk decreases with maturity, but noticeable risk reductions are harder to attain above CMM 3.

PROCESS IMPROVEMENTS : Process improvements increase with maturity, based on shorter review cycles and increased process oversight. Artificial Intelligence (AI) and Machine Learning (ML) can make process improvements near real-time at CMM 5.

STAKEHOLDER VALUE : The perceived value of security controls increases with maturity, but plateaus after CMM 3 and decreases after CMM 4. The value of the additional cost and complexity is harder to justify after CMM 3.