SECURE CONTROLS FRAMEWORK

# SECURE CONTROLS FRAMEWORK (SCF) RECOMMENDED PRACTICES

version 2021.1

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

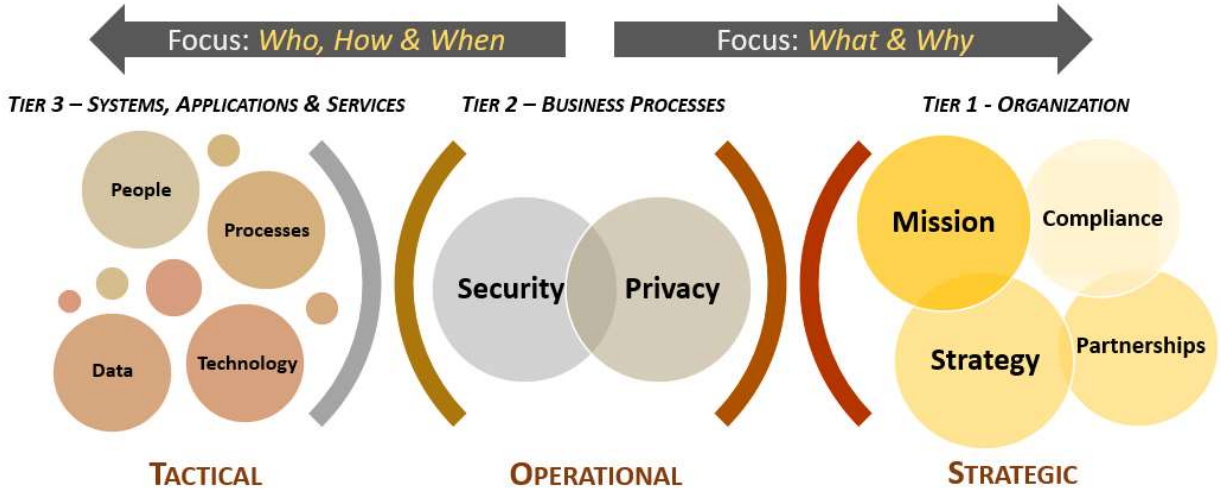


NOTE - This guide is for educational purposes only. You are highly encouraged to work with a cybersecurity, privacy or audit professional to validate any compliance-related assumptions.

## EXECUTIVE SUMMARY

The Secure Controls Framework™ (SCF) focuses on internal controls. These are the cybersecurity and privacy-related policies, standards, procedures and other processes that are designed to provide reasonable assurance that business objectives will be achieved and undesired events will be prevented, detected and corrected.

Using the SCF should be viewed as a long-term tool to not only help with compliance-related efforts but to ensure security and privacy principles are properly designed, implemented and maintained. The SCF helps implement a holistic approach to protecting the Confidentiality, Integrity, Availability and Safety (CIAS) of your data, systems, applications and other processes. The SCF can be used to assist with strategic planning down to tactical needs that impact the people, processes and technologies directly impacting your organization.




This "best practices" guide covers the following topics:

- Level setting what the SCF is and what it is not;
- Recommendations to tailor the control set for your needs;
- Leveraging the Security & Privacy Capability Maturity Model (SP-CMM); and
- Ways to operationalize the SCF.

This document is designed for cybersecurity & privacy practitioners to gain an understanding of how the SCF is intended to be used in their organization.

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.

## Section 1: Level Setting What The SCF Is and It Is Not

It is important for users of the SCF to understand what the SCF is and what it is not. We are very transparent on what the SCF offers and we want to help ensure that SCF users understand their role in using the SCF in their efforts to secure their organization.

### Why Should I Use The SCF?


There is no sales pitch for using the SCF – it is a free resource so there is no financial incentive for us to make companies use it. For companies that have just one 1-2 compliance requirements, the SCF might be considered overkill for your needs. However, for companies that have 3+ compliance requirements (e.g., organization that has requirements to address ISO 27002, SOC 2, PCI DSS and GDPR), then the SCF is a great tool to streamline the management of cybersecurity and privacy controls.

In developing the SCF, we identified and analyzed over 100 statutory, regulatory and contractual frameworks. Through analyzing these thousands of legal, regulatory and framework requirements, we identified commonalities and this allows several thousand unique controls to be addressed by the less than 750 controls that makeup the SCF. For instance, a requirement to maintain strong passwords is not unique, since it is required by dozens of laws, regulations and frameworks. This allows one well-worded SCF control to address multiple requirements. This focus on simplicity and sustainability is key to the SCF, since it can enable various teams to speak the same controls language, even though they may have entirely different statutory, regulatory or contractual obligations that they are working towards.

The SCF targets silos, since siloed practices within any organization are inefficient and can lead to poor security, due to poor communications and incorrect assumptions.

### What The SCF Is

The SCF is a comprehensive catalog of controls that is designed to enable companies to design, build and maintain secure processes, systems and applications. The SCF addresses both cybersecurity and privacy, so that these principles are designed to be "baked in" at the strategic, operational and tactical levels.

The SCF is:

- A control set.
- A useful tool to provide a "Rosetta Stone" approach to organizing cybersecurity and privacy controls so that the same controls can be used among companies and teams (e.g., privacy, cybersecurity, IT, project, procurement, etc.).
- Free for businesses to use. A result of a volunteer-led effort that uses "expert derived assessments" to perform the mapping from the controls to applicable laws, regulations and other frameworks.

The SCF also contains helpful guidance on possible tools and solutions to address controls. Additionally, it contains maturity criteria that can help an organization plan for and evaluate controls, based on a target maturity level.

### What The SCF Is Not

While the SCF is a comprehensive catalog of controls that is designed to enable companies to design, build and maintain secure processes, systems and applications, the SCF will only ever be a control set and is not a "magic bullet" technology solution to address every possible cybersecurity and privacy compliance obligation that an organization faces.

The SCF is not:

- A substitute for performing due care to understand your specific compliance needs.
- A complete technology or documentation solution to address all your security & privacy needs (e.g., the policies, standards, procedures and processes you need to have in place to be secure and compliant).
- Infallible or guaranteed to meet every compliance requirement your organization offers, since the controls are mapped based on expert-derived assessments to provide the control crosswalking that relies on human expertise and that is not infallible.

## Designing & Building An Audit-Ready Cybersecurity & Privacy Program

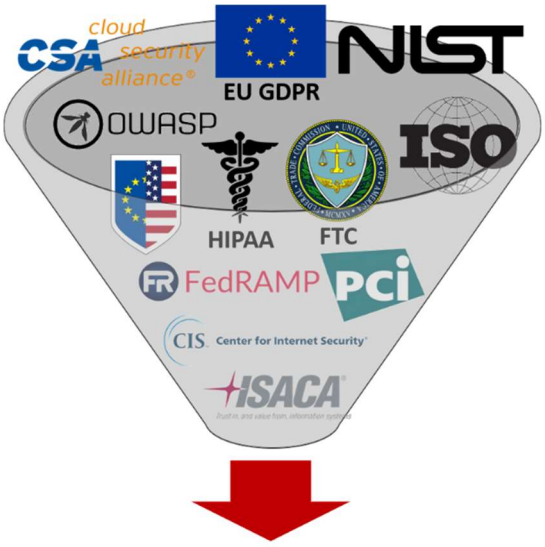

Building an audit-ready cybersecurity & privacy program requires addressing the holistic nature of security and privacy concerning how people, processes and technology impact security practices.

Building a security program that routinely incorporates security and privacy practices into daily operations requires a mastery of the basics. 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.

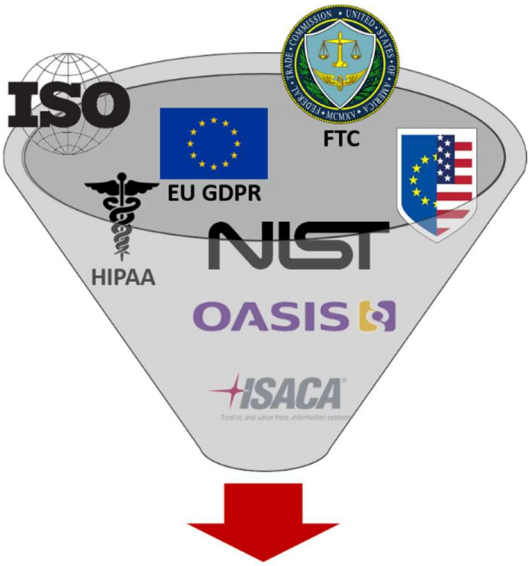
Once you master the fundamentals with LEGO®, it is easy to keep building and become immensely creative since you know how everything interacts. However, when the fundamentals are ignored, the LEGO® structure will be weak and include systemic flaws. Security and privacy really are not much different, 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 you envision each component that makes up a security or privacy "best practice" is a LEGO® block, it is possible to conceptualize 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!

Think of the SCF as a toolkit for you to build out your overall security program domain-by-domain so that cybersecurity and privacy principles are designed, implemented and managed by default!




**Security by Design (SbD)**




**Privacy by Design (PbD)**

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.

## SECTION 2: ADOPTING "SECURE BY DESIGN" PRINCIPLES

For an organization that just "does" ISO 27002, it is easy to say, "We're an ISO shop and we exclusively use ISO 27002 cybersecurity principles" and that would be routinely accepted as being adequate. However, what about companies that have complex cybersecurity and compliance needs, such as a company that has to address SOC2, ISO 27002, CCPA, EU GDPR, PCI DSS and NY DFS? In these complex cases that involve multiple frameworks, ISO 27002 principles alone do not cut it. This is why it is important to understand what secure principles your organization is aligned with, so that the controls it implements are appropriate to build secure and compliant processes. What works for one company or industry does not necessarily work for another, since requirements are unique to the organization.

Most companies have requirements to document security and privacy processes, but lack the knowledge and experience to undertake such documentation efforts. That means organizations are faced to either outsource the work to expensive consultants or they ignore the requirement and hope they do not get in trouble for being non-compliant. In either situation, it is not a good place to be.

### SECURE PRACTICES ARE COMMON EXPECTATIONS

While the European Union General Data Protection Regulation (EU GDPR) made headlines for requiring organizations to demonstrate security & privacy principles are by both "by default and by design," security & privacy engineering principles are not just limited to EU GDPR and are actually very common requirements:

- NIST 800-53 - **SA-8**
- NIST Cybersecurity Framework - **PR.IP-2**
- ISO 27002 - **14.2.5 & 18.1.4**
- Defense Federal Acquisition Regulations Supplement (DFARS) 252.204-7012 (NIST 800-171) - **3.13.1 & 3.13.2**
- Federal Acquisition Regulations (FAR) **52.204-21 - 4**
- National Industrial Security Program Operating Manual (NISPOM) - **8-302 & 8-311**
- ISACA Trust Services Criteria (TSC) (SOC 2) - **CC3.2**
- Generally Accepted Privacy Principles (GAPP) - **4.2.3, 6.2.2, 7.2.2 & 7.2.3**
- New York State Department of Financial Service (DFS) - **23 NYCRR 500.08**
- Payment Card Industry Data Protection Standard (PCI DSS) - **2.2**
- Center for Internet Security Critical Security Controls (CIS CSC) - **1.2, 5.9, 6.2, 6.3, 6.4, 6.5, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 8.6, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6, 11.4, 11.5, 11.6, 11.7, 13.4, 13.5 & 16.5**

### COMPLIANCE SHOULD BE VIEWED AS A NATURAL BYPRODUCT OF SECURE PRACTICES

It is vitally important for any SCF user to understand that compliant does not mean secure. However, if you design, build and maintain secure systems, applications and processes, then compliance will be a natural byproduct of those secure practices.


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 security & privacy principles to help an organization ensure that secure practices are implemented by design and by default.

You may be asking yourself, "What security & privacy principles should I be using?" and that is a great question. The SCF helped with this common question by taking the 32 domains of the SCF and creating principles that an organization can use. The idea is that by focusing on these secure principles, an organization will design, implement and maintain secure systems, applications and processes that will by default help the organization comply with its compliance obligations.

### SECURITY & PRIVACY BY DESIGN (S|P) PRINCIPLES

The concept of building security and privacy into technology solutions both by default and by design is a basic expectation for businesses, regardless of the industry. The adoption of security and privacy principles is a crucial step in building a secure, audit-ready program.

The S|P is a set of 32 security and privacy principles that leverage the SCF's extensive cybersecurity and privacy control set. You can download the free poster by clicking the image to the right.

The "S pipe P" logo is a nod to the computing definition of the | or "pipe" symbol (e.g., shift + backslash), which is a computer command line mechanism that allows the output of one process to be used as input to another process. In this way, a series of commands can be linked to more quickly and easily perform complex, multi-stage processing. Essentially, the concept is that security principles are being "piped" with privacy principles to create secure processes in an efficient 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.

## STEPS TO USE THE S|P PRINCIPLES

1. Read through the S|P principles to familiarize yourself with the 32 domains to understand how they come together to address the cybersecurity, privacy and physical security considerations for a modern security program.
2. Identify the applicable SCF controls that your organization needs to implement to address its applicable statutory, regulatory and contractual compliance needs.
3. Implement and monitor those SCF controls to ensure the S|P principles are being met by your day-to-day practices.

The S|P establishes 32 common-sense principles to guide the development and oversight of a modern security and privacy program. Those 32 S|P principles are listed below:

## SCF DOMAINS & S|P PRINCIPLES

**1) Security & Privacy Governance (GOV)**
- Principle: Govern a documented, risk-based program that encompasses appropriate security and privacy principles to address all applicable statutory, regulatory and contractual obligations.
- Intent: Organizations specify the development of an organization's security and privacy programs, including criteria to measure success, to ensure ongoing leadership engagement and risk management.

**2) Asset Management (AST)**
- Principle: Manage all technology assets from purchase through disposition, both physical and virtual, to ensure secured use, regardless of the asset's location.
- Intent: Organizations ensure technology assets are properly managed throughout the lifecycle of the asset, from procurement through disposal, ensuring only authorized devices are allowed to access the organization's network and to protect the organization's data that is stored, processed or transmitted on its assets.

**3) Business Continuity & Disaster Recovery (BCD)**
- Principle: Maintain the capability to sustain business-critical functions while successfully responding to and recovering from incidents through a well-documented and exercised process.
- Intent: Organizations establish processes that will help the organization recover from adverse situations with the minimal impact to operations, as well as provide the ability for e-discovery.

**4) Capacity & Performance Planning (CAP)**
- Principle: Govern the current and future capacities and performance of technology assets.
- Intent: Organizations prevent avoidable business interruptions caused by capacity and performance limitations by proactively planning for growth and forecasting, as well as requiring both technology and business leadership to maintain situational awareness of current and future performance.

**5) Change Management (CHG)**
- Principle: 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.
- Intent: Organizations ensure both technology and business leadership proactively manage change. This includes the assessment, authorization and monitoring of technical changes across the enterprise so as to not impact production systems uptime, as well as allow easier troubleshooting of issues.

**6) Cloud Security (CLD)**
- Principle: Govern cloud instances as an extension of on-premise technologies with equal or greater security protections than the organization's own internal controls.
- Intent: Organizations govern the use of private and public cloud environments (e.g., IaaS, PaaS and SaaS) to holistically manage risks associated with third-party involvement and architectural decisions, as well as to ensure the portability of data to change cloud providers, if needed.

**7) Compliance (CPL)**
- Principle: 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.
- Intent: Organizations ensure controls are in place to be aware of and comply with applicable statutory, regulatory and contractual compliance obligations, as well as internal company standards.

**8) Configuration Management (CFG)**
- Principle: Govern the establishment and ongoing management of secure configurations for systems, applications and services according to vendor-recommended and industry-recognized secure practices.
- Intent: Organizations establish and maintain the integrity of systems. Without properly documented and implemented configuration management controls, security features can be inadvertently or deliberately omitted or rendered inoperable, allowing processing irregularities to occur or the execution of malicious code.

9) **Continuous Monitoring (MON)**
   - Principle: Maintain situational awareness of security-related events through the centralized collection and analysis of event logs from systems, applications and services.
   - Intent: Organizations establish and maintain ongoing situational awareness across the enterprise through the centralized collection and review of security-related event logs. Without comprehensive visibility into infrastructure, operating system, database, application and other logs, the organization will have "blind spots" in its situational awareness that could lead to system compromise, data exfiltration, or unavailability of needed computing resources.
10) **Cryptographic Protections (CRY)**
   - Principle: 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.
   - Intent: Organizations ensure the confidentiality of the organization's data through implementing appropriate cryptographic technologies to protect systems and data.
11) **Data Classification & Handling (DCH)**
   - Principle: 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.
   - Intent: Organizations ensure that technology assets, both hardware and media, are properly classified and measures implemented to protect the organization's data from unauthorized disclosure, regardless if it is being transmitted or stored. Applicable statutory, regulatory and contractual compliance requirements dictate the minimum safeguards that must be in place to protect the confidentiality, integrity and availability of data.
12) **Embedded Technology (EMB)**
   - Principle: Provide additional scrutiny to the risks associated with embedded technology, based on the potential damages posed when used maliciously.
   - Intent: Organizations specify the development, proactive management and ongoing review of security embedded technologies, including hardening of the "stack" from the hardware, to firmware, software, transmission and service protocols used for Internet of Things (IoT) and Operational Technology (OT) devices.
13) **Endpoint Security (END)**
   - Principle: Harden endpoint devices to protect against reasonable threats to those devices and the data they store, transmit and process.
   - Intent: Organizations ensure that endpoint devices are appropriately protected from security threats to the device and its data. Applicable statutory, regulatory and contractual compliance requirements dictate the minimum safeguards that must be in place to protect the confidentiality, integrity, availability and safety considerations.
14) **Human Resources Security (HRS)**
   - Principle: Foster a security and privacy-minded workforce through sound hiring practices and ongoing personnel management.
   - Intent: Organizations create a security and privacy-minded workforce and an environment that is conducive to innovation, considering issues such as culture, reward and collaboration.
15) **Identification & Authentication (IAC)**
   - Principle: 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.
   - Intent: Organizations implement the concept of "least privilege" through limiting access to the organization's systems and data to authorized users only.
16) **Incident Response (IRO)**
   - Principle: 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).
   - Intent: Organizations establish and maintain a capability to guide the organization's response when security or privacy-related incidents occur and to train users how to detect and report potential incidents.
17) **Information Assurance (IAO)**
   - Principle: 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.
   - Intent: Organizations ensure the adequately of security and controls are appropriate in both development and production environments.
18) **Maintenance (MNT)**
   - Principle: Utilize secure practices to maintain technology assets, according to current vendor recommendations for configurations and updates, including those supported or hosted by third-parties.
   - Intent: Organizations ensure that technology assets are properly maintained to ensure continued performance and effectiveness. Maintenance processes apply additional scrutiny to the security of end-of-life or unsupported assets.

19) **Mobile Device Management (MDM)**
    - Principle: 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.
    - Intent: Organizations govern risks associated with mobile devices, regardless if the device is owned by the organization, its users or trusted third-parties. Wherever possible, technologies are employed to centrally manage mobile device access and data storage practices.
20) **Network Security (NET)**
    - Principle: Architect a defense-in-depth methodology that enforces the concept of "least functionality" through restricting network access to systems, applications and services.
    - Intent: Organizations ensure sufficient security and privacy controls are architected to protect the confidentiality, integrity, availability and safety of the organization's network infrastructure, as well as to provide situational awareness of activity on the organization's networks.
21) **Physical & Environmental Security (PES)**
    - Principle: Implement layers of physical security and environmental controls that work together to protect both physical and digital assets from theft and damage.
    - Intent: Organizations minimize physical access to the organization's systems and data by addressing applicable physical security controls and ensuring that appropriate environmental controls are in place and continuously monitored to ensure equipment does not fail due to environmental threats.
22) **Privacy (PRI)**
    - Principle: Implement a privacy program that ensures industry-recognized privacy practices are identified and operationalized throughout the lifecycle of systems, applications and services.
    - Intent: Organizations align privacy engineering decisions with the organization's overall privacy strategy and industry-recognized leading practices to secure Personal Information (PI).
23) **Project & Resource Management (PRM)**
    - Principle: 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.
    - Intent: Organizations ensure that security-related projects have both resource and project/program management support to ensure successful project execution.
24) **Risk Management (RSK)**
    - Principle: Govern a risk management capability that ensures risks are consistently identified, assessed, categorized and appropriately remediated.
    - Intent: Organizations ensure that security and privacy-related risks are visible to and understood by the business unit(s) that own the assets and / or processes involved. The security and privacy teams only advise and educate on risk management matters, while it is the business units and other key stakeholders who ultimately own the risk.
25) **Secure Engineering & Architecture (SEA)**
    - Principle: Implement secure engineering and architecture processes to ensure industry-recognized secure practices are identified and operationalized throughout the lifecycle of systems, applications and services.
    - Intent: Organizations align cybersecurity engineering and architecture decisions with the organization's overall technology architectural strategy and industry-recognized leading practices to secure networked environments.
26) **Security Operations (OPS)**
    - Principle: Assign appropriately-qualified personnel to deliver security and privacy operations that provide reasonable protective, detective and responsive services.
    - Intent: Organizations ensure appropriate resources and a management structure exists to enable the service delivery of cybersecurity operations.
27) **Security Awareness & Training (SAT)**
    - Principle: Develop a security and privacy-minded workforce through ongoing user education about evolving threats, compliance obligations and secure workplace practices.
    - Intent: Organizations develop a security and privacy-minded workforce through continuous education activities and practical exercises, in order to refine and improve on existing training.
28) **Technology Development & Acquisition (TDA)**
    - Principle: Govern the development process for any acquired or developed system, application or service to ensure secure engineering principles are operationalized and functional.
    - Intent: Organizations ensure that security and privacy principles are implemented into any products/solutions that are either developed internally or acquired to make sure that the concepts of "least privilege" and "least functionality" are incorporated.

29) **Third-Party Management (TPM)**
    - Principle: Implement ongoing third-party risk management practices to actively oversee the supply chain so that only trustworthy third-parties are used.
    - Intent: Organizations ensure that security and privacy risks associated with third-parties are minimized and enable measures to sustain operations should a third-party become defunct.
30) **Threat Management (THR)**
    - Principle: 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.
    - Intent: Organizations establish a capability to proactively identify and manage technology-related threats to the security and privacy of the organization's systems, data and business processes.
31) **Vulnerability & Patch Management (VPM)**
    - Principle: Utilize a risk-based approach to vulnerability and patch management practices that minimizes the attack surface of systems, applications and services.
    - Intent: Organizations proactively manage the risks associated with technical vulnerability management that includes ensuring good patch and change management practices are utilized.
32) **Web Security (WEB)**
    - Principle: Govern all Internet-facing technologies to ensure those systems, applications and services are securely configured and monitored for anomalous activity.
    - Intent: Organizations address the risks associated with Internet-accessible technologies by hardening devices, monitoring system file integrity, enabling auditing, and monitoring for malicious activities.

## SECTION 3: TAILORING THE SCF FOR YOUR NEEDS

Some people freak out and think they have to do all 740+ controls in the SCF and that is just not the case. It is best to visualize the SCF as a "buffet of cybersecurity and privacy controls," where there is a selection of 740+ controls available to you. You as you do not eat everything possible on a buffet table, the same applies to the SCF's control set. Once you know what is applicable to you, you can generate a customized control set that gives you just the controls you need to address your statutory, regulatory and contractual obligations.

### TAILORING IS REQUIRED - NOT ALL SCF CONTROLS ARE APPLICABLE TO YOUR ORGANIZATION

Understanding the requirements for both cybersecurity and privacy principles involves a simple process of distilling expectations. This process is all part of documenting reasonable expectations that are "right-sized" for an organization, since every organization has unique requirements.

The approach looks at the following spheres of influence to identify applicable SCF controls:

- Statutory Obligations - These are laws (e.g., US state, federal and international laws).
- Regulatory Obligations - These are requirements from regulatory bodies or governmental agencies.
- Contractual Obligations - These are requirements that are stipulated in contracts, vendor agreements, etc.
- Industry-Recognized Practices - These are requirements that are based on an organization's specific industry that are considered reasonably-expected practices.

### WHAT ARE YOUR APPLICABLE STATUTORY, REGULATORY AND CONTRACTUAL REQUIREMENTS?

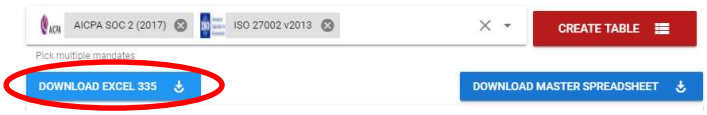
Please keep in mind that the SCF is a tool and it is only as good as its used – just like a pocketknife shouldn't be used as a prybar. Realistically, if you do not scope the controls from the SCF correctly, you will not address your applicable compliance requirements since you are missing what is expected. That is not a deficiency of the SCF – that is simply negligence on the part of the user of the tool.

To make sure scoping is done properly, it is imperative for you to speak with your legal, IT, project management, cybersecurity and procurement teams. The reason for this collaboration is so that you can get a complete picture of all the applicable laws, regulations and frameworks that your organization is legally obligated to comply with. Those teams will likely provide the best insights into what is required and that list of requirements then makes it simple to go through and customize the SCF for your specific needs!

In a basic example of how important scoping is please:

> Based on the business processes, vendor requirements and locations your organization operates, it has to comply with SOC 2 (ISACA TSC), Cloud Security Alliance Cloud Controls Matrix (CSA CCM), ISO 27002, ISO 29100, PCI DSS, Oregon Identity Theft Protection Act & the European Union General Data Protection Regulation (EU GDPR). The SCF helps pare this down 454 unique SCF controls that address the needs of those 7 laws, regulations and frameworks.
>
> However, if the user doing the scoping is unaware of the complete picture for the organization's obligations and only filters on SOC 2 and ISO 27002, there will only be 335 unique controls. While there will be a lot of overlap, in this specific case there are over 100 unique controls that are not being addressed. Without any type of follow-up internal or external audit processes that confirm the scoping of the controls, that error in mapping could lead to significant legal and financial exposure to the company from ignoring applicable controls it is obligated to perform.


Properly Scoped Example = 454 Controls




Improperly Scoped Example = 335 Controls

In this example listed above, the SCF worked just fine since it provided the controls that are applicable to the laws, regulations and frameworks selected by the user. What was broken is the organization's due diligence practices, where there was no clear oversight of the applicable cybersecurity and privacy requirements that the organization has to address. This is why knowing your organization's applicable statutory, regulatory and contractual obligations are vital to using the SCF (or any control set for that matter).

## CUSTOMIZING THE SCF: USE EXCEL TO MANUALLY FILTER CONTROLS

The SCF is fundamentally an Excel spreadsheet. Therefore, you can use your Excel skills to manually filter the requirements. If you are comfortable in Excel, it might take you 5-10 minutes to do this filtering, based on how many requirements you need to map to.

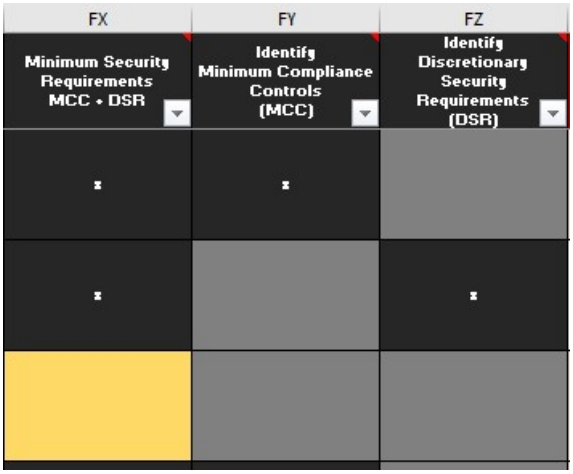
As previously mentioned, the Integrated Controls Management (ICM) model is a methodology that an organization can use categorize its applicable controls according to "must have" vs "nice to have" requirements:

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

There is a column that exists in the SCF to help with this task and is call the "Minimum Security Requirements (MSR) Filter" that will assist you in this process.

Follow these steps:

1. Either hide or delete all of the columns containing laws, regulations or frameworks that are not applicable to your organization (e.g., if you only have to comply with ISO 27002, PCI DSS and EU GDPR, then you can delete or hide all other mapping columns but those).
2. Using the filter option in Excel (little gray arrow on the top row in each column), you would then filter the columns to only show cells that contain content (e.g., don't show blank cells in that column).
3. In that **MCC column**, simply put an "x" to mark that control as being "must have" controls. In the **DSR column**, simply put an "x" to mark that control as being "nice to have" controls. A selection of either MCC or DSR will select MSR. Do this for all the rows shown in that column.
4. Unfilter the column you just performed this task on and do it to the next law, regulation or framework that you need to map.
5. Repeat step 3 and step 4 until all your applicable laws and regulations are mapped to.
6. The **MSR column** will now have an "x" that marks each SCF control that is applicable for your needs, based on what was selected for MCC and DSR controls.



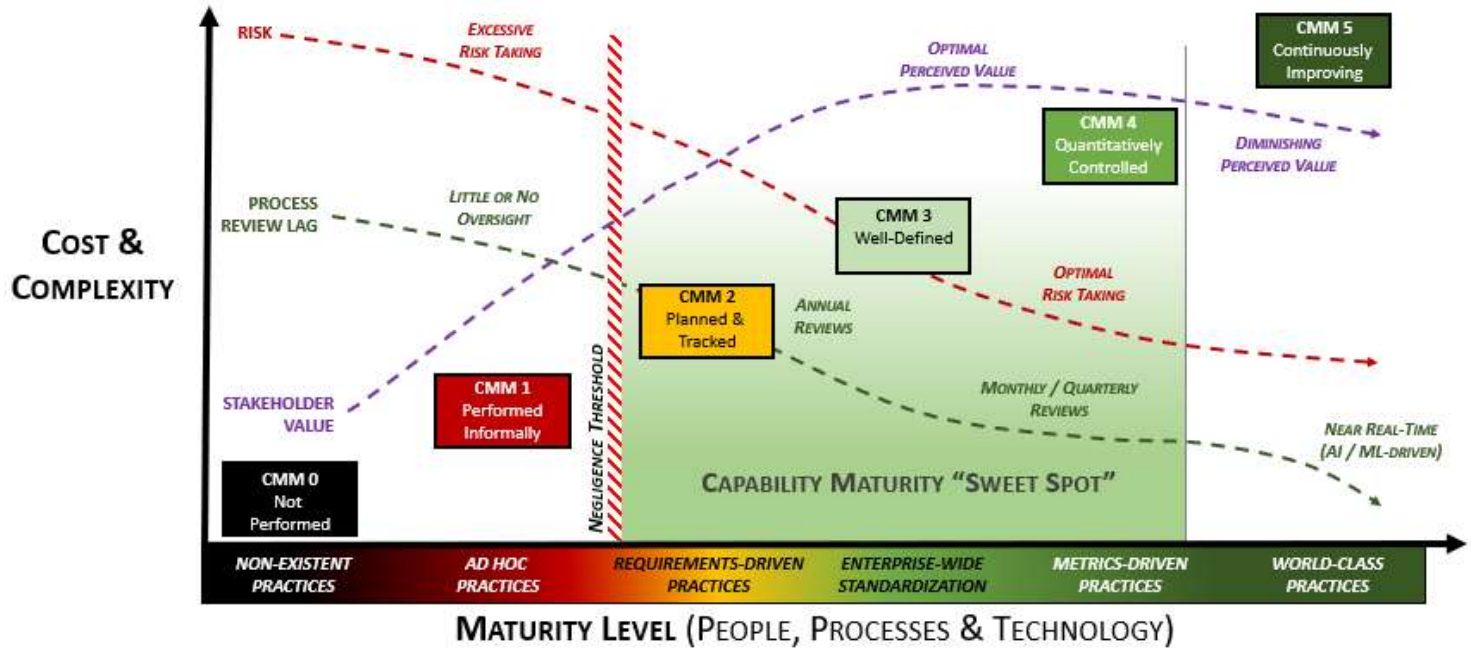

This will leave you with a SCF control set that is tailored for your specific needs.

## Section 4: Identifying A Target Maturity Level To Define What "Right" Looks Like

The SCF contains maturity criteria for its controls catalog to help organizations both build to and assess against quantifiable targets for maturity. 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.

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

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.




**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.

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).

*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.*

### 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.*

## Summary of CCM vs Organization Size Considerations

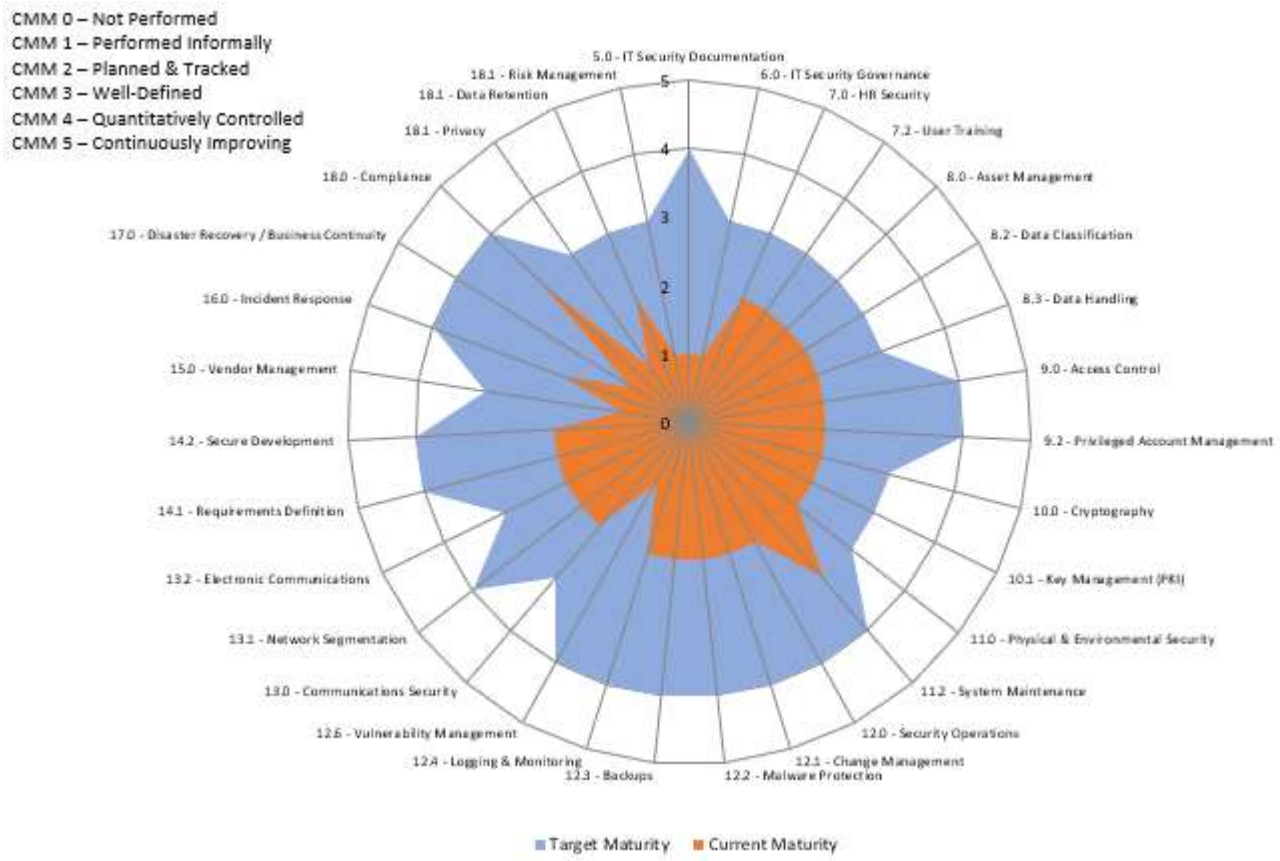
The following table summarizes the high-level expectations for small/medium/large organizations to meet each level of maturity.

| 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.<br>▪ [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.<br>▪ IT support is likely outsourced with a limited support contract.<br>▪ [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.<br>▪ Focus is on general IT operations without clear standards that implement secure systems and processes.<br>▪ [LIKELY NEGLIGENT] | |
| SP-CMM 2 | ▪ Internal IT role(s) has clear requirements and is supported to meet applicable cybersecurity / privacy compliance obligations; or<br>▪ 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.<br>▪ 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.<br>▪ 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.<br>▪ In addition to the existence of a dedicated cybersecurity team, there are specialists (e.g., engineers, SOC analysts, GRC analysts, privacy, etc.).<br>▪ 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.<br>▪ In addition to the existence of a dedicated cybersecurity team, there are specialists (e.g., engineers, SOC analysts, GRC analysts, privacy, etc.).<br>▪ 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.<br>▪ 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.<br>▪ In addition to the existence of a dedicated cybersecurity team, there are specialists (e.g., engineers, SOC analysts, GRC analysts, privacy, etc.).<br>▪ 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.<br>▪ 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.<br>▪ 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.<br>▪ 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. |

## SP-CMM 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.

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***

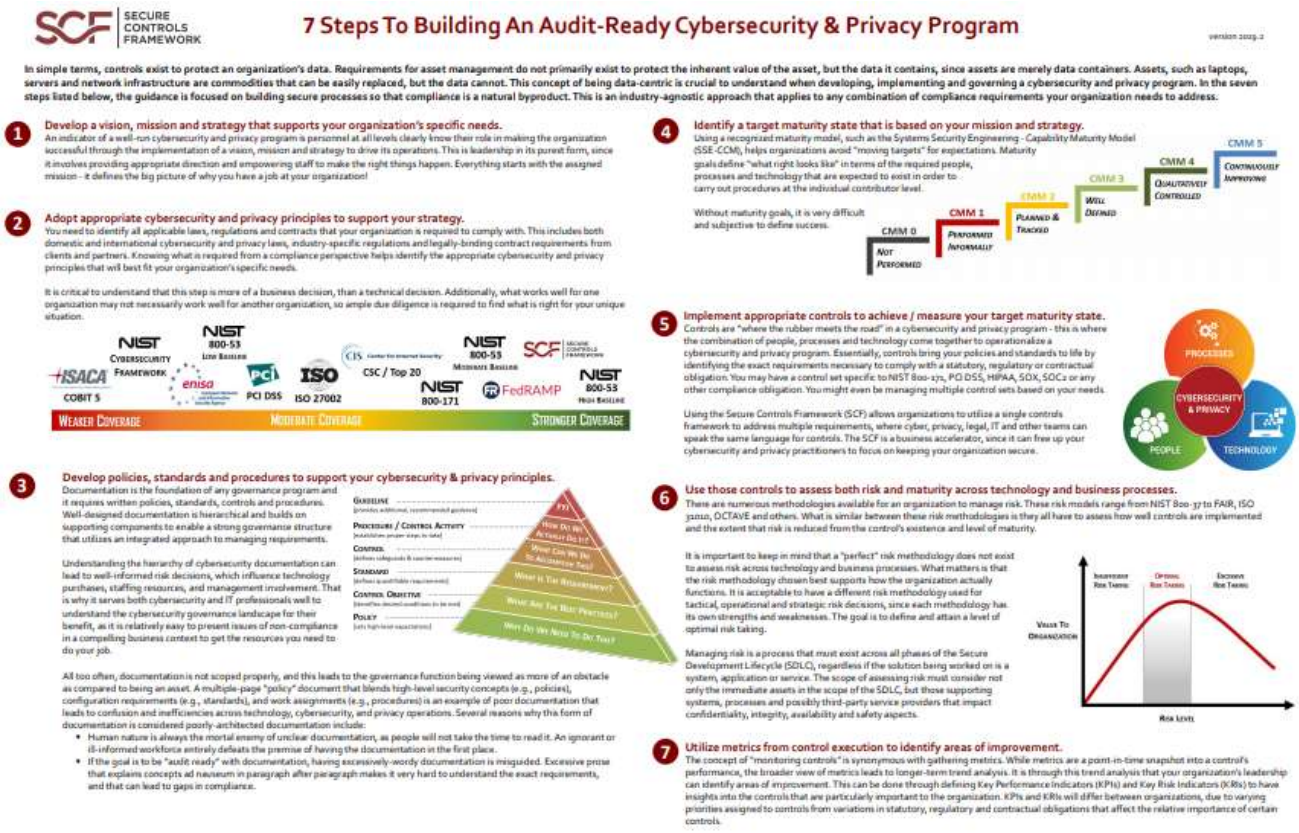
***that is in control or do you want to be in a controlled environment?"*** CMM 3 maturity is generally considered "an environment that is in control" where it is well-managed, whereas being in a CMM 4 environment is more of a "controlled environment" that is more controlled and less free. Given those 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*,"[1] 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.




[1] 7 Steps To Building An Audit-Ready Cybersecurity & Privacy Program - http://scf.securecontrolsframework.com/scf-security-privacy-by-design-principles.pdf

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.

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 ~750 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.[2] 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.


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.

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

## SP-CMM 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.

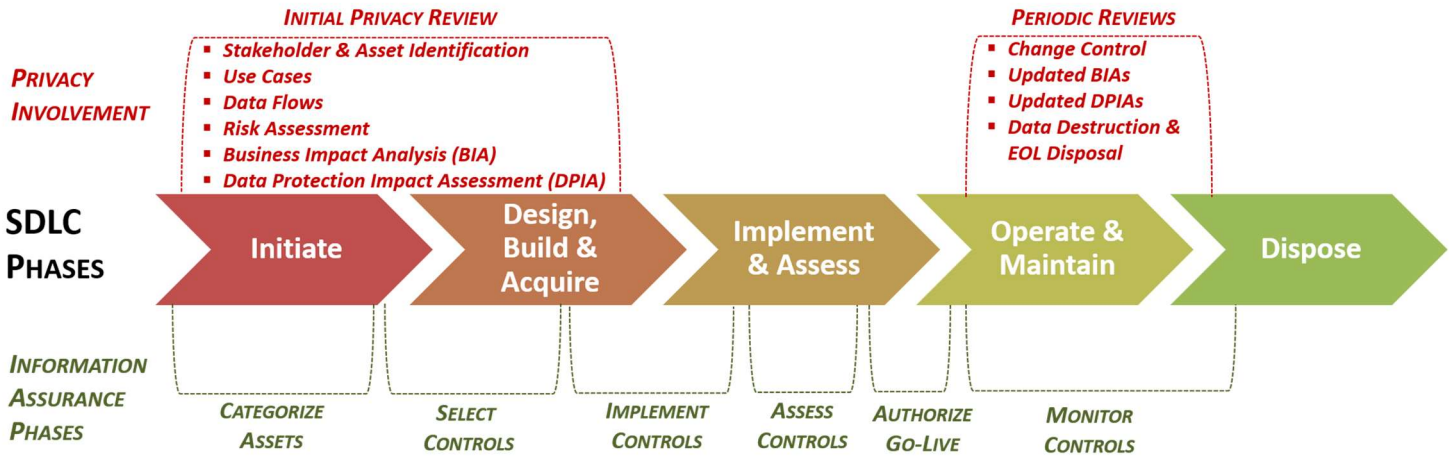
**Identifying The Problem**

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 ~750 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.[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 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.

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

## SP-CMM 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**

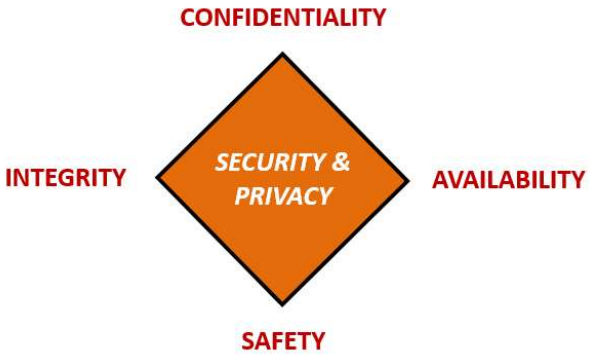
In managing a cybersecurity and privacy program, it is important to address controls in a holistic manner, which includes governing the supply chain. TSPs are commonly considered the "soft underbelly" for an organization's security program, since TSP oversight has traditionally been weak or non-existent 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 ~750 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.[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 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.

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

## SECTION 5: WAYS TO OPERATIONALIZE A CONTROL SET

We want companies to really get the maximum use from the SCF. We know that organizations from the Fortune 500 down to small businesses use the SCF, so it is very scalable and is flexible enough to support nearly any industry's cybersecurity and privacy needs.

The biggest issue comes down to the "Now what?" question, once an organization has a wonderful control set that provides a comprehensive list of their cybersecurity and privacy requirements.

### NOW WHAT? I'VE GOT A CONTROL SET, BUT WHAT DO I DO WITH IT?

If you are a small company with a limited budget and staff, it makes the most sense to work from the Excel version of the SCF. We've seen people import it into Microsoft Access databases and even turn it into internally-facing intranet webpages. This really comes down to the creativity and time you have to make it fit your needs.

For medium and large organizations, it really doesn't make sense to use Excel. This is where buying a Governance, Risk & Compliance (GRC) or Integrated Risk Management (IRM) solution makes the most sense.

- If you currently use a GRC/IRM, then your next step would be talking with your GRC/IRM admin to import the SCF into your instance.
- If you do not currently have a GRC/IRM but are in the process of getting one, your next step would be talking with the professional services or pre-sales engineering team about importing the SCF into your future instance.

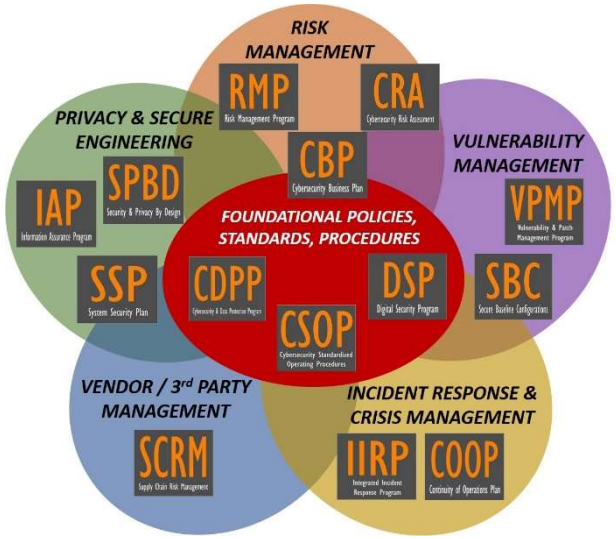
We've had SCF users report using the SCF with nearly all of the well-known GRC/IRM platforms, since it is expected for these tools to allow for the importing of a customized control set. Several of those GRC/IRM platforms are listed here:
https://www.securecontrolsframework.com/scf-solution-providers

### POLICIES, STANDARDS & PROCEDURES TO OPERATIONALIZE THE SCF

Now that you've got a set of controls, the missing piece in your cybersecurity and privacy documentation is going to be the policies, standards and procedures needed to fully operationalize the SCF. You can either write it yourself or buy it. ComplianceForge offers several products that directly map to the SCF:

- Digital Security Program (DSP) – policies, control objectives, standards, guidelines and metrics that have 1-1 mapping to the SCF.
- Cybersecurity Standardized Operating Procedures (CSOP) – procedures/control activities that have 1-1 mapping to the SCF.

ComplianceForge also offers near turnkey bundles of cybersecurity and privacy documentation that can further operationalize the SCF. These bundles are offered at significant discounts!




**ComplianceForge**
https://www.complianceforge.com
support@complianceforge.com
+1-855-205-8437