SECURE CONTROLS FRAMEWORK

SECURITY & PRIVACY CAPABILITY MATURITY MODEL (SP-CMM) OVERVIEW

version 2022.1

con·trol
/kən trol/

A control is the power to influence or direct behaviors and the course of events. That is precisely why the Secure Controls Framework™ (SCF) was developed – we want to influence secure practices within organizations so that both cybersecurity and privacy principles are designed, implemented and managed in an efficient and sustainable manner.

NOTE - This guide is for educational purposes only. You are highly encouraged to work with a cybersecurity, privacy or audit professional to validate any compliance-related assumptions. For more information, please visit www.SecureControlsFramework.com

Table of Contents

© 2022. Secure Controls Framework Council, LLC. All Rights Reserved.
This guide is for educational purposes only. You are encouraged to work with a cybersecurity, privacy or audit professional to validate any compliance-related assumptions.

EXECUTIVE SUMMARY

Thank you for showing interest in the **Secure Controls Framework's™ (SCF) Security & Privacy Capability Maturity Model (SP-CMM)**! This was a massive undertaking by SCF contributors to define maturity levels for the SCF's control catalog. The result of that work is each of the SCF's controls has corresponding CMM 0-5 criteria defined.

This document is designed for cybersecurity & privacy practitioners to gain an understanding of what the SP-CMM is and how it can be used in their organization.

Just like the SCF itself, the SP-CMM is free for organizations to use through the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

OBJECTIVES OF THE SP-CMM

The SP-CMM is meant to solve the problem of objectivity in both establishing and evaluating cybersecurity and privacy controls. 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.

There are likely many other use cases that the SP-CMM can be used, but those three objectives listed above drove the development of this project. The reason for this simply comes down to a need by businesses, regardless of size or industry, for a solution that can help fix those three common frustrations that exist in most cybersecurity and privacy programs. We want to help eliminate, or at least minimize, the Fear, Uncertainty & Doubt (FUD) that is used to justify purchases and/or evaluate controls by injecting objectivity into the process.

NOT JUST ANOTHER CMM

There are many competing models that exist to demonstrate maturity. Given the available choices, the SCF decided to leverage an existing framework, rather than reinvent the wheel. In simple terms, we provided control-level criteria to an existing CMM model.

The SP-CMM draws upon the high-level structure of the **Systems Security Engineering Capability Maturity Model v2.0 (SSE-CMM)**, since we felt it was the best model to demonstrate varying levels of maturity for people, processes and technology at a control level. If you are unfamiliar with the SSE-CMM, it is well-worth your time to read through the SSE-CMM Model Description Document that is hosted by the US Defense Technical Information Center (DTIC).

The SSE-CMM has been around for over two decades and is a community-owned maturity model, so it is free to use. The SSE-CMM is also referenced as ISO/IEC 21827:2008 *Information technology -- Security techniques -- Systems Security Engineering -- Capability Maturity Model (SSE-CMM).*[1]

NESTED APPROACH TO MATURITY

By using the term "nested" regarding maturity, we are referring how the SP-CMM's control criteria were written to acknowledge that each succeeding level of maturity is built upon its predecessor. Essentially, you cannot run without first learning how to walk. Likewise, you cannot walk without first learning how to crawl. This approach to defining cybersecurity & privacy control maturity is how the SP-CMM is structured.

[1] *ISO/IEC 21827:2008 - https://www.iso.org/standard/44716.html*

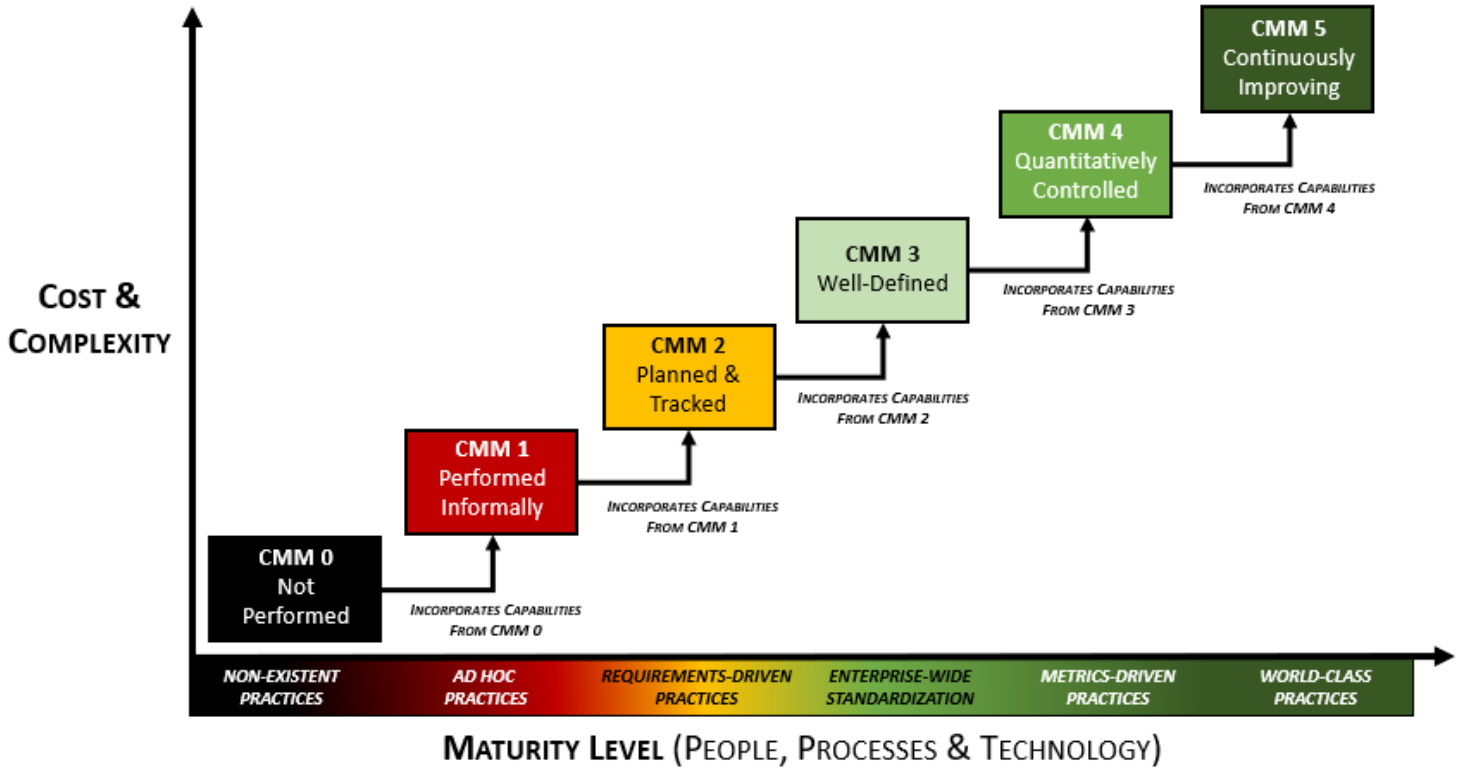
© 2022. Secure Controls Framework Council, LLC. All Rights Reserved.
This guide is for educational purposes only. You are encouraged to work with a cybersecurity, privacy or audit professional to validate any compliance-related assumptions.

Security & Privacy Capability Maturity Model (SP-CMM) Overview

The SP-CMM draws upon the high-level structure of the **Systems Security Engineering Capability Maturity Model v2.0 (SSE-CMM)**, since we felt it was the best model to demonstrate varying levels of maturity for people, processes and technology at a control level. If you are unfamiliar with the SSE-CMM, it is well-worth your time to read through the SSE-CMM Model Description Document that is hosted by the US Defense Technical Information Center (DTIC).

The six SP-CMM levels are:

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



CMM 0 – Not Performed

This level of maturity is defined as "non-existence practices," where the control is not being performed.

- There are no identifiable work products of the process.

CMM 0 practices, or a lack thereof, are generally considered to be negligent. The reason for this is if a control is reasonably-expected to exist, by not performing the control that would be negligent behavior. The need for the control could be due to a law, regulation or contractual obligation (e.g., client contract or industry association requirement).

CMM 1 – Performed Informally

This level of maturity is defined as "ad hoc practices," where the control is being performed, but lacks completeness & consistency.

- Base practices of the process area are generally performed.
- The performance of these base practices may not be rigorously planned and tracked.
- Performance depends on individual knowledge and effort.
- There are identifiable work products for the process.

CMM 1 practices are generally considered to be negligent. The reason for this is if a control is reasonably-expected to exist, by only implementing ad-hoc practices in performing the control that could be considered negligent behavior. The need for the control could be due to a law, regulation or contractual obligation (e.g., client contract or industry association requirement).

© 2022. Secure Controls Framework Council, LLC. All Rights Reserved.
This guide is for educational purposes only. You are encouraged to work with a cybersecurity, privacy or audit professional to validate any compliance-related assumptions.

Note – The reality with a CMM 1 level of maturity is often:

- *For smaller organizations, the IT support role only focuses on "break / fix" work or the outsourced IT provider has a limited scope in its support contract.*
- *For medium / large organizations, there is IT staff but there is no management focus to spend time on the control.*

CMM 2 – Planned & Tracked

This level of maturity is defined as "requirements-driven practices," where the expectations for controls are known (e.g., statutory, regulatory or contractual compliance obligations) and practices are tailored to meet those specific requirements.

- Performance of the base practices in the process area is planned and tracked.
- Performance according to specified procedures is verified.
- Work products conform to specified standards and requirements.

CMM 2 practices are generally considered to be "audit ready" with an acceptable level of evidence to demonstrate due diligence and due care in the execution of the control. CMM 2 practices are generally targeted on specific systems, networks, applications or processes that require the control to be performed for a compliance need (e.g., PCI DSS, HIPAA, NIST 800-171, etc.).

It can be argued that CMM 2 practices focus more on compliance over security. The reason for this is the scoping of CMM 2 practices are narrowly-focused and are not organization-wide.

Note – The reality with a CMM 2 level of maturity is often:

- *For smaller organizations:*
  - *IT staff have clear requirements to meet applicable compliance obligations or the outsourced IT provider is properly scoped in its support contract to address applicable compliance obligations.*
  - *It is unlikely that there is a dedicated cybersecurity role and at best it is an additional duty for existing personnel.*
- *For medium / large organizations:*
  - *IT staff have clear requirements to meet applicable compliance obligations.*
  - *There is most likely a dedicated cybersecurity role or a small cybersecurity team.*

CMM 3 – Well-Defined

This level of maturity is defined as "enterprise-wide standardization," where the practices are well-defined and standardized across the organization.

- Base practices are performed according to a well-defined process using approved, tailored versions of standard, documented processes.
- Process is planned and managed using an organization-wide, standardized process.

CMM 3 practices are generally considered to be "audit ready" with an acceptable level of evidence to demonstrate due diligence and due care in the execution of the control. Unlike CMM 2 practices that are narrowly focused, CMM 3 practices are standardized across the organization.

It can be argued that CMM 3 practices focus on security over compliance, where compliance is a natural byproduct of those secure practices. These are well-defined and properly-scoped practices that span the organization, regardless of the department or geographic considerations.

Note – The reality with a CMM 3 level of maturity is often:

- *For smaller organizations:*
  - *There is a small IT staff that has clear requirements to meet applicable compliance obligations.*
  - *There is 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.*
- *For medium / large organizations:*
  - *IT staff have clear requirements to implement standardized cybersecurity & privacy principles across the enterprise.*
  - *In addition to the existence of a dedicated cybersecurity team, there are specialists (e.g., engineers, SOC analysts, GRC, 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.*

© 2022. Secure Controls Framework Council, LLC. All Rights Reserved.
This guide is for educational purposes only. You are encouraged to work with a cybersecurity, privacy or audit professional to validate any compliance-related assumptions.

CMM 4 – Quantitatively Controlled

This level of maturity is defined as "metrics-driven practices," where in addition to being well-defined and standardized practices across the organization, there are detailed metrics to enable governance oversight.

- Detailed measures of performance are collected and analyzed. This leads to a quantitative understanding of process capability and an improved ability to predict performance.
- Performance is objectively managed, and the quality of work products is quantitatively known.

CMM 4 practices are generally considered to be "audit ready" with an acceptable level of evidence to demonstrate due diligence and due care in the execution of the control, as well as detailed metrics enable an objective oversight function. Metrics may be daily, weekly, monthly, quarterly, etc.

Note – The reality with a CMM 4 level of maturity is often:

- *For smaller organizations, it is unrealistic to attain this level of maturity.*
- *For medium / large organizations:*
  - *IT staff have clear requirements to implement standardized cybersecurity & privacy principles across the enterprise.*
  - *In addition to the existence of a dedicated cybersecurity team, there are specialists (e.g., engineers, SOC analysts, GRC, 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). This situational awareness is made possible through detailed metrics.*

CMM 5 – Continuously Improving

This level of maturity is defined as "world-class practices," where the practices are not only well-defined and standardized across the organization, as well as having detailed metrics, but the process is continuously improving.

- Quantitative performance goals (targets) for process effectiveness and efficiency are established, based on the business goals of the organization.
- Continuous process improvement against these goals is enabled by quantitative feedback from performing the defined processes and from piloting innovative ideas and technologies.

CMM 5 practices are generally considered to be "audit ready" with an acceptable level of evidence to demonstrate due diligence and due care in the execution of the control and incorporates a capability to continuously improve the process. Interestingly, this is where **Artificial Intelligence (AI)** and **Machine Learning (ML)** would exist, since AI/ML would focus on evaluating performance and making continuous adjustments to improve the process. However, AI/ML are not requirements to be CMM 5.

Note – The reality with a CMM 5 level of maturity is often:

- *For smaller organizations, it is unrealistic to attain this level of maturity.*
- *For medium-sized organizations, it is unrealistic to attain this level of maturity.*
- *For large organizations:*
  - *IT staff have clear requirements to implement standardized cybersecurity & privacy principles across the enterprise.*
  - *In addition to the existence of a dedicated cybersecurity team, there are specialists (e.g., engineers, SOC analysts, GRC, 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). This 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.*

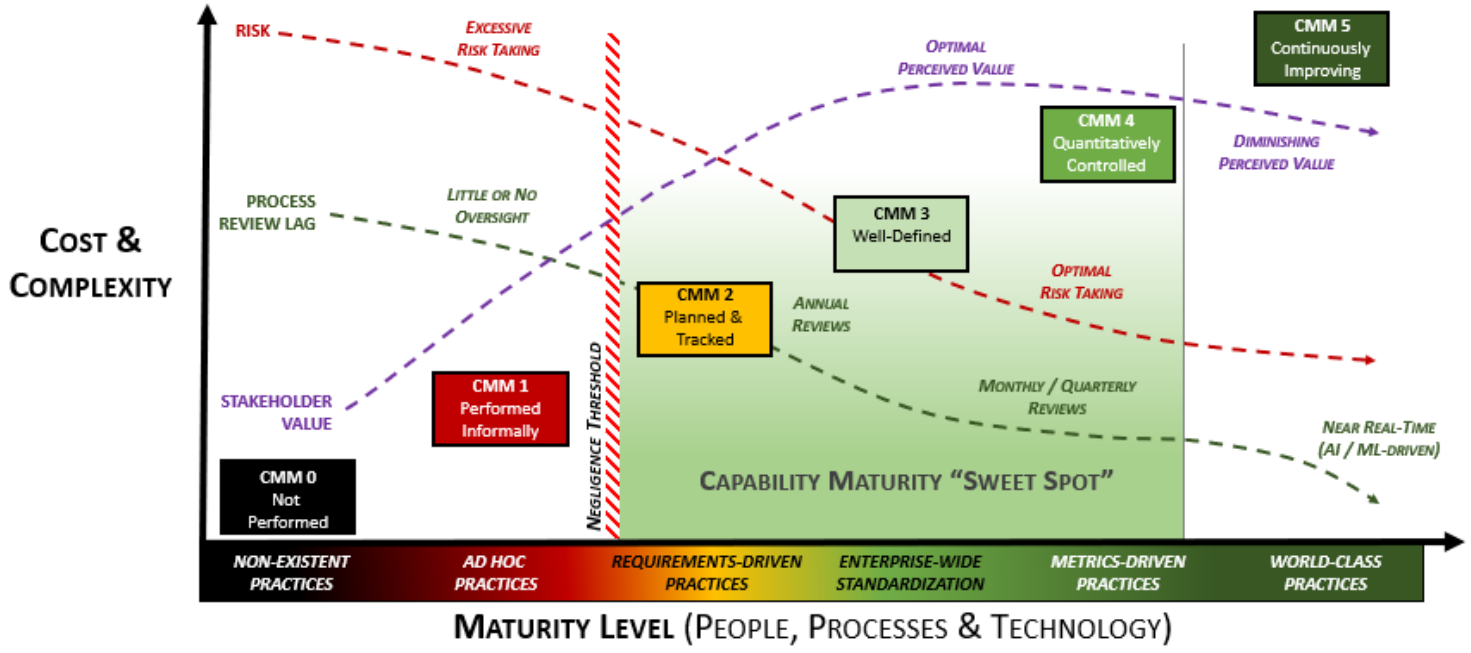
© 2022. Secure Controls Framework Council, LLC. All Rights Reserved.
This guide is for educational purposes only. You are encouraged to work with a cybersecurity, privacy or audit professional to validate any compliance-related assumptions.

Defining A Capability Maturity "Sweet Spot"

For most organizations, the "sweet spot" for maturity targets is between CMM 2 and 4 levels. What defines the ideal target within this zone is generally based on resource limitations and other business constraints, so it goes beyond just the cybersecurity and privacy teams dictating targets. Identifying maturity targets is meant to be a team effort between both technologists and business stakeholders.

From a business consideration, the increase in cost and complexity will always require cybersecurity and privacy leadership to provide a compelling business case to support any maturity planning needs. Speaking in terms the business can understand is vitally important.

Note - During the development of the SP-CMM, a contributor identified an interesting insight that CMM 0-3 are "internal" maturity levels for cybersecurity and privacy teams, whereas CMM 4-5 are "external" maturity levels that expand beyond those teams. When you look at the stakeholders involved in CMM 0-3, it is almost entirely IT, cybersecurity and privacy. It isn't until CMM 4-5 where there is true business stakeholder involvement in oversight and process improvement. This creates an internal to external shift in owning the cybersecurity & privacy program.



Negligence Considerations

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

Risk Considerations

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

Process Review Lag Considerations

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

Stakeholder Value Considerations

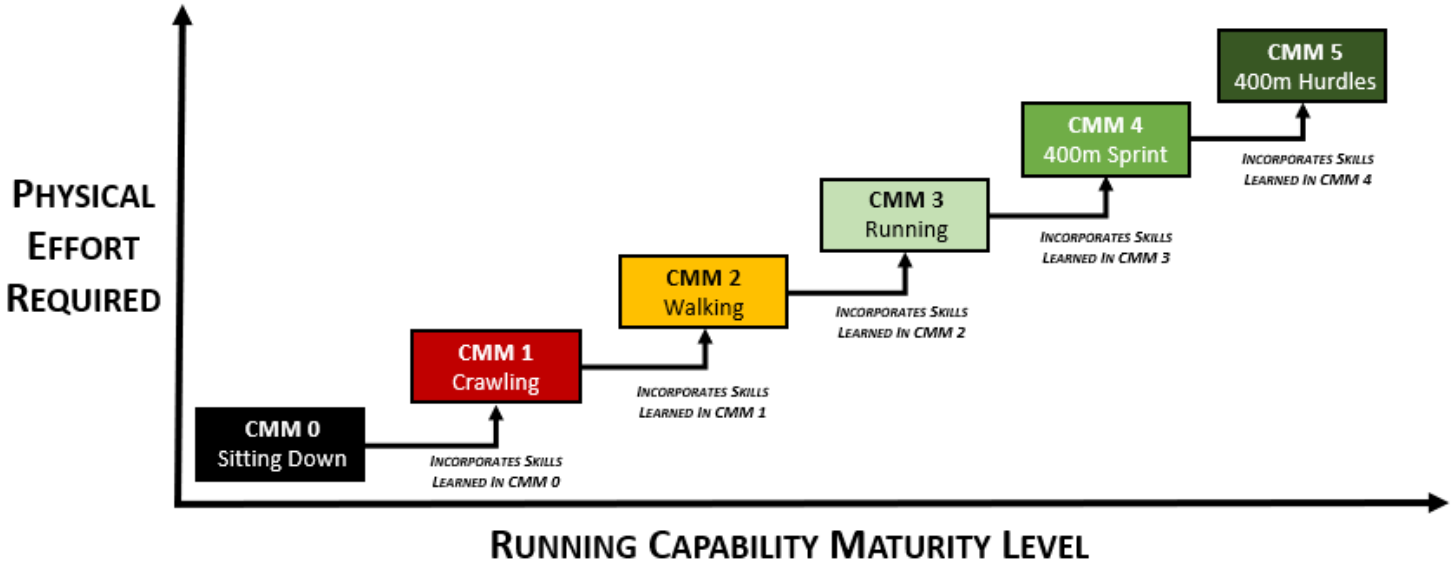
The perceived value of security controls increases with maturity. However, perceived value tends to decrease after CMM 3 since the value of the additional cost and complexity becomes harder to justify to business stakeholders. Companies that are genuinely focused on being industry leaders are ideal candidates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

© 2022. Secure Controls Framework Council, LLC. All Rights Reserved.
This guide is for educational purposes only. You are encouraged to work with a cybersecurity, privacy or audit professional to validate any compliance-related assumptions.

Analog Example – Sit / Crawl / Walk / Run / Sprint / Hurdle

The following example shows this approach being applied to the maturity levels for running, where it demonstrates the nested approach to the maturity levels by each succeeding level of maturity incorporates skills learned by the preceding level.

The point of this example is to demonstrate a relatable scenario that readers can comprehend how being asked to jump straight into an advanced level of maturity is not practical, where it requires some level of lesser maturity. For example, if you were just learning how to walk, it would be foolish to try and run the 400m hurdles that require both the strength and skill of sprinting, but also the knowledge of how to jump over an obstacle.



In this example, this maturity model is applied to a control to raise an individual's resting heart rate through exercise.

- **CMM 0 – Sitting Down**
  - Sitting down would be non-existent effort. No evidence of exercise exists.
  - Sitting down would be considered deficient in terms of meeting this control.
- **CMM 1 – Crawling**
  - Crawling is at best considered ad-hoc exercise and likely doesn't meet the intent of the control.
  - Crawling would be considered deficient in terms of meeting this control.
- **CMM 2 – Walking**
  - Walking builds on skills learned through crawling and demonstrates a capability that raises the individuals' resting heart rate.
  - Walking would meet the intent of the control, but there is clearly room for improvement.
- **CMM 3 – Running**
  - Running builds on the skills learned through walking and meets the control's intent.
  - Running would be the "sweet spot" of maturity for this example.
- **CMM 4 – 400-meter Sprint**
  - Sprinting builds on the skills learned through running and meets the control's intent.
  - Sprinting requires mastery of running skills to do it properly and avoid injury.
- **CMM 5 – 400-meter Hurdles**
  - Running the hurdles builds upon skills learned through sprinting and meets the control's intent.
  - Hurdling requires a mastery of sprinting, since jumping hurdles is in addition to a sprinting race.

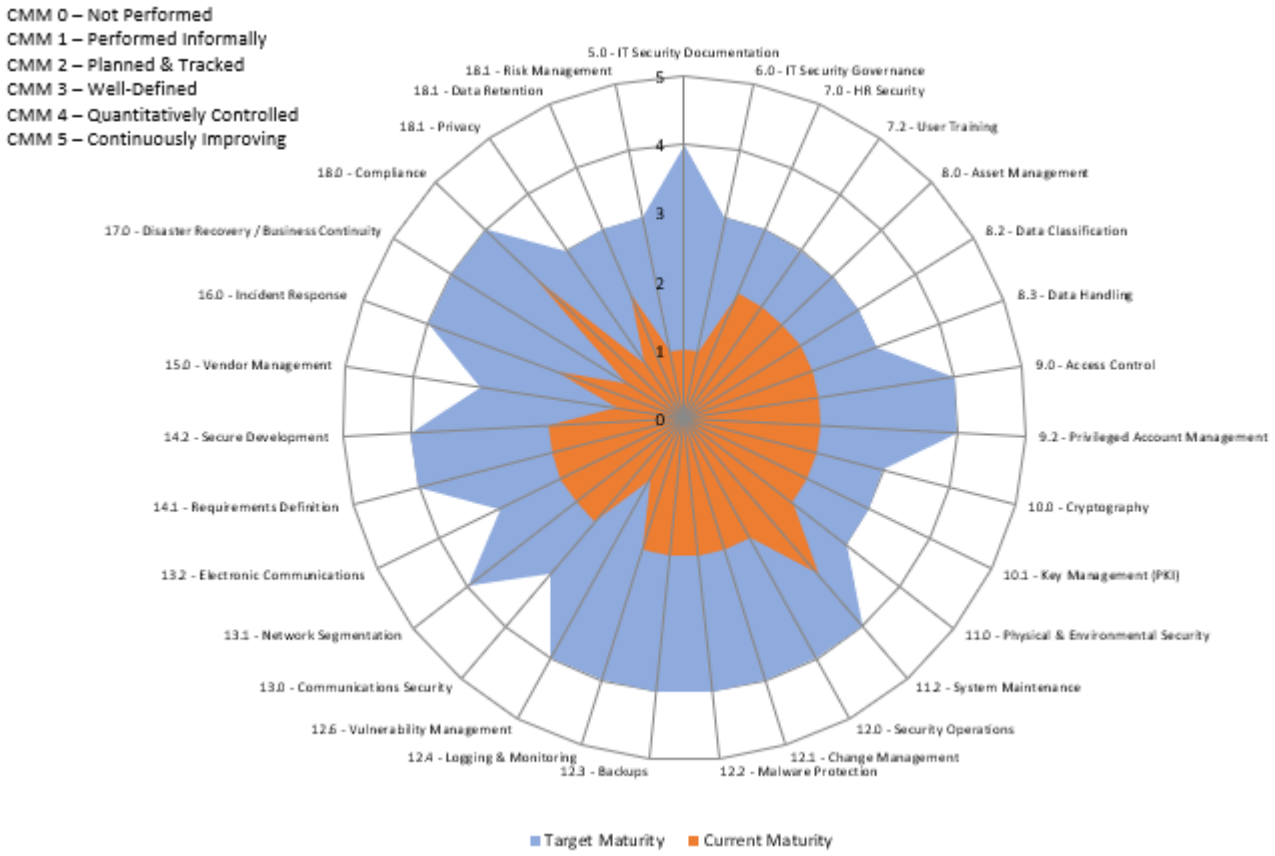
© 2022. Secure Controls Framework Council, LLC. All Rights Reserved.
This guide is for educational purposes only. You are encouraged to work with a cybersecurity, privacy or audit professional to validate any compliance-related assumptions.

EXPECTED SP-CMM USE CASES

USE CASE #1 – OBJECTIVE CRITERIA TO BUILD A CYBERSECURITY & PRIVACY PROGRAM

Identifying a target maturity state is intended to support your organization's mission and strategy so without first understanding the broader mission of the organization and having prioritized objectives, a CISO/CIO/CPO will be guessing when it comes to establishing expectations for capability maturity. Like anything in life, if you fail to plan you plan to fail - CMM rollouts are no exception.

The time to execute a business plan to mature a cybersecurity and privacy program generally spans several years, where certain capabilities are prioritized over other capabilities. This means the CISO/CIO/CPO will establish CMM targets that evolve each year, based on prioritization. In the graphic below, the use of a spider chart can be beneficial to identify current vs future gaps with the SP-CMM. Prioritization of capability maturities may be based on risk assessments, audits, compliance obligations or management direction.



IDENTIFYING THE PROBLEM

Using a CMM helps organizations avoid "moving targets" for expectations. Maturity goals define "what right looks like" in terms of the required people, processes and technology that are expected to exist in order to execute controls at the individual contributor level. Without maturity goals, it is very difficult and subjective to define success for a security & privacy program.

All too often, unprincipled cybersecurity & privacy leaders manipulate the business through **Fear, Uncertainty and Doubt (FUD)** to scare other technology and business leaders into supporting cybersecurity initiatives. These bad actors maintain the illusion of a strong cybersecurity & privacy program, when in reality the department is an array of disjointed capabilities that lacks a unifying plan. These individuals stay in the job long enough to claim small victories, implement some cool technology, and then jump ship for larger roles in other organizations to extend their path of disorder. In these cases, a common theme is the lack of viable business planning beyond a shopping list of technologies and headcount targets to further their career goals.

CONSIDERATIONS

Cybersecurity & privacy departments are a cost center, not a revenue-generating business function. That means cybersecurity & privacy compete with all other departments for budget, and it necessitates a compelling business case to justify needed technology and staffing. Business leaders are getting smarter on the topic of cybersecurity & privacy, so these leaders need to rise above the FUD mentality and deliver value that is commensurate with the needs of the business.

© 2022. Secure Controls Framework Council, LLC. All Rights Reserved.
This guide is for educational purposes only. You are encouraged to work with a cybersecurity, privacy or audit professional to validate any compliance-related assumptions.

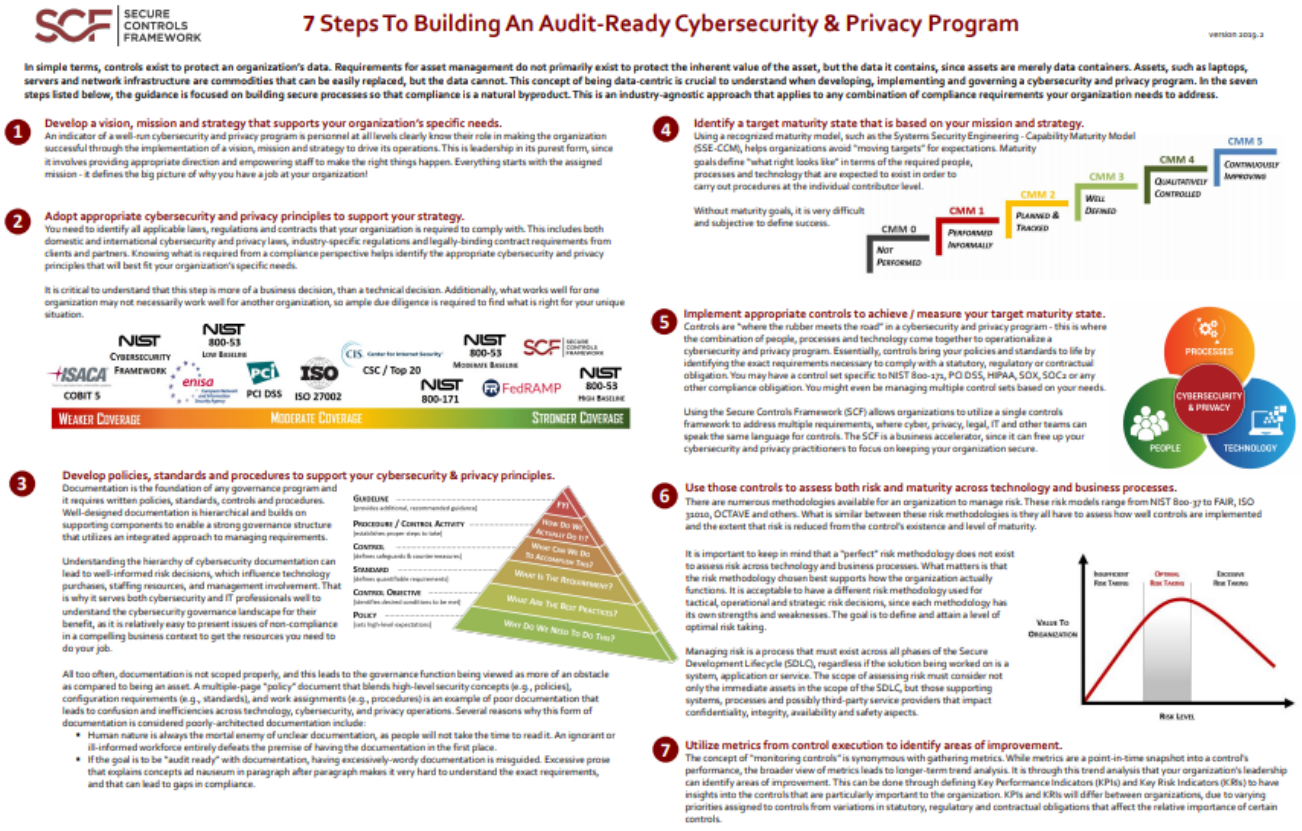
When identifying a target level of maturity, it is crucial to account for your organization's culture. The reason for this is the implementation of perceived "draconian" levels of security can cause a revolt in organizations not accustomed to heavy restrictions. One good rule of thumb when deciding between CMM 3 and CMM 4 targets is this simple question***: "Do you want to be in an environment that is in control or do you want to be in a controlled environment?"*** CMM 3 maturity is generally considered "an environment that is in control" where it is well-managed, whereas being in a CMM 4 environment is more of a "controlled environment" that is more controlled and less free. Given those considerations, environments not used to heavy restrictions may want to target CMM 3 as the highest-level of maturity targets. Additionally, the cost to mature from a CMM 3-4 or CMM 4-5 could be hundreds of thousands to millions of dollars, so there is a very real cost associated with picking a target maturity level. This is again where having management support is crucial to success, since this is ultimately a management decision.

From a CISO/CIO/CPO perspective, identifying a target level of maturity is also very beneficial in obtaining budget and protecting their professional reputation. In cases where business leadership doesn't support reaching the proposed target level of maturity, the CISO/CIO/CPO at least has documentation to prove he/she demonstrated a defined resourcing need (e.g., CMM level to support a business need) and the request was denied. Essentially, this can help cover a CISO/CIO/CPO in case an incident occurs and blame is pointed. That is just the reality of life for anyone in a high-visibility leadership position and being able to deflect unwarranted criticism is professional reputation insurance.

IDENTIFYING A SOLUTION

Defining a target maturity state is Step 4 in the "*7 Steps To Building An Audit-Ready Cybersecurity & Privacy Program*,"[2] a free resource from the SCF. That guide can be useful, since it helps establish two key pre-requisites to identifying CMM targets:

1. Prioritization of efforts (including resourcing); and
2. Identification of applicable statutory, regulatory and contractual obligations.



[2] *7 Steps To Building An Audit-Ready Cybersecurity & Privacy Program* - *http://scf.securecontrolsframework.com/scf-security-privacy-by-design-principles.pdf*

© 2022. Secure Controls Framework Council, LLC. All Rights Reserved.
This guide is for educational purposes only. You are encouraged to work with a cybersecurity, privacy or audit professional to validate any compliance-related assumptions.

Once a CISO/CIO/CPO has defined the prioritization and applicable compliance requirements, it is necessary to parse the SCF's controls catalog and then identify maturity targets for those applicable controls:

Parsing The SCF For Your Specific Needs

While there are over 1,000 controls in the SCF's controls catalog, it is necessary for an organization to pare down that catalog to only what is applicable to your organization (e.g., laws, regulations, contracts and industry expectations). This step simply involves filtering out the controls in the SCF that are not applicable and it can be easily done on the Customize The SCF page on the SCF website.[3] Additionally, this step can also be done within Excel or within a GRC solution. In the end, the result is a tailored set of controls that meet your organization's specific needs.

Identifying Maturity Targets

Now that you have pared down the SCF's controls catalog to only what is applicable, it is a manual review process to identify the appropriate level of maturity for each of the controls. There are several ways to approach this.

The most efficient manner we can recommend would be to first look at the thirty-two domains that make up the SCF and assign a high-level CMM level target for each domain. These domains are well-summarized in the SCF's free Security & Privacy by Design Principles (SIP) document and can be used by a CISO/CIO/CPO to quickly align a maturity target to each domain, in accordance with previously-established prioritization and business needs.

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 nearly 750 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:

SCF SECURE CONTROLS FRAMEWORK version 2019.2

1. Security & Privacy Governance
Govern a documented, risk-based program that encompasses appropriate security and privacy principles to address all 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 the capability to sustain business-critical functions while successfully responding to and recovering from incidents through a well-documented and exercised process.

4. Capacity & Performance Planning
Govern the current and future capacities and performance of technology assets.

5. Change Management
Govern 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 controls.

7. Compliance
Oversee the execution of cybersecurity and privacy controls to create appropriate evidence of due care and due diligence, demonstrating compliance with all applicable statutory, regulatory and contractual obligations.

8. Configuration Management
Govern the establishment and ongoing management of 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
Publish and enforce a 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 the risks associated with embedded technology, based on the potential damages posed when used maliciously.

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

14. Human Resources Security
Foster a security and privacy-minded workforce through sound hiring practices and ongoing personnel management.

15. Identification & Authentication
Implement an Identity and Access Management (IAM) capability to ensure the concept of "least privilege" is consistently implemented across all systems, applications and services for individual, group and service accounts.

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

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

18. Maintenance
Utilize secure practices to maintain technology assets, according to current vendor recommendations for configurations and updates, including those supported or hosted by third-parties.

19. Mobile Device Management
Govern mobile devices through a centralized or decentralized model to restrict logical and physical access to the devices, as well as the amount and type of data that can be stored, transmitted or processed.

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

21. Physical & Environmental Security
Implement layers of physical security and environmental controls that work together to protect both physical and digital assets from theft and damage.

22. Privacy
Implement a privacy program that ensures industry-recognized privacy practices are identified and operationalized throughout the lifecycle of systems, applications and services.

23. Project & Resource Management
Utilize a risk-based approach to prioritize the planning and resourcing of all security and privacy aspects for projects and other initiatives to alleviate foreseeable governance, risk and compliance roadblocks.

24. Risk Management
Govern a risk management capability that ensures risks are consistently identified, assessed, categorized and appropriately remediated.

25. Secure Engineering & Architecture
Implement secure engineering and architecture processes to ensure industry-recognized secure practices are identified and operationalized throughout the lifecycle of systems, applications and services.

26. Security Operations
Assign appropriately-qualified personnel to deliver security and privacy operations that provide reasonable protective, detective and responsive services.

27. Security Awareness & Training
Develop a security and privacy-minded workforce through ongoing user education about evolving threats, compliance obligations and secure workplace practices.

28. Technology Development & Acquisition
Govern the development process for any acquired or developed system, application or service to ensure secure engineering principles are operationalized and functional.

29. Third-Party Management
Implement ongoing third-party risk management practices to actively oversee the supply chain so that only trustworthy third-parties are used.

30. Threat Management
Identify, assess and remediate technology-related threats to assets and business processes, based on a thorough risk analysis to determine the potential risk posed from the threat.

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
Govern all Internet-facing technologies to ensure those systems, applications and services are securely configured and monitored for anomalous activity.

While a CISO/CIO/CPO can stop at the domain level to target CMM levels, it is expected that they or their subordinates go through each of the corresponding SCF controls to then tag each control with the appropriate target CMM level. These control targets can then be assigned to managers and Individual Contributors (IC) to develop operational plans to reach those goals. Ideally, a quarterly status review is conducted to oversee the progress made towards reaching the target CMM levels.

[3] *Customize The SCF - https://www.securecontrolsframework.com/customize-the-scf*

© 2022. Secure Controls Framework Council, LLC. All Rights Reserved.
This guide is for educational purposes only. You are encouraged to work with a cybersecurity, privacy or audit professional to validate any compliance-related assumptions.

USE CASE #2 – ASSIST PROJECT TEAMS TO APPROPRIATELY PLAN & BUDGET SECURE PRACTICES

When you consider regulations such as the EU General Data Protection Regulation (GDPR), there is an expectation for systems, applications and processes to identify and incorporate cybersecurity and privacy by default and by design. In order to determine what is appropriate and to evaluate it prior to "go live" it necessitates expectations for control maturity to be defined.

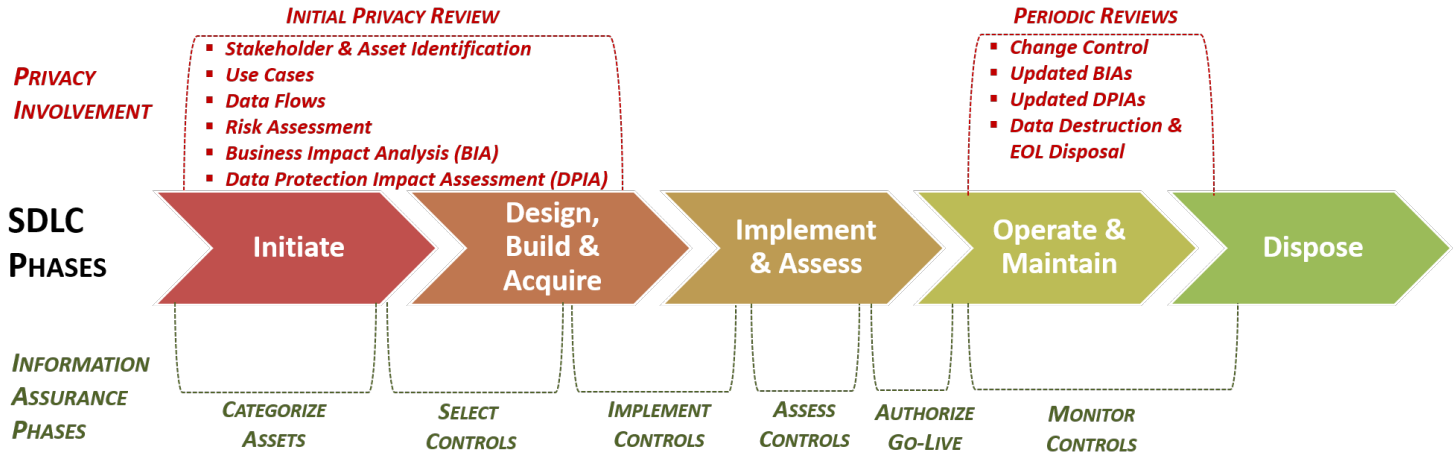
IDENTIFYING THE PROBLEM

In planning a project or initiative, it is important to establish "what right looks like" from security and privacy controls that must be implemented to address all compliance needs. This includes internal requirements, as well as external requirements from applicable laws, regulations and contracts. Prior planning of requirements can reduce delays and other costs associated with re-engineering.

CONSIDERATIONS

Referencing back to the SP-CMM Overview section of this document, CMM 0-1 levels of maturity are identified as being deficient from a "reasonable person perspective" in most cases. Therefore, project teams need to look at the "capability maturity sweet spot" between CMM 2-4 to identify the reasonable people, processes and technologies that need to be incorporated into the solution.

As previously-covered, avoiding negligent behavior is a critical consideration. The most common constraints that impact a project's maturity are: (1) budget and (2) time. A System Development Life Cycle (SDLC) has constraints and the expectations are that security and privacy controls are applied throughout the SDLC.



Projects do not have unlimited budgets, nor do they tend to have overly flexible timelines that allow for new security & privacy tools to be installed and trained upon. From a project perspective, this is often going to limit target CMM levels to CMM 2-3 for planning purposes.

IDENTIFYING A SOLUTION

While there are over 1,000 controls in the SCF's controls catalog, it is necessary for a project team to pare down that catalog to only what is applicable to the project (e.g., ISO 27002, PCI DSS, CCPA, etc.). This step simply involves filtering out the controls in the SCF that are not applicable and it can be easily done on the Customize The SCF page on the SCF website.[4] Additionally, this step can also be done within Excel or within a GRC solution. In the end, the result is a tailored set of controls that meet the project's specific needs.

Now that you have pared down the SCF's controls catalog to only what is applicable, it is a manual review process to identify the appropriate level of maturity for each of the controls. Ideally, the project will inherit the same target maturity level for controls as used throughout the organization. For any deviations, based on budget, time or other constraints, a risk assessment should be conducted to ensure a lower level of maturity for project-specific controls is appropriate.

[4] *Customize The SCF - https://www.securecontrolsframework.com/customize-the-scf*

© 2022. Secure Controls Framework Council, LLC. All Rights Reserved.
This guide is for educational purposes only. You are encouraged to work with a cybersecurity, privacy or audit professional to validate any compliance-related assumptions.

USE CASE #3 – PROVIDE OBJECTIVE CRITERIA TO EVALUATE THIRD-PARTY SERVICE PROVIDER SECURITY

It is now commonplace for Third-Party Service Providers (TSPs), including vendors and partners, to be contractually bound to implement and manage a baseline set of cybersecurity and privacy controls. This necessitates oversight of TSPs to ensure controls are properly implemented and managed.

IDENTIFYING THE PROBLEM

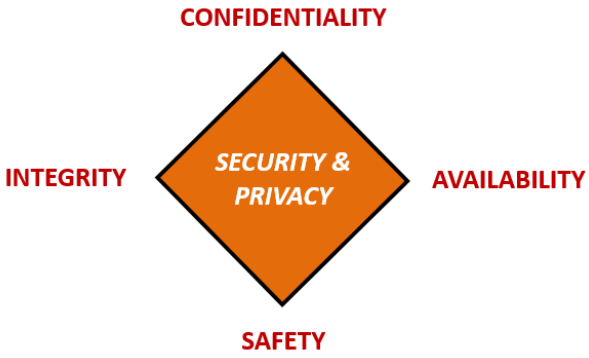
In managing a cybersecurity and privacy program, it is important to address controls in a holistic manner, which includes governing the supply chain. TSPs are commonly considered the "soft underbelly" for an organization's security program, since TSP oversight has traditionally been weak or non-existent in most organizations. There have been numerous publicized examples of TSPs being the source of an incident or breach.

One of the issues with managing TSPs is most questionnaires ask for simple yes, no or not applicable answers. This approach lacks details that provide critical insights into the actual security posture of the TSP. The SP-CMM can be used to obtain more nuanced answers from TSPs by having those TSPs select from CMM 0-5 to answer if the control is implemented and how mature the process is.

CONSIDERATIONS

Referencing back to the SP-CMM Overview section of this document, CMM 0-1 levels of maturity are identified as being deficient from a "reasonable person perspective" in most cases. Therefore, organizations need to look at the "capability maturity sweet spot" between CMM 2-4 to identify the reasonable people, processes and technologies that need TSPs need to be able to demonstrate to properly protect your systems, applications, services and data, regardless of where it is stored, transmitted or processed. From a TSP management perspective, this is often going to limit target CMM levels to CMM 2-3 for most organizations.

TSP controls are expected to cover both your internal requirements, as well as external requirements from applicable laws, regulations and contracts. Using the SP-CMM can be an efficient way to provide a level of quality control over TSP practices. Being able to demonstrate proper cybersecurity and privacy practices is built upon the security principles of protecting the confidentiality, integrity, availability and safety of your assets, including data.



IDENTIFYING A SOLUTION

While there are over 1,000 controls in the SCF's controls catalog, it is necessary to pare down that catalog to only what is applicable to that specific TSP's scope of control (e.g., Managed Service Provider (MSP), Software as a Service (SaaS) provider, etc.). This step simply involves filtering out the controls in the SCF that are not applicable and it can be easily done on the Customize The SCF page on the SCF website.[5] Additionally, this step can also be done within Excel or within a GRC solution. In the end, the result is a tailored set of controls that address the TSP's specific aspects of the cybersecurity & privacy controls that it is responsible for or influences.

Now that you have pared down the SCF's controls catalog to only what is applicable, it is a manual review process to identify the appropriate level of maturity for each of the controls that would be expected for the TSP. Ideally, the TSP will inherit the same target maturity level for controls as used throughout the organization. For any deviations, based on contract clauses, budget, time or other constraints, a risk assessment should be conducted to ensure a lower level of maturity for TSP-specific controls is appropriate.

[5] *Customize The SCF - https://www.securecontrolsframework.com/customize-the-scf*

© 2022. Secure Controls Framework Council, LLC. All Rights Reserved.
This guide is for educational purposes only. You are encouraged to work with a cybersecurity, privacy or audit professional to validate any compliance-related assumptions.