GETTING STARTED WITH THE SECURITY, COMPLIANCE & RESILIENCE PROGRAM (SCRP) & SECURE CONTROLS FRAMEWORK (SCF)

version 2026.1

Table of Contents

FOREWORD

Security + Compliance + Resilience needs to be a unified objective. This involves a multi-discipline approach to cybersecurity and data protection, so it requires involvement beyond just the cybersecurity department.

This approach signals that an organization isn't just protected, but it also meets its compliance requirements and can quickly bounce back from incidents.

ComplianceForge's Security, Compliance & Resilience Program (SCRP) has two goals:

1. Minimize an organization's attack surface; and
2. Enable the generation of "defensible evidence" of reasonable practices (e.g. evidence of due diligence and due care).

The SCRP directly supports an organization's ability to implement and maintain secure, compliant and resilient capabilities as described in the Secure Controls Framework (SCF) Security, Compliance & Resilience Management System (SCRMS).[1]

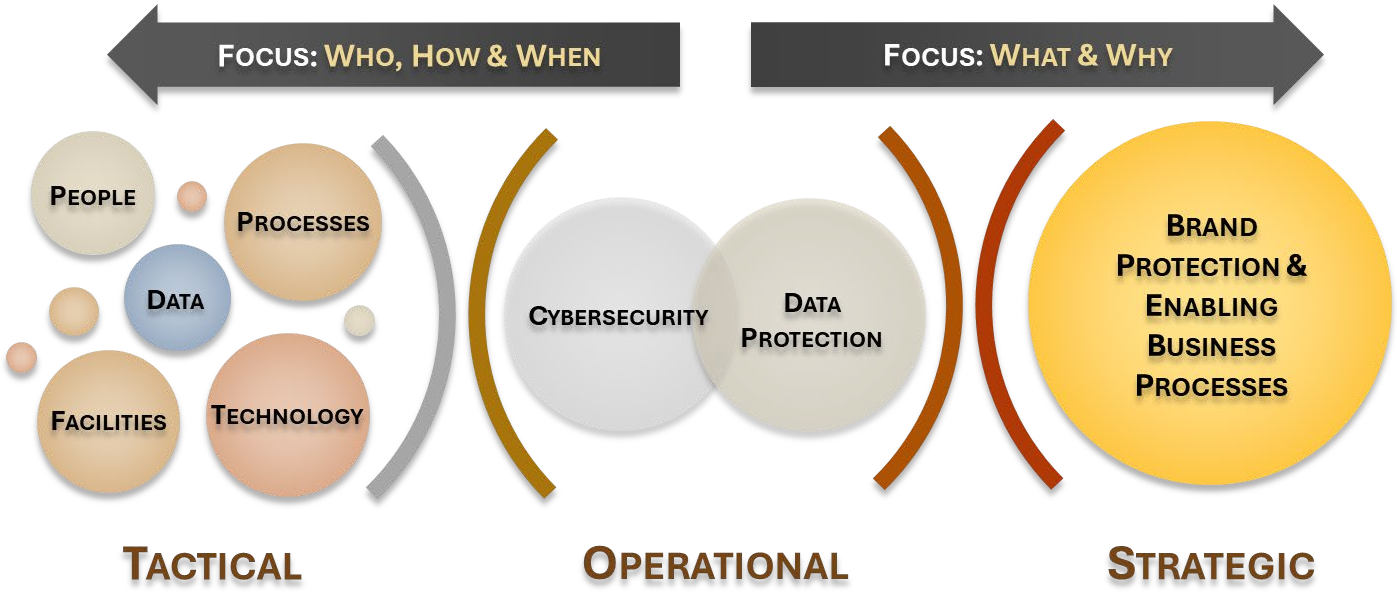
[1] *SCF SCRMS - https://securecontrolsframework.com/free-content/security-compliance-resilience-management-system-scrms*

Executive Summary

In order to help you maximize the value of the Security, Compliance & Resilience Program (SCRP), we want to properly orient you to the documentation you are receiving as part of this purchase, so that you can easily find what you are looking for.

Keep in mind the SCRP is a tool, so just like a hammer or screwdriver there are right ways and wrong ways to use it. We want you to build something great with this tool, so we are providing this guidance to help you on the right path. If you do get stuck or have some questions, please reach out to us at support@complianceforge.com since we are happy to help answer any product-related questions you have.

Using the SCRP 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 SCRP helps implement a holistic approach to protecting the Confidentiality, Integrity, Availability and Safety (CIAS) of your data, systems, applications and other processes. The SCRP can be used to assist with strategic planning down to tactical needs that impact the people, processes and technologies directly impacting your organization.



This document is designed for Cybersecurity & Data Privacy practitioners to gain an understanding of how the SCRP and SCF are intended to be used in their organization. The following topics are addressed:

- Level setting what the SCRP and Secure Controls Framework (SCF) are and what they are not;
- Recommendations to tailor the SCRP and SCF for your needs;
- Leveraging the Secure, Compliant & Resilient Capability Maturity Model (SCR-CMM); and
- Ways to operationalize the SCRP and SCF.

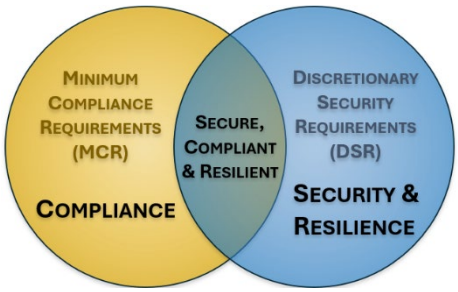
It is recommended that you start off with the following steps:

- Familiarizing yourself with the various documents listed below to gain a basic understanding of what they are (components are listed on the next page)
- Read through the ***"Security, Compliance & Resilience Management System (SCRMS) Overview"*** PDF to get an understanding for "what right looks like" from a documentation governance perspective since the structure described in the document is particular to how the SCRP was developed and how it is intended to be used for Governance, Risk & Compliance (GRC) operations (it is included in the supplemental documentation & graphics folder).
- From there, follow the steps in this guide to identify how to scope / customize the SCRP for your specific needs.

Defining What It Means To Be "Secure, Compliant & Resilient"

It is important to understand and clarify the difference between "compliant" versus "secure" since that is necessary to have coherent risk management discussions. To assist in this process, an organization needs to categorize its applicable controls according to "must have" vs "nice to have" requirements:

- **Minimum Compliance Requirements (MCR)** 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" MCR, 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.



Secure and compliant operations exist when both MCR and DSR are implemented and properly governed:

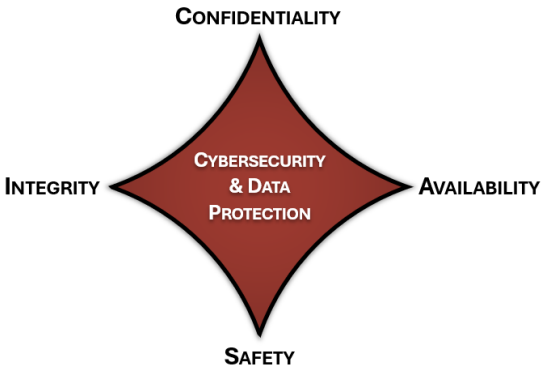
- MCR are primarily externally-influenced, based on industry, government, state and local regulations. MCR should never imply adequacy for secure practices and data protection, since they are merely compliance-related.
- DSR are primarily internally-influenced, based on the organization's respective industry and risk tolerance. While MCR establish the foundational floor that must be adhered to, DSR are where organizations often achieve improved efficiency, automation and enhanced security.

What Does It Mean To Be Secure?

An entity can reasonably claim it is secure if it has implemented and operational defenses focused on Confidentiality, Integrity, Availability and Safety (CIAS). An entity's level of security is dynamic, based on its:

1. Implemented defensive capabilities; and
2. Applicable risks and threats.

Effective security requires a unified effort involving those that interact with the entity's Technology Assets, Applications, Services and/or Data (TAASD). Commensurate with applicable risk and threats, cybersecurity and data protection measures must be implemented to guard against unauthorized access to, alteration, disclosure or destruction of TAASD. This also includes protection against accidental loss or destruction. The protection of TAASD must include safeguards to offset possible threats, as well as controls to ensure confidentiality, integrity, availability and safety.



- **Confidentiality** addresses preserving authorized restrictions on access and disclosure to authorized users and services, including means for protecting personal data privacy and proprietary information.
- **Integrity** addresses protecting against improper modification or destruction, including ensuring non-repudiation and authenticity.
- **Availability** addresses timely, reliable access to data, systems and services for authorized users, services and processes.
- **Safety** addresses reducing risk associated with technologies that could fail or be manipulated by nefarious actors to cause death, injury, illness, damage to or loss of equipment.

What Does It Mean To Be Compliant?

An entity can reasonably claim it is compliant if it has the ability to demonstrate conformity with applicable laws, regulations and other obligations. The scope of compliance includes both external and internal requirements.

What Does It Mean To Be Resilient?

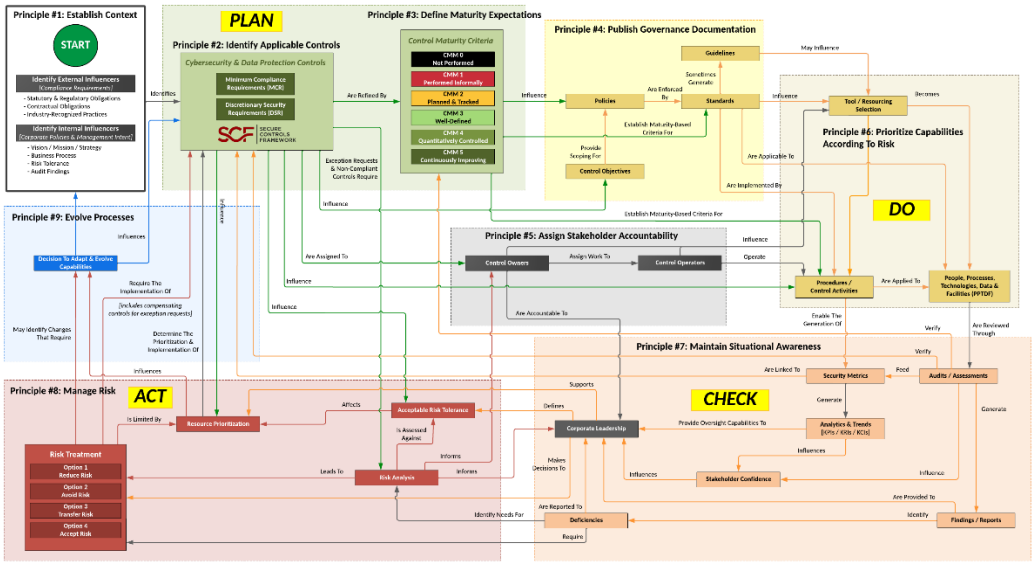
An entity can reasonably claim it is resilient if it has prepared for and has the ability to adapt to changing conditions, where it can withstand and/or recover rapidly from disruption.

Resilience includes the ability to withstand and recover from deliberate attacks, accidents or naturally occurring threats or incidents.

ComplianceForge helped develop the Security, Compliance & Resilience Management System (SCRMS) model to help streamline the traditional "governance, risk management & compliance" functions. There are eight (8) principles associated with SCRMS:

1. Establish Context
2. Identify Applicable Controls
3. Define Maturity Expectations
4. Publish Governance Documentation
5. Assign Stakeholder Accountability
6. Prioritize Capabilities According To Risk
7. Maintain Situational Awareness
8. Manage Risk
9. Evolve Processes

The SCRMS is very much worth your time to familiarize yourself with: https://securecontrolsframework.com/free-content/security-compliance-resilience-management-system-scrms



[graphic can be downloaded from https://complianceforge.com/content/pdf/scrms-plan-do-check-act.pdf]

People, Processes, Technology, Data & Facilities (PPTDF) Control Applicability

Control scoping does not mean all controls apply uniformly to every asset, individual or facility. This misunderstanding of applicability vs scoping is one of the biggest hurdles that organizations face, since there is a common misconception that if something is "in scope" then every control will be applicable across the entire boundary of the assessment. This is an incorrect assumption. When looking at the breath of controls that an organization is obligated to comply with, the controls are often administrative, technical or physical in nature. This means that there may be controls that are not applicable to certain systems, applications and/or processes.

Example 1: Network firewall

- A network firewall is a technical control, where certain other controls would be applicable, such as Multi-Factor Authentication (MFA), access control, secure baseline configurations and patch management.
- Since a network firewall is a device, it not capable of having end user training, completing a Non-Disclosure Agreement (NDA) or conducting incident response exercises.

Example 2: User awareness training

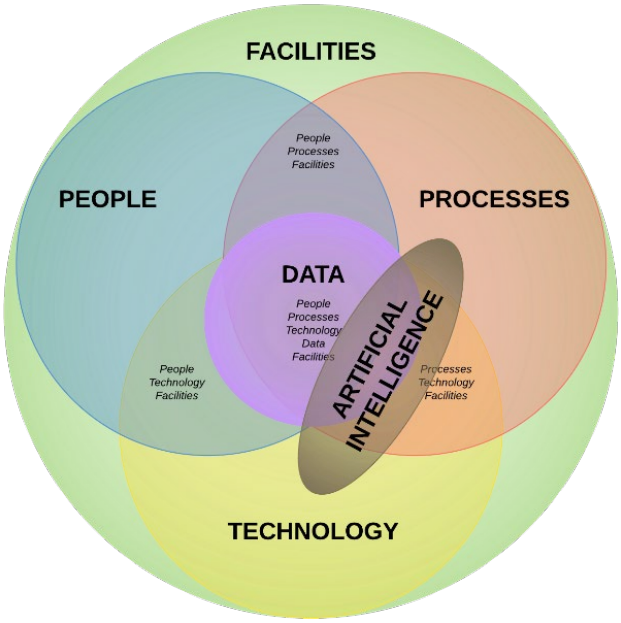
- User awareness training is focused on personnel, such as employees and applicable third-parties who will be interacting with the organization's systems and data. NDAs, threat intelligence awareness, acceptable use notifications are all applicable to individuals.
- Since an individual is not a device, an individual is not capable of having a secure baseline configuration applied, be scanned by a vulnerability assessment tool, or have missing patches installed.

Example 3: Incident Response Plan (IRP)

- An IRP is a documented process that is a tool to be used to guide incident response operations.
- Since an IRP is a not an individual or technology, it cannot sign a NDA, have MFA or be patched.

The People, Processes, Technology, Data and Facilities (PPTDF-AI) model provides a comprehensive approach to address control applicability. These six (6) components provide a lens to view the applicability of controls.

- People - A "people" control is primarily applied to humans (e.g., employees, contractors, third-parties, etc.)
- Process - A "process" control is primarily applied to a manual or automated process.
- Technology - A "technology" control is primarily applied to a system, application and/or service.
- Data - A "data" control is primarily applied to data (e.g., CUI, CHD, PII, etc.).
- Facility - A "facility" control is primarily applied to a physical building (e.g., office, data center, warehouse, home office, etc.)
- Artificial Intelligence (AI). AI and autonomous technologies applies across technologies, processes and data.



Documentation Included In The SCRP

The following documentation is part of the SCRP:

Word Documents

- **Security, Compliance & Resilience Program (SCRP)**
  - This is the core SCRP in Microsoft Word format that contains the policies, control objectives, standards and guidelines.

- **SCRP Supplemental - Annexes Forms & References** o This contains a lot of useful templates and references.
  - Most important in this document are the Annexes that provide invaluable information to implement and maintain the SCRP:
    - Annex 1: Data Classification & Handling Guidelines
    - Annex 2: Data Classification Examples
    - Annex 3: Data Retention Periods
    - Annex 4: Baseline Security Categorization Guidelines
    - Annex 5: Rules of Behavior (Acceptable & Unacceptable Use)
    - Annex 6: Guidelines for Personal Use of Organizational IT Resources
    - Annex 7: Risk Management Framework (RMF)
    - Annex 8: System Hardening
    - Annex 9: Safety Considerations With Embedded Technology
    - Annex 10: Indicators of Compromise (IoC)

- **SCRP Supplemental – Educational Reference On SCRP Policies**
  - This is an optional reference/tool that you can use to help educate users on the SCRP's policies.
  - The intent is this can be used as a handout or made into an Intranet webpage to educate all users on the policies.

- **SCRP Supplemental - Cybersecurity Roles & Responsibilities**
  - This is an optional reference for cybersecurity and privacy roles & responsibilities.
  - This is based on the NIST NICE Cybersecurity Workforce Framework, the closest thing to a "best practice" for roles and responsibilities.

- **Errata – SCRP**
  - This document contains version change information (errata).

Excel Document

- **Security, Compliance & Resilience Program (SCRP) - Framework Mapping**
  - This Excel spreadsheet contains multiple tabs and is where you will find the mapping from the SCRP to other frameworks.
  - The most important tabs to familiar yourself with are:
    - SCRP Domains & Principles
    - Authoritative Sources
    - SCRP Framework Mapping
    - Metrics, KRIs & KPIs

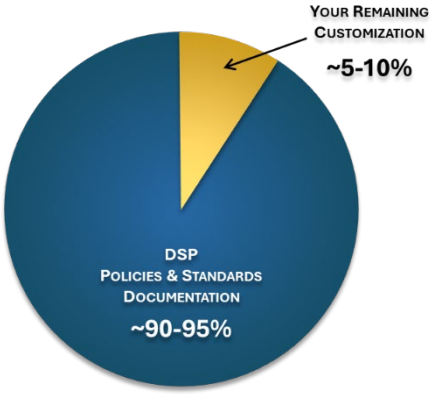
PowerPoint Documents

- Cybersecurity Awareness Training o This is an optional reference that can be used to build a training presentation.
- Data Classification Icons o This contains editable data classification icons.

SECTION 1: UNDERSTANDING THE SCRP

The **Security, Compliance & Resilience Program (SCRP)** is a template that is meant to provide the foundation for your cybersecurity program by consolidating your cybersecurity policies, control objectives, standards and guidelines into one document. This makes managing your cybersecurity documentation more efficient by reducing "boilerplate text" and also is much easier for users to find the information they are looking for, as compared to searching multiple, standalone policy documents.

Given the difficult nature of writing templated policies and standards, we aimed for approximately a "90 to 95% solution" since we feel that **customization is absolutely necessary to make it specific to your organization's needs**. The reason for that is pretty clear - every organization has different compliance requirements, available resources, technologies in use, and a unique corporate culture so no one set of templatized policies and standards can be 100% equally applied across multiple organizations.



ComplianceForge did the heavy lifting and it is up to you, as the client, to provide the final customization that is necessary to make it specific to your organization.

UNDERSTANDING THE TERMINOLOGY OF THE SCRP

Cybersecurity, IT professionals and legal professionals routinely abuse the terms "policy" and "standard" as if these words are synonymous. In reality, these terms have quite different implications, and those differences should be kept in mind since the use of improper terminology has cascading effects that can negatively impact the internal controls of an organization.

con·trol / kən'trōl – *According to ISACA, "internal controls" include the policies, standards, procedures and other organizational structures that are designed to provide reasonable assurance that business objectives will be achieved and undesired events will be prevented, detected and corrected. Essentially, governance over these controls is the power to influence or direct people's behavior or the course of events.*

WHY YOU SHOULD CARE ABOUT TERMINOLOGY

Governance is built on words. Beyond just using terminology properly, understanding the meaning of these concepts is crucial in being able to properly implement cybersecurity and privacy governance within an organization. An indicator of a well-run governance program is the implementation of hierarchical documentation since it involves bringing together the right individuals to provide appropriate direction based on the scope of their job function.

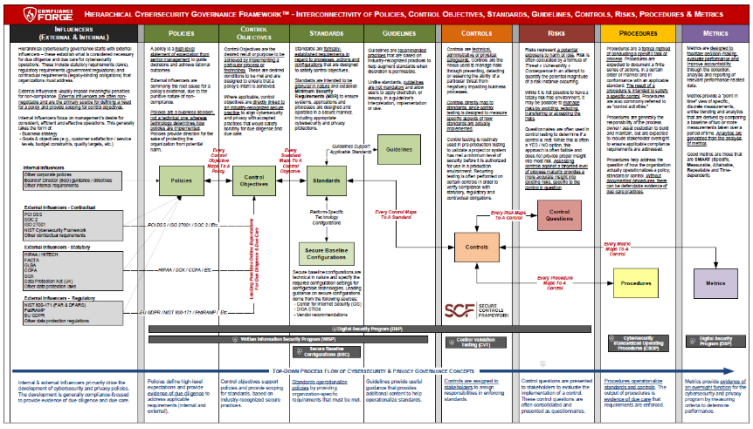
To help visualize that concept, imagine the board of directors of your organization publishing procedural process guidance for how a security analyst performs daily log review activities. Most would agree that such a scenario is absurd since the board of directors should be focused on the strategic direction of the company and not day-to-day procedures.

However, in many organizations, the inverse occurs where the task of publishing the entire range of cybersecurity documentation is delegated down to individuals who might be competent technicians but do not have insights into the strategic direction of the organization. This is where the concept of hierarchical documentation is vitally important since there are strategic, operational, and tactical documentation components that have to be addressed to support governance functions.

Please reference the **Understanding Key Terminology Section** to better understand the leading practices' definitions of policies, standards, controls, etc. That understanding is useful when viewing how the SCRP is created to make a scalable, hierarchical solution for cybersecurity and privacy documentation.

Hierarchical Cybersecurity Governance Framework (HCGF)

ComplianceForge Hierarchical Cybersecurity Governance Framework™ (HCGF) takes a comprehensive view towards the necessary documentation components that are key to being able to demonstrate evidence of due diligence and due care. This framework addresses the interconnectivity of policies, control objectives, standards, guidelines, controls, risks, procedures & metrics. The Secure Controls Framework (SCF) fits into this model by providing the necessary cybersecurity and privacy controls an organization needs to implement to stay both secure and compliant.



ComplianceForge has simplified the concept of the hierarchical nature of cybersecurity and privacy documentation in the following downloadable diagram to demonstrate the unique nature of these components, as well as the dependencies that exist.

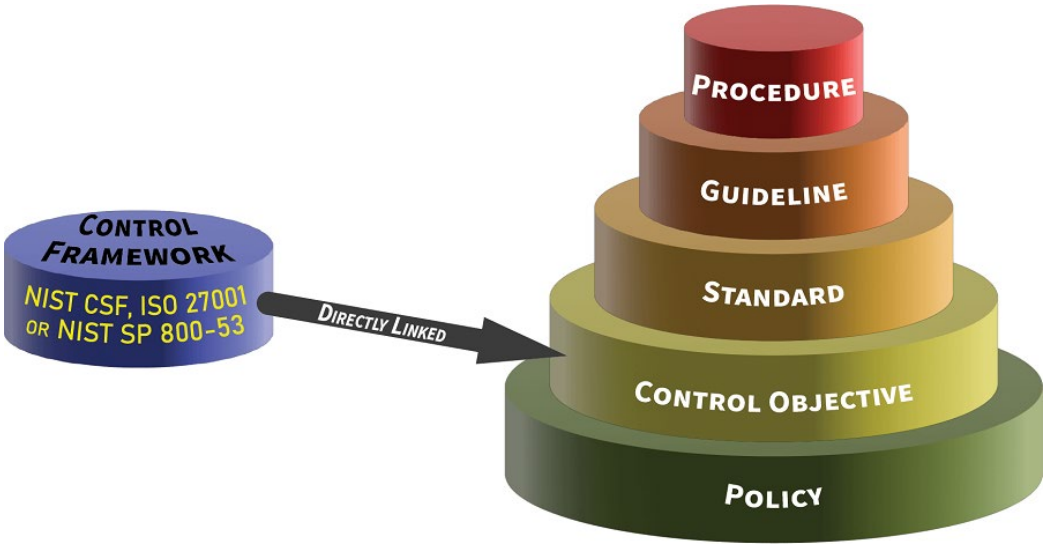
A picture is sometimes worth 1,000 words – this concept can be seen here the swim lane diagram shown on the right. This is also included in the "supplemental documentation" folder.

What "Right" Looks Like

Based on the hierarchical nature of documentation as shown in the HCGF, we believe the most efficient form of cybersecurity and privacy documentation is scalable and concise. We avoid "rambling prose" that makes it difficult for users to find the exact requirements they are looking for, since it is both efficient and provides a more accurate answer for the user.

Well-designed documentation is generally comprised of six (6) main parts:

1. Policies establish management's intent;
2. Control Objectives identify leading practices (mapped to requirements from laws, regulations and frameworks);
3. Standards provide quantifiable requirements;
4. Controls identify desired conditions that are expected to be met (requirements from laws, regulations and frameworks);
5. Procedures / Control Activities establish how tasks are performed to meet the requirements established in standards and to meet controls; and
6. Guidelines are recommended, but not mandatory.



Note: Procedures are not a part of the SCRP, but are available as part of the Cybersecurity Standardized Operating Procedures (CSOP) product available through ComplianceForge.

What "Wrong" Looks Like

All too often, documentation is not scoped properly and this leads to the governance function being more of an obstacle, as compared to an asset. A multiple-page "policy" document that blends high-level security concepts (e.g., policies), configuration requirements (e.g., standards), and work assignments (e.g., procedures) is an example of poor governance documentation that leads to confusion and inefficiencies across technology, cybersecurity, and privacy operations.

Several reasons why this form of "policy" document is considered poorly-architected documentation include:

- Human nature is always the mortal enemy of unclear documentation, as people will not take the time to read it. An ignorant or ill-informed workforce entirely defeats the premise of having the documentation in the first place.
- If the goal is to be "audit ready" with documentation, having excessively-wordy documentation is misguided. Excessive prose that explains concepts ad nauseum in paragraph after paragraph makes it very hard to understand the exact requirements, and that can lead to gaps in compliance.

SECTION 2: HIGH-LEVEL STEPS TO USING THE SCRP

Note: For those new to the Secure Controls Framework (SCF), the Security, Compliance & Resilience Management System (SCRMS) is the source for how to build secure, compliant and resilient capabilities.[2] Additionally, the SCRMS-PIG is the operational companion to the SCRMS. It provides a sequenced, dependency-aware roadmap for implementing SCRMS capabilities in a way that:

- Supports the entity's mission and business practices;
- Avoids rework from implementing capabilities where dependencies exist that results in cascading failures from misaligned capabilities;
- Aligns funding and resources with business risk;
- Avoids systemic weaknesses by building foundational capabilities before chasing advanced capabilities; and
- Provides assurance to stakeholders through audit-ready evidence.

The steps below are recommended, based on years of helping companies implement ComplianceForge documentation products:

STEP 1: FAMILIARIZE YOURSELF WITH THE SCRP & SUPPLEMENTAL DOCUMENTATION

- Make a pot of coffee (or your beverage of choice) and start reading through the documentation at a HIGH LEVEL so you can familiarize yourself with the structure and content of the SCRP. There is no getting around this step.
- Within the Supplemental Documentation folder that comes with the SCRP, you will find several useful resources. Most importantly, you will find an Excel spreadsheet that contains a mapping from the SCRP's standards to leading frameworks. This spreadsheet will be important in the next step.

STEP 2: IDENTIFY ALL APPLICABLE COMPLIANCE REQUIREMENTS

- If you do no already have a crystal-clear understanding of the statutory, regulatory and contractual obligations that are applicable to your organization, set up a meeting with your procurement and legal experts since those two stakeholders generally know what requirements your organization is required to address.
- In the following section of this guide, there is a review on the differences between statutory, regulatory and contractual requirements. This is important, since it can help you prioritize your efforts.

STEP 3: IDENTIFY STANDARDS THAT DO NOT APPLY TO YOUR BUSINESS MODEL

- When you know what is applicable to your organization, it is also possible to identify all those other standards in the SCRP that might not currently be applicable to your organization.
- For all the standards that are not required for a business need (e.g., meeting a statutory, regulatory or contractual obligation), there are two main options:
  - Option 1: Delete the standard that is not applicable (NOTE - this is NOT the preferred method)
  - Option 2: Preface the standard that is not applicable to remove the standard from the general scope of requirements.
  - with a statement such as:
    - "As required to meet a business obligation, …"
    - "Where technically feasible, …"
    - "When sensitive/regulated data is being processed, stored and/pr transmitted, …"
- ComplianceForge's opinion is that Option 2 is the preferred method, based on these reasons:
  - If your requirements change, you simply remove the prefaced statement vs reworking the entire SCRP.
  - You maintain the structure and mapping of the SCRP and SCF.

STEP 4: CUSTOMIZE THE SCRP BASED ON YOUR UNIQUE NEEDS

- This is where you really get into the details to make the SCRP specific to your organization.
- The SCRP is an editable Word document – you can edit it for your needs.
- Given the understanding that out of the box the SCRP is not customized specific to your organization, there is an expectation that key stakeholders within your organization will want to review and make recommendations for edits to the SCRP.
- Reviewing and editing the policies and standards is just part of good cybersecurity governance.

[2] *SCF SCRMS - https://securecontrolsframework.com/free-content/security-compliance-resilience-management-system-scrms*

Step 5: Coordinate With Stakeholders For A Rollout

- Once the policies and standards are reviewed and accepted, the next hurdle is rolling out the SCRP.
- There are several options to rolling out the SCRP:
  - Option 1: Phased rollout (portions of the SCRP are made applicable over time)
  - Option 2: Direct rollover (at a certain date, the SCRP is effective and replaces existing policies & standards)
  - Option 3: Direct rollover with phased deadlines (similar to Option 2, but only "critical" standards are made effective immediately and a phased timeline for compliance with other standards is established, where those pending standards are viewed as guidance).
  - *Note: Generally, Option 2 is the most efficient and least-confusing way to roll out the SCRP.*
- A key point to remember is that the SCRP should not be seen as punitive. On the contrary, rolling out the SCRP should be seen as a benefit to technology teams to help justify budget for new technology, processes and/or personnel.
- With any rollout, any standard that cannot be complied with needs to have a risk assessment performed and someone needs to accept the risk associated with a standard not being met. This is a common governance process for evaluating requests for exceptions to standards.
- There should NEVER be an exception to a POLICY, just a STANDARD (*please review the section on terminology if that does not make sense*).

Step 6: Monitor & Made Changes As Needed

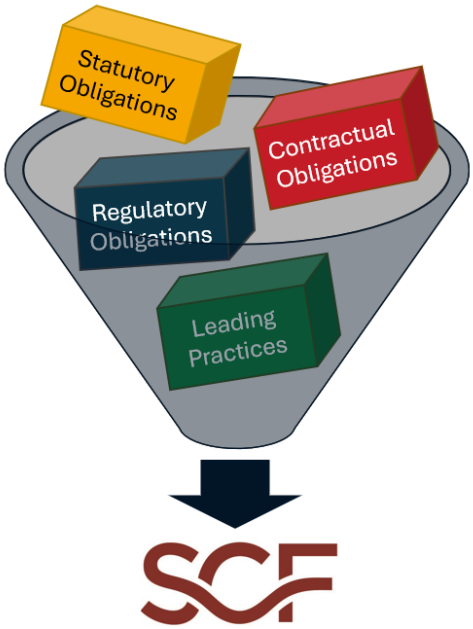
- There should be some form of annual review of policies and standards as part of your organization's governance process.
- Ideally, Key Performance Indicators (KPIs) or other metrics will be used as part of the evaluation process to understand what aspects are working well and others that need improvements.

Section 3: Understanding The SCF

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 diligence and due care to understand and manage your specific compliance needs.
- A complete technology or documentation solution to address all your cybersecurity & data 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 Security, Compliance & Resilience Program

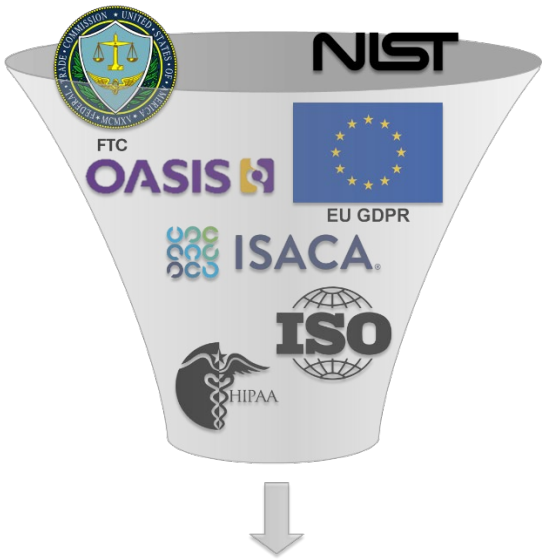
Building an audit-ready security, compliance and resilience program requires addressing the holistic nature of security and privacy concerning how people, processes and technology impact security practices.

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.

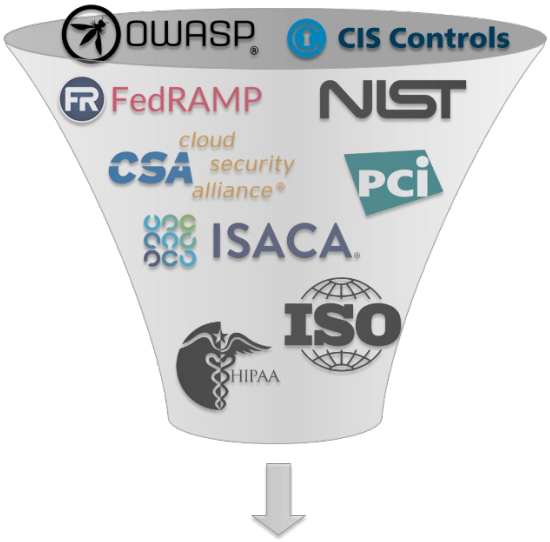
Once you master the fundamentals with LEGO®, it is easy to keep building and become immensely creative since you know how everything interacts. However, when the fundamentals are ignored, the LEGO® structure will be weak and include systemic flaws. Security and privacy really are not much different, 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!



Privacy by Design (PbD)



Security by Design (SbD)

SECTION 4: 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 cybersecurity & data 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 cybersecurity & data privacy principles are by both "by default and by design," Secure Engineering & Data Privacy (SEDP) principles are not just limited to EU GDPR. SEDP principles are actually common requirements in the constantly-evolving statutory and regulatory landscapes. The following are common statutory, regulatory and contractual requirements that expect SEDP practices:

- AICPA Trust Services Principles (ESP) (e.g., System and Organization Controls (SOC) 2 Type 1) – CC2.2, CC3.2, CC5.1 & CC5.2
- Cloud Computing Compliance Controls Catalogue (C5) – KOS-01 & KOS-07
- Criminal Justice Information Services (CJIS) Security Policy – 5.10.1.1 & 5.10.1.5
- COBIT 2019 – DSS06.06
- COSO 2017 – Principles 10 & 11
- European Union Agency for Network and Information Security (ENISA) Technical Guideline of Security Measures – SO12
- European Union General Data Protection Regulation (EU GDPR) – Art 5.2, 24.1, 24.2, 24.3, 25.1, 25.2, 25.3, 32.1, 32.2 & 40.2
- Federal Risk and Authorization Management Program (FedRAMP) – SA-8, SC-7(18) & SI-01
- Food & Drug Administration (FDA) 21 CFR Part 11 – §11.30
- Federal Trade Commission (FTC) Act - §45(a) & §45b(d)(1)
- Generally Accepted Privacy Principles (GAPP) – 4.2.3, 6.2.2, 7.2.2 & 7.2.3
- Health Insurance Portability and Accountability Act (HIPAA) - 164.306, 164.308, 164.312, 164.314 & 164.530
- ISO 27002:2013 – 8.3.2
- ISO 27018 – A.10.1, A.10.4, A.10.5 & A.10.6
- ISO 29100 – 5.10 & 5.11
- National Industry Security Program Operating Manual (NISPOM) – 8-101, 8-302 & 8-311
- NIST SP 800-53 – PT-1, SA-8, SA-13, SC-7(18) & SI-1
- NIST SP 800-171 – 3.13.1, 3.13.3 & Non-Federal Organization (NFO)
- NIST Cybersecurity Framework – PR.IP-1
- Payment Card Industry Data Security Standard (PCI DSS) – 1.2, 1.3, 1.4, 1.5, 2.2, 6.5 & 12.5

COMPLIANCE SHOULD BE VIEWED AS A NATURAL BYPRODUCT OF SECURE PRACTICES

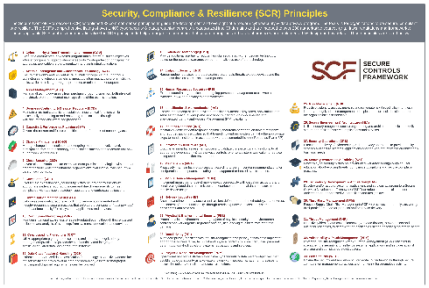
It is vitally important for any SCF user to understand that "compliant" does not mean "secure." However, if you design, build and maintain secure systems, applications and processes, then compliance will be a natural byproduct of those secure practices.

The SCF's comprehensive listing of over 1,000 cybersecurity & data privacy controls is categorized into thirty-three (33) domains that are mapped to over 110 statutory, regulatory and contractual frameworks. Those applicable SCF controls can operationalize the cybersecurity & data privacy principles to help an organization ensure that secure practices are implemented by design and by default.

You may be asking yourself, "What cybersecurity & data privacy principles should I be using?" and that is a great question. The SCF helped with this common question by taking the thirty-three (33) 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.

Secure, Compliant & Resilient (SCR) Principles



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

The SCR is a set of thirty-three (33) cybersecurity & data privacy principles that leverage the SCF's extensive cybersecurity & data privacy control set. You can download the free poster at https://securecontrolsframework.com/domains-principles/.

Steps To Operationalize The SCR Principles

1. Read through the SCR principles to familiarize yourself with the thirty-three (33) 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 SCR principles are being met by your day-to-day practices.

The SCR establishes thirty-three (33) common-sense principles to guide the development and oversight of a modern cybersecurity & data privacy program. Those thirty-three (33) SCR principles are listed below:

SCF Domains & SCR Principles

#	SCF Domain	SCF Identifier	Cybersecurity & Data Privacy by Design (SCR) Principles	Principle Intent
1	Cybersecurity & Data Privacy Governance	GOV	Execute a documented, risk-based program that supports business objectives while encompassing appropriate cybersecurity & data privacy principles that address applicable statutory, regulatory and contractual obligations.	Organizations specify the development of an organization's cybersecurity & data privacy programs, including criteria to measure success, to ensure ongoing leadership engagement and risk management.
2	Artificial and Autonomous Technology	AAT	Ensure trustworthy and resilient Artificial Intelligence (AI) and autonomous technologies to achieve a beneficial impact by informing, advising or simplifying tasks, while minimizing emergent properties or unintended consequences.	Organizations ensure Artificial Intelligence (AI) and autonomous technologies are designed to be reliable, safe, fair, secure, resilient, transparent, explainable and data privacy-enhanced. In addition, AI-related risks are governed according to technology-specific considerations to minimize emergent properties or unintended consequences.
3	Asset Management	AST	Manage all technology assets from purchase through disposition, both physical and virtual, to ensure secured use, regardless of the asset's location.	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.
4	Business Continuity & Disaster Recovery	BCD	Maintain a resilient capability to sustain business-critical functions while successfully responding to and recovering from incidents through well-documented and exercised processes.	Organizations establish processes that will help the organization recover from adverse situations with minimal impact to operations, as well as provide the capability for e-discovery.

5	Capacity & Performance Planning	CAP	Govern the current and future capacities and performance of technology assets.	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.
6	Change Management	CHG	Manage change in a sustainable and ongoing manner that involves active participation from both technology and business stakeholders to ensure that only authorized changes occur.	Organizations ensure both technology and business leadership proactively manage change, including the assessment, authorization and monitoring of technical changes across the enterprise so as to not impact production systems uptime and allow easier troubleshooting of issues.
7	Cloud Security	CLD	Govern cloud instances as an extension of on-premise technologies with equal or greater security protections than the organization's own internal cybersecurity & data privacy controls.	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.
8	Compliance	CPL	Oversee the execution of cybersecurity & data privacy controls to ensure appropriate evidence required due care and due diligence exists to meet compliance with applicable statutory, regulatory and contractual obligations.	Organizations ensure controls are in place to ensure adherence to applicable statutory, regulatory and contractual compliance obligations, as well as internal company standards.
9	Configuration Management	CFG	Enforce secure configurations for systems, applications and services according to vendor-recommended and industry-recognized secure practices.	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.
10	Continuous Monitoring	MON	Maintain situational awareness of security-related events through the centralized collection and analysis of event logs from systems, applications and services.	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.
11	Cryptographic Protections	CRY	Utilize appropriate cryptographic solutions and industry-recognized key management practices to protect the confidentiality and integrity of sensitive/regulated data both at rest and in transit.	Organizations ensure the confidentiality and integrity of its data through implementing appropriate cryptographic technologies to protect systems, applications, services and data.

12	Data Classification & Handling	DCH	Enforce a standardized data classification methodology to objectively determine the sensitivity and criticality of all data and technology assets so that proper handling and disposal requirements can be followed.	Organizations ensure that technology assets, both electronic and physical, are properly classified and measures implemented to protect the organization's data from unauthorized disclosure, or modification, 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.
13	Embedded Technology	EMB	Provide additional scrutiny to reduce the risks associated with embedded technology, based on the potential damages posed from malicious use of the technology.	Organizations specify the development, proactive management and ongoing review of security embedded technologies, including hardening of the "stack" from the hardware, firmware and software to transmission and service protocols used for Internet of Things (IoT) and Operational Technology (OT) devices.
14	Endpoint Security	END	Harden endpoint devices to protect against reasonable threats to those devices and the data those devices store, transmit and process.	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.
15	Human Resources Security	HRS	Execute sound hiring practices and ongoing personnel management to cultivate a cybersecurity & data privacy-minded workforce.	Organizations create a cybersecurity & data privacy-minded workforce and an environment that is conducive to innovation, considering issues such as culture, reward and collaboration.
16	Identification & Authentication	IAC	Enforce the concept of "least privilege" consistently across all systems, applications and services for individual, group and service accounts through a documented and standardized Identity and Access Management (IAM) capability.	Organizations implement the concept of "least privilege" through limiting access to the organization's systems and data to authorized users only.
17	Incident Response	IRO	Maintain a viable incident response capability that trains personnel on how to recognize and report suspicious activities so that trained incident responders can take the appropriate steps to handle incidents, in accordance with a documented Incident Response Plan (IRP).	Organizations establish and maintain a viable and tested capability to respond to cybersecurity or data privacy-related incidents in a timely manner, where organizational personnel understand how to detect and report potential incidents.
18	Information Assurance	IAO	Execute an impartial assessment process to validate the existence and functionality of appropriate cybersecurity & data privacy controls, prior to a system, application or service being used in a production environment.	Organizations ensure the adequately of cybersecurity & data privacy controls in development, testing and production environments.

19	Maintenance	MNT	Proactively maintain technology assets, according to current vendor recommendations for configurations and updates, including those supported or hosted by third-parties.	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.
20	Mobile Device Management	MDM	Implement measures to restrict mobile device connectivity with critical infrastructure and sensitive/regulated data that limit the attack surface and potential data exposure from mobile device usage.	Organizations govern risks associated with mobile devices, regardless of ownership (organization-owned, employee-owned or third-party owned). Wherever possible, technologies are employed to centrally manage mobile device access and data storage practices.
21	Network Security	NET	Architect and implement a secure and resilient defense-in-depth methodology that enforces the concept of "least functionality" through restricting network access to systems, applications and services.	Organizations ensure sufficient cybersecurity & data 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.
22	Physical & Environmental Security	PES	Protect physical environments through layers of physical security and environmental controls that work together to protect both physical and digital assets from theft and damage.	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.
23	Data Privacy	PRI	Align data privacy practices with industry-recognized data privacy principles to implement appropriate administrative, technical and physical controls to protect regulated personal data throughout the lifecycle of systems, applications and services.	Organizations align data privacy engineering decisions with the organization's overall data privacy strategy and industry-recognized leading practices to secure Personal Data (PD) that implements the concept of data privacy by design and by default.
24	Project & Resource Management	PRM	Operationalize a viable strategy to achieve cybersecurity & data privacy objectives that establishes cybersecurity as a key stakeholder within project management practices to ensure the delivery of resilient and secure solutions.	Organizations ensure that security-related projects have both resource and project/program management support to ensure successful project execution.
25	Risk Management	RSK	Proactively identify, assess, prioritize and remediate risk through alignment with industry-recognized risk management principles to ensure risk decisions adhere to the organization's risk threshold.	Organizations ensure that the business unit(s) that own the assets and / or processes involved are made aware of and understand all applicable cybersecurity & data privacy-related risks. The cybersecurity & data privacy teams advise and educate on risk management matters, while it is the business units and other key stakeholders that ultimately own the risk.
26	Secure Engineering & Architecture	SEA	Utilize industry-recognized secure engineering and architecture principles to deliver secure and resilient systems, applications and services.	Organizations align cybersecurity engineering and architecture decisions with the organization's overall technology architectural strategy and industry-

				recognized leading practices to secure networked environments.
27	Security Operations	OPS	Execute the delivery of cybersecurity & data privacy operations to provide quality services and secure systems, applications and services that meet the organization's business needs.	Organizations ensure appropriate resources and a management structure exists to enable the service delivery of cybersecurity, physical security and data privacy operations.
28	Security Awareness & Training	SAT	Foster a cybersecurity & data privacy-minded workforce through ongoing user education about evolving threats, compliance obligations and secure workplace practices.	Organizations develop a cybersecurity & data privacy-minded workforce through continuous education activities and practical exercises.
29	Technology Development & Acquisition	TDA	Develop and test systems, applications or services according to a Secure Software Development Framework (SSDF) to reduce the potential impact of undetected or unaddressed vulnerabilities and design weaknesses.	Organizations ensure that cybersecurity & data privacy principles are implemented into any products/solutions, either developed internally or acquired, to make sure that the concepts of “least privilege” and “least functionality” are incorporated.
30	Third-Party Management	TPM	Execute Supply Chain Risk Management (SCRM) practices so that only trustworthy third-parties are used for products and/or service delivery.	Organizations ensure that cybersecurity & data privacy risks associated with third-parties are minimized and enable measures to sustain operations should a third-party become compromised, untrustworthy or defunct.
31	Threat Management	THR	Proactively identify and assess technology-related threats, to both assets and business processes, to determine the applicable risk and necessary corrective action.	Organizations establish a capability to proactively identify and manage technology-related threats to the cybersecurity & data privacy of the organization’s systems, data and business processes.
32	Vulnerability & Patch Management	VPM	Leverage industry-recognized Attack Surface Management (ASM) practices to strengthen the security and resilience systems, applications and services against evolving and sophisticated attack vectors.	Organizations proactively manage the risks associated with technical vulnerability management that includes ensuring good patch and change management practices are utilized.
33	Web Security	WEB	Ensure the security and resilience of Internet-facing technologies through secure configuration management practices and monitoring for anomalous activity.	Organizations address the risks associated with Internet-accessible technologies by hardening devices, monitoring system file integrity, enabling auditing, and monitoring for malicious activities.

SECTION 5: UNDERSTANDING WHAT IT MEANS TO ADOPT "PRIVACY BY DESIGN" PRINCIPLES

Through our interactions with organizations, we identified that many organizations understand the cybersecurity framework they wanted or needed to align with, but had no understanding of the privacy principles their organization should be aligned with. We 7set out to fix that issue and what we did was select over 5632a dozen of the most common privacy frameworks to create a "best in class" approach to managing privacy principles. The best part is these are all mapped to the SCF and is built into the SCF, so you can leverage the SCF for both your cybersecurity & data privacy needs!

Why should you care? When you tie the broader SCR in with the SCF Data Privacy Management Principles (DPMP), you have an excellent foundation for building and maintaining secure systems, applications and services that address cybersecurity & data privacy considerations by default and by design. The DPMP is included in the SCF download as a separate tab in the Excel spreadsheet.[3]

Think of the SCF Privacy Management Principles as a supplement to the SCR to assist in defining and managing privacy principles, based on selected privacy frameworks. This can enable your organization to align with multiple privacy frameworks that also map to your cybersecurity & data privacy control set, since we found the "apples to oranges" comparison between disparate privacy frameworks was difficult for most non-privacy practitioners to comprehend.

#	Principle Name	SCF Data Privacy Management Principle (SCF-DPMP) Description	AICPA TSC SOC 2 (2017)	APEC	EU GDPR	EU-US Data Privacy Framework	FIPPs (DHS)	FIPPs (OMB)	GAPP	HIPAA Privacy Rule	ISO 27701 v2019	ISO 29100 v2011	NIST SP 800-53 rev4	NIST SP 800-53 rev5	NIST Privacy Framework v1.0	OECD	OMB A-130	PIPEDA	US-California CPRA	US-Nevada SB220	Secure Controls Framework (SCF)
1	Data Privacy by Design	Establish and maintain a comprehensive data privacy program that ensures data privacy considerations are addressed by design in the development of policies, standards, processes, systems, applications, projects and third-party contracts.		1	Art 32.1 Art 32.2 Art 32.3 Art 32.4	Principle 2.7.a			8.2.1		5.3.1 5.3.2 5.3.3 5.4 5.4.1 5.4.2 5.5	5.1 5.10 5.11	AR-1	PM-1 PM-18 PM-20 PT-1	GV.PO-P1 CM.PO-P1 CM.AW-P2 CT.DM-P9 CT.DM-P10 CT.PO-P2		5(f)(1)(ii) App1-3(b) App1-3(b)(1) App1-3(f) App1-4(c)(2)		7007(m) 7002(d)(1) 7002(d)(3) 7002(b) 7002(b)(1)		OCV-01 PRI-01 PRI-01.3
1.1	Assigned Responsibilities	Assign accountability through documented roles and responsibilities to qualified data subjects, including key internal and external stakeholders, for maintaining compliance with all applicable data privacy requirements that involves appropriately monitoring and documenting the data privacy program.			Art 35.2 Art 37.1 Art 37.2 Art 37.3 Art 37.4		Accountability & Auditing	Accountability	1.1.0 1.1.2 1.2.1 1.2.2 1.2.8	164.530(a)(1)	6.15.1.4 8.5	5.10		PM-19	CM.PO-P2 CT.PO-P2		4(h) 5(c)(8) 5(f)(1)(i) App1-4(e)	1			PRI-01.1 PRI-01.4
1.2	Data Classification	Classify data according to the sensitivity and type of personal data as defined by appropriate statutory, regulatory and contractual contexts.			Art 4 Art 9						6.5.2.1			PT-7 PT-7(1) PT-7(2)							DCH-02 PRI-05.7
1.3	Registering Databases	Register applicable databases containing personal data with the appropriate Data Authority, when required.			Art 30.4																PRI-15
1.4	Resource Planning	Identify and plan for resources needed to operate a data privacy program and include data privacy requirements in solicitations for technology solutions and services.			Art 32.1 Art 32.2						6.3.1.5						5(e)(1)(vi)(I) 5(d)(3)(iv) App1-4(b)(1) App1-4(b)(2)				PRM-01
1.5	Inventory of Personal Data	Maintain an inventory of both the type of personal data and specific data element, as well as the systems, applications and processes that collect, create, use, disseminate, maintain, and/or disclose that personal data.			Art 4 Art 5.2 Art 9				7.2.2				SE-1	PM-5(1)	ID.IM-P1 ID.IM-P3 ID.IM-P8		5(e)(1)(vi)(I) 5(f)(1)(iii) App1-4(b)(2)(iv)				PRI-05.5 PRI-05.6
1.6	Data Privacy Training	Provide recurring data privacy awareness and training for all employees and contractors.							1.1.1 1.2.10	164.504 164.530	6.4.2.2		AR-5 AT-3(4) AT-4	AT-1 AT-2 AT-2(1)	GV.PO-P1 GV.AT-P1 GV.AT-P2		App1-4(h)(1) App1-4(h)(2) App1-4(h)(3)		7100(a) 7100(b)		SAT-01 SAT-02 SAT-02.1
1.7	Personal Data Categories	Define and implement data handling and protection requirements for specific categories of sensitive Personal Data (PD).																	7002(f)		PRI-05.7
1.8	Data Subject Communications	Craft disclosures and communications to data subjects so the material is readily accessible and written in a manner that is concise, unambiguous and understandable by a reasonable person.																	7002(a) 7003(b)(1) 7003(b)(2) 7003(b)(3) 7011(d)		PRI-17
1.9	Conspicuous Link To Data Privacy Notice	Design websites and mobile applications to include a conspicuous link to the organization's data privacy notice.																	7003(d) 7010(b) 7010(e) 7011(c)		PRI-17.1
1.10	Notice of Financial Incentive	Provide data subjects with a Notice of Financial Incentive that explains the material terms of a financial incentive, price or service difference so the data subject can make an informed decision about whether to participate.																	7010(d) 7013(a) 7013(b) 7013(c) 7013(d)		PRI-17.2
2	Data Subject Participation	data subjects are directly involved in the decision-making process regarding the fair and lawful processing of the individual's personal data and, to the extent practicable, directly-engaged to receive explicit permission to use their personal data.	P2.1 P3.2	9	Art 6.1 Art 7.1 Art 7.2 Art 7.3 Art 7.4	Principle 2.2.a(i) Principle 2.2.a(ii) Principle 2.2.b Principle 2.2.c Principle 2.2.c(i)	Individual Participation	Individual Participation	3.2.1 3.2.2 3.2.3 3.2.4	164.506 164.508	7.2.3 7.2.4 7.3.4 7.3.5 8.5.7	5.2	IP-1 IP-1(1)	PT-4	CT.PO-P1 CT.PO-P3	7		3	7002(a) 7002(d) 7004(a) 7004(a)(1) 7004(a)(2)		PRI-03
2.1	Clear Choices	Provide clear and conspicuous choices that enable an individual, or a person authorized by the individual, to permit or prohibit the collection, creation, use, dissemination, maintenance, retention, and/or disclosure of the individual's personal data. This is also referred to as the right to "opt out."			Art 7.1 Art 7.2 Art 7.3 Art 7.4 Art 12.2	Principle 2.2.a(i) Principle 2.2.a(ii) Principle 2.2.b Principle 2.2.c Principle 2.2.c(i)				164.508(b)(3) 164.510 (a) and (b)	7.3.4		TR-1 TR-1(1)	PM-20(1) PT-5	CT.PO-P3			3	7002(e) 7002(f) 7004(a) 7004(a)(1) 7004(a)(2)		PRI-03

DATA PRIVACY PRACTICES ARE COMMON EXPECTATIONS

For organizations, we found the "apples to oranges" comparison between disparate privacy frameworks was difficult for most non-privacy lawyers to understand. What this project did was identify a dozen of the leading privacy frameworks and create a set of simplified, yet comprehensive, privacy management principles. Below are the thirty-one (31) different frameworks the SCF Data Privacy Management Principles is mapped to:

1. AICPA TSC 2017:2022 (used for SOC 2)
2. Asia-Pacific Economic Cooperation (APEC) Privacy Framework 2015
3. Generally Accepted Privacy Principles (GAPP)
4. ISO 27701:2025
5. ISO 29100:2024
6. NIST Privacy Framework 1.0
7. NIST 800-53 R5
8. NIST CSF 2.0
9. Organization for Economic Co-operation and Development (OECD) Privacy Principles
10. US Federal - Data Privacy Framework (DPF)
11. US Federal - Fair Information Practice Principles (FIPPs)
12. US Federal - HIPAA Administrative Simplification 2013
13. US State - Alaska Personal Information Protection Act (PIPA)
14. US State - California Consumer Privacy Act (CCPA) January 2026 (amended California Privacy Rights Act (CPRA))
15. US State - Colorado Privacy Act
16. US State - Illinois Biometric Information Privacy Act (BIPA)
17. US State - Illinois Identity Protection Act (IPA)

[3] *SCF DPMP - https://securecontrolsframework.com/data-privacy-management-principles/*

18. US State - Illinois Personal Information Protection Act (PIPA)
19. US State - Nevada Privacy Law (SB220)
20. US State - Oregon Consumer Privacy Act (SB 619)
21. US State - Tennessee Information Protection Act
22. US State - Texas BC521
23. US State - Virginia Consumer Data Protection Act (CDPA) 2025
24. US State - Vermont Act 171 of 2018
25. EMEA - European Union General Data Protection Regulation (EU GDPR)
26. EMEA - Saudi Arabia Personal Data Protection Law (PDPL)
27. APAC - Australia Privacy Act
28. APAC - Australian Privacy Principles
29. APAC - India DPDPA 2023
30. APAC - New Zealand Privacy Act of 2020
31. Americas - Canada Personal Information Protection and Electronic Documents Act (PIPEDA)

We took these frameworks and looked for similarities and also for gaps. If you download the SCF Data Privacy Management Principles, you will see the direct mapping to these leading privacy frameworks so you know the origin of the principle we include in our document. This will be a great tool for organizations that may have to address multiple requirements, since it brings a common language to simply things.

The eighty-six (86) principles of the SCF Data Privacy Management Principles are organized into eleven (11) domains:

1. Privacy by Design
2. Data Subject Participation
3. Limited Collection & Use
4. Transparency
5. Data Lifecycle Management
6. Data Subject Rights
7. Security by Design
8. Incident Response
9. Risk Management
10. Third-Party Management
11. Business Environment

SECTION 6: TAILORING THE SCRP & SCF FOR YOUR NEEDS

Some people freak out and think they have to do 1,000+ 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 1,000+ 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.

Beyond just using compliance terminology properly, understanding which of the three types of compliance is crucial in managing both cybersecurity and privacy risk within an organization. The difference between non-compliance can be as stark as (1) going to jail, (2) getting fined, (3) getting sued, (4) losing a contract or (5) an unpleasant combination of the previous options.

Understanding the "hierarchy of pain" with compliance leads to well-informed risk decisions that influence technology purchases, staffing resources and management involvement. That is why it serves both cybersecurity and IT professionals well to understand the compliance landscape for their benefit, since you can present issues of non-compliance in a compelling business context to get the resources you need to do your job.

The most common types of compliance requirements are:

- Statutory
- Regulatory
- Contractual

STATUTORY REQUIREMENTS

Statutory obligations are required by law and refer to current laws that were passed by a state or federal government. These laws are generally static and rarely change unless a new law is passed that updates it, such as the HITECH Act, which provided updates to the two-decades-old HIPAA.

From a cybersecurity and privacy perspective, statutory compliance requirements include:

- **US – Federal Laws**
  - Children's Online Privacy Protection Act (COPPA)
  - Fair and Accurate Credit Transactions Act (FACTA) – including "Red Flags" rule
  - Family Education Rights and Privacy Act (FERPA)
  - Federal Information Security Management Act (FISMA)
  - Federal Trade Commission (FTC) Act
  - Gramm-Leach-Bliley Act (GLBA)
  - Health Insurance Portability and Accountability Act (HIPAA) / HITECH Act
  - Sarbanes-Oxley Act (SOX)
- **US – State Laws**
  - California SB1386
  - Massachusetts 201 CMR 17.00
  - Oregon ORS 646A.622
- **International Laws**
  - Canada – Personal Information Protection and Electronic Documents Act (PIPEDA)
  - UK – Data Protection Act (DPA)
  - Other countries' variations of Personal Data Protect Acts (PDPA)

Regulatory Requirements

Regulatory obligations are required by law, but they are different from statutory requirements in that these requirements refer to rules issued by a regulating body that is appointed by a state or federal government. These are legal requirements through proxy, where the regulating body is the source of the requirement. It is important to keep in mind that regulatory requirements tend to change more often than statutory requirements.

From a cybersecurity and privacy perspective, regulatory compliance examples include:

- **US Regulations**
  - Defense Federal Acquisition Regulation Supplement (DFARS) (NIST 800-171)
  - Federal Acquisition Regulation (FAR)
  - Federal Risk and Authorization Management Program (FedRAMP)
  - DoD Information Assurance Risk Management Framework (DIARMF)
  - National Industrial Security Program Operating Manual (NISPOM)
  - New York Department of Financial Services 23 NYCRR 500
- **International Regulations**
  - European Union General Data Protection Regulation (EU GDPR)

Contractual Requirements

Contractual obligations are required by legal contract between private parties. This may be as simple as a cybersecurity or privacy addendum in a vendor contract that calls out unique requirements. It also includes broader requirements from an industry association that membership brings certain obligations.

From a cybersecurity and privacy perspective, common contractual compliance requirements include:

- Payment Card Industry Data Security Standard (PCI DSS)
- Service Organization Control (SOC)
- Generally Accepted Privacy Principles (GAPP)
- Center for Internet Security (CIS) Critical Security Controls (CSC)
- Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM)

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!

Customizing The Control Set: Use Excel To Manually Filter Controls

The Secure Controls Framework (SCF), the controls within the SCRP, 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 Security, Compliance & Resilience Management System (SCRMS) model is a methodology that an organization can use categorize its applicable controls according to "must have" vs "nice to have" requirements:

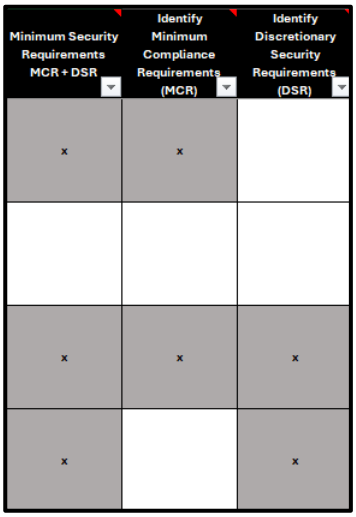
- **Minimum Compliance Criteria (MCR)** are the absolute minimum requirements that must be addressed to comply with applicable laws, regulations and contracts.
- **Discretionary Security Requirements (DSR)** are tied to the organization's risk appetite since DSR are "above and beyond" MCR, where the 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.

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

Within the SCF, there is a column labelled "Minimum Security Requirements (MSR) MCR + MSR" that will assist you in this process.

Follow these steps to tailor the SCF:

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).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).
2. A selection of either MCR or DSR will automatically select the MSR + DSR column:
    a. In the MCR column, simply put an "x" to mark that control as being "must have" controls.
    b. In the DSR column, simply put an "x" to mark that control as being "nice to have" controls.
3. Unfilter the column you just performed this task on and do it to the next law, regulation or framework that you need to map.
4. Repeat steps 2 and step 3 until all your applicable laws, regulations and frameworks are mapped to.



Minimum Security Requirements MCR + DSR	Identify Minimum Compliance Requirements (MCR)	Identify Discretionary Security Requirements (DSR)
x	x	
x	x	x
x		x

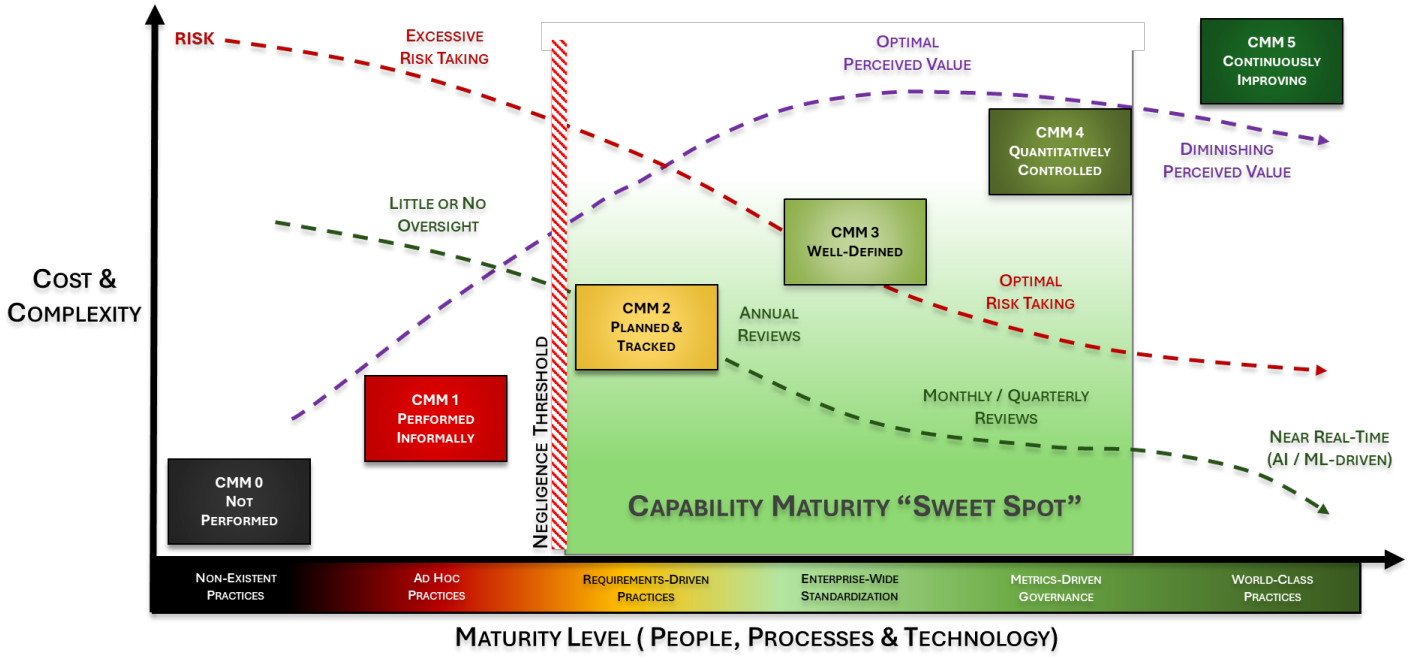
EXPERT INSIGHT (BASELINING): The MSR + DSR resulting column shows the SCF controls that considered an organization's Minimum Security Requirements (MSR) that will be used. The MSR is the baseline set of controls the organization should implement to be both secure and compliant.

Section 7: 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 SCR-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.

Secure, Compliant & Resilient Capability Maturity Model (SCR-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 SCR-CMM 1 and SCR-CMM 2. The reason for this is at SCR-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 SCR-CMM 3. Oversight and process automation can decrease risk, but generally not as noticeably as steps taken to attain SCR-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 SCR-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 SCR-CMM 5 targets to support their aggressive business model needs.

The SCR-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 (6) SCR-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

SCR-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).

SCR-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 SCR-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.*

SCR-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.

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

Note – The reality with a SCR-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.*

SCR-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 SCR-CMM 2 practices that are narrowly focused, SCR-CMM 3 practices are standardized across the organization.

It can be argued that SCR-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 SCR-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 & Data 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.*

SCR-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 SCR-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 & Data 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.

SCR-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.

SCR-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 SCR-CMM 5.

Note – The reality with a SCR-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 & Data 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

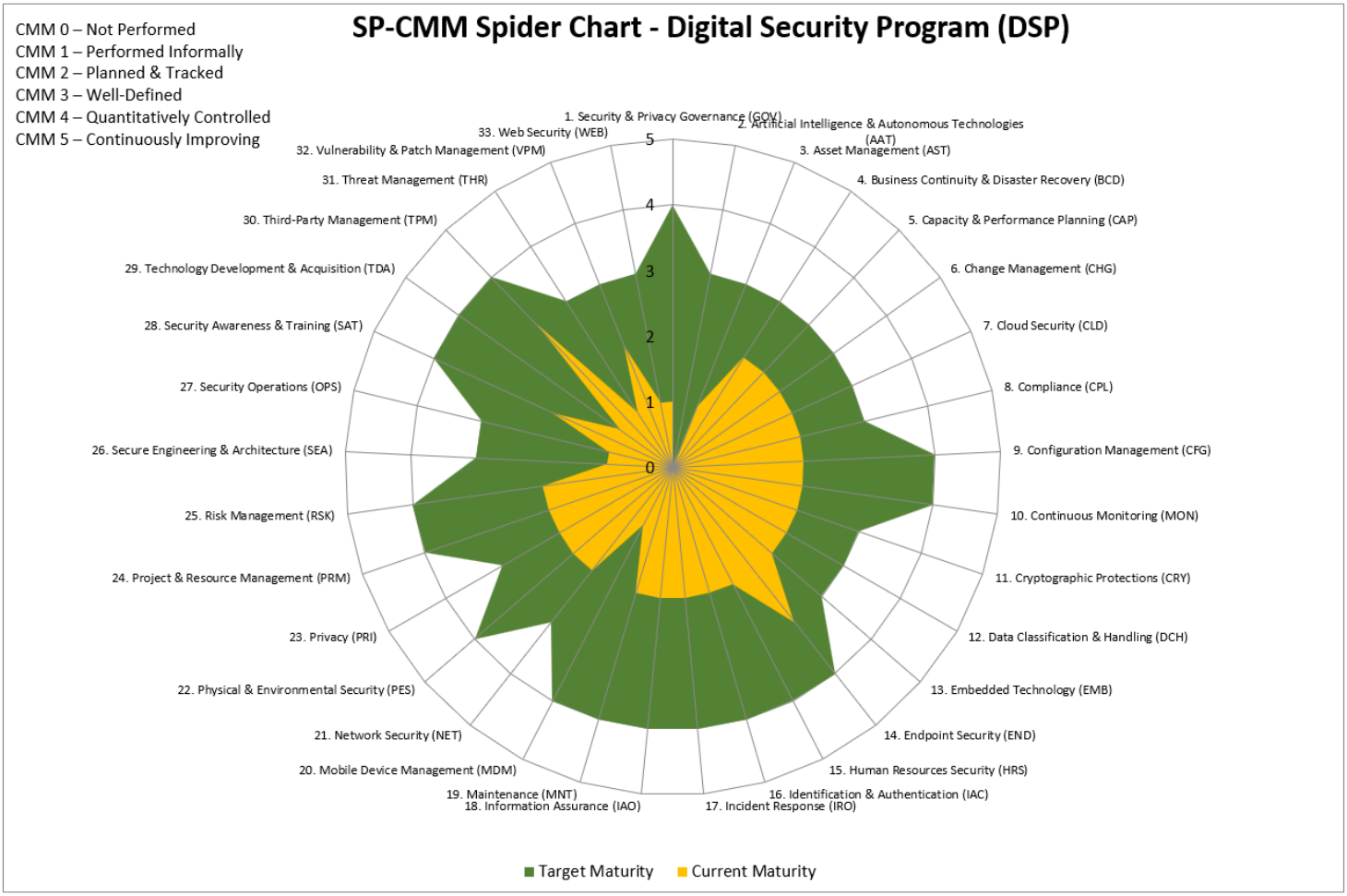
The following table summarizes the high-level expectations for small/medium/large organizations to meet each level of maturity.

Maturity Level	Small Organizations	Medium Organizations	Large Organizations
SCR-CMM 0	▪ Lack of processes would be considered negligent behavior. This is generally due to a lack of a cybersecurity and privacy program. ▪ [NEGLIGENT]		It is unlikely for a large organization to completely ignore cybersecurity and privacy requirements.
SCR-CMM 1	▪ IT support focuses on reactionary "break / fix" activities and are ad hoc in nature. ▪ IT support is likely outsourced with a limited support contract. ▪ [LIKELY NEGLIGENT]	▪ Internal IT staff exists, but there is no management support to spend time or budget on security / privacy controls that leads to ad hoc control implementation. ▪ Focus is on general IT operations without clear standards that implement secure systems and processes. ▪ [LIKELY NEGLIGENT]	
SCR-CMM 2	▪ Internal IT role(s) has clear requirements and is supported to meet applicable cybersecurity / privacy compliance obligations; or ▪ The outsourced IT provider is properly scoped in its support contract to address applicable compliance obligations.	▪ IT staff have clear requirements to meet applicable compliance obligations. ▪ There is most likely a dedicated cybersecurity role or a small cybersecurity team.	
SCR-CMM 3	▪ There is a small IT staff that has clear requirements to meet applicable compliance obligations. ▪ There is likely a very competent leader (e.g., security manager / director) with solid cybersecurity experience who has the authority to direct resources to enact secure practices across the organization.	▪ IT staff have clear requirements to meet applicable compliance obligations. ▪ In addition to the existence of a dedicated cybersecurity team, there are specialists (e.g., engineers, SOC analysts, GRC analysts, privacy, etc.). ▪ There is a very competent leader (e.g., CISO) with solid cybersecurity experience who has the authority to direct resources to enact secure practices across the organization.	
SCR-CMM 4	It is unrealistic for a small organization to attain this level of maturity.	▪ IT staff have clear requirements to meet applicable compliance obligations. ▪ In addition to the existence of a dedicated cybersecurity team, there are specialists (e.g., engineers, SOC analysts, GRC analysts, privacy, etc.). ▪ There is a very competent leader (e.g., CISO) with solid cybersecurity experience who has the authority to direct resources to enact secure practices across the organization. ▪ Business stakeholders are made aware of the status of the cybersecurity and privacy program (e.g., quarterly business reviews to the CIO/CEO/board of directors). Situational awareness is made possible through detailed metrics.	
SCR-CMM 5	It is unrealistic for a small or medium organization to attain this level of maturity.		▪ IT staff have clear requirements to meet applicable compliance obligations. ▪ In addition to the existence of a dedicated cybersecurity team, there are specialists (e.g., engineers, SOC analysts, GRC analysts, privacy, etc.). ▪ There is a very competent leader (e.g., CISO) with solid cybersecurity experience who has the authority to direct resources to enact secure practices across the organization. ▪ Business stakeholders are made aware of the status of the cybersecurity and privacy program (e.g., quarterly business reviews to the CIO/CEO/board of directors). Situational awareness is made possible through detailed metrics. ▪ The organization has a very aggressive business model that requires not only IT, but its cybersecurity and privacy practices, to be innovative to the point of leading the industry in how its products and services are designed, built or delivered. ▪ The organization invests heavily into developing AI/ML technologies to made near real-time process improvements to support the goal of being an industry leader.

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 data 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 SCR-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 L3 and L4 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?"*** L3 maturity is generally considered "an environment that is in control" where it is well-managed, whereas being in a L4 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 L3 as the highest-level of maturity targets. Additionally, the cost to mature from a L3-4 or L4-5 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 Security, Compliance & Resilience Management System (SCRMS) model is 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.

The most efficient manner we can recommend would be to first look at the thirty-three (33) 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, Compliance & Resilience (SCR) Principles 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.

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 data 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.

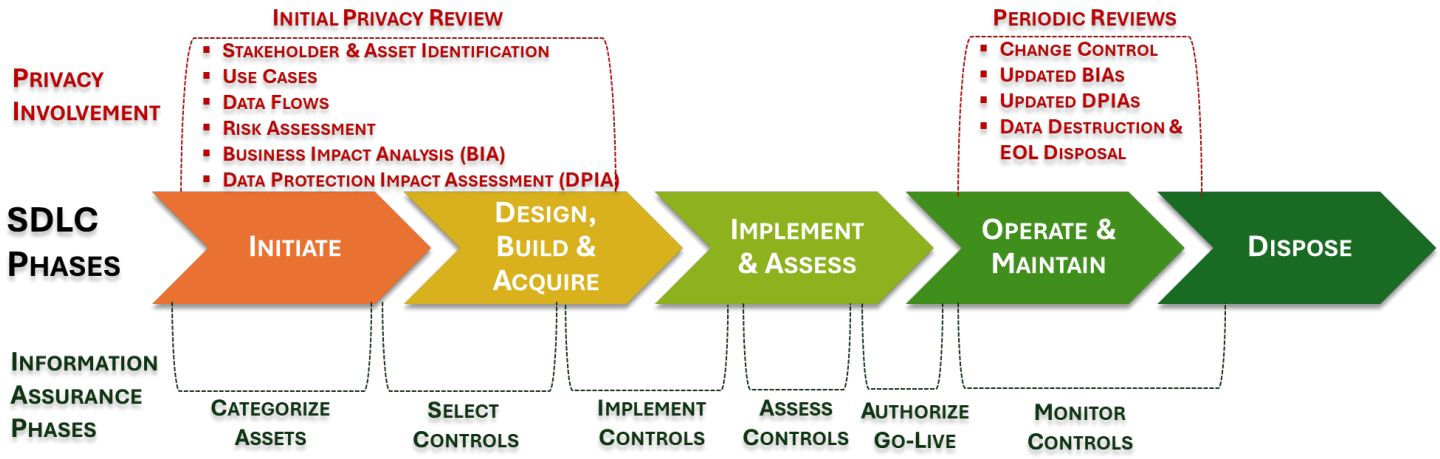
Identifying The Problem

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 SCR-CMM Overview section of this document, L0-1 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 L2-L4 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 L2-3 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. This step can also be done within Excel or within a GRC solution (e.g., SCF Connect). In the end, the result is a tailored set of controls that meets 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.

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

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

IDENTIFYING THE PROBLEM

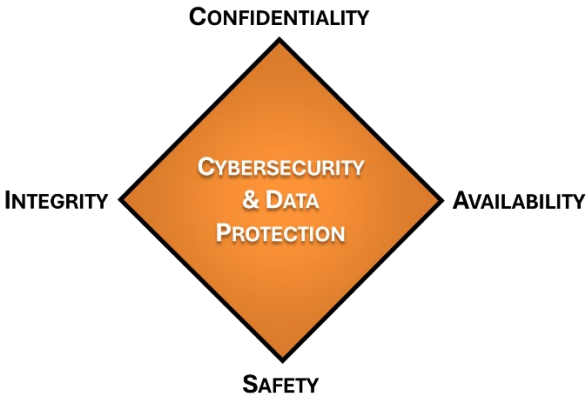
In managing a cybersecurity and data privacy program, it is important to address controls in a holistic manner, which includes governing the supply chain. ESPs are commonly considered the "soft underbelly" for an organization's security program, since ESP oversight has traditionally been weak or non-existent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

One of the issues with managing ESPs 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 ESP. The SCR-CMM can be used to obtain more nuanced answers from ESPs by having those ESPs select from L0-5 to answer if the control is implemented and how mature the process is.

CONSIDERATIONS

Referencing back to the SCR-CMM Overview section of this document, L0-1 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 L2-L4 to identify the reasonable people, processes and technologies that need ESPs 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 ESP management perspective, this is often going to limit target CMM levels to L2-3 for most organizations.

ESP controls are expected to cover both your internal requirements, as well as external requirements from applicable laws, regulations and contracts. Using the SCR-CMM can be an efficient way to provide a level of quality control over ESP practices. Being able to demonstrate proper cybersecurity and data 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 ESP'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. This step can also be done within Excel or within a GRC solution (e.g., SCF Connect, Cyturus, etc.). In the end, the result is a tailored set of controls that address the ESP'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 ESP. Ideally, the ESP 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 ESP-specific controls is appropriate.

Use Case #4 – Due Diligence In Mergers, Acquisitions & Divestitures (MA&D)

It is commonplace to conduct a cybersecurity and data privacy practices assessment as part of Mergers, Acquisitions & Divestitures (MA&D) due diligence activities. The use of a gap assessment against a set of baseline MA&D controls (e.g., SCF-B control set) can be used to gauge the level of risk. In practical terms, this type of maturity-based gap assessment can be used in a few ways:

- Sellers can provide the results from a first- or third-party gap assessment to demonstrate both strengths and weaknesses, as a sign of transparency.
- Buyers can identify unforeseen deficiencies that can:
  - Lead to a lower buying price; or
  - Backing out of the deal.

SCF Mergers, Acquisitions & Divestitures Security Standards (MADSS)

The SCF took on an ambitious project to "build a better mousetrap" to fix the common complaints associated with MA&D due diligence. The Mergers, Acquisitions & Divestitures Security Standards (MADSS) is a standard to normalize MA&D-related assessment practices.[4]

The MADSS is not "one-size-fits-all." Instead, the guidance throughout this document should be adopted and tailored to the unique size, resources and risk circumstances of each organization. It can be modified, or augmented, with specific requirements. By following this methodology, cybersecurity and data privacy practitioners can improve the currently disjointed approach used to perform assessments of cybersecurity and/or data privacy controls.

Identifying The Problem

Acquiring another entity involves a considerable amount of trust. Cybersecurity MA&D due diligence exists to prevent the purchasing entity from potentially acquiring a class-action lawsuit or multi-million-dollar data protection-related fines (worst case scenarios). MA&D is a game of cat and mouse between the two parties:

- The divesting entity is going to want to "put its best foot forward" and gloss over deficiencies; and
- The acquiring entity wants to know the truth about strengths and weaknesses.

If the acquiring entity only leverages a single framework (e.g., NIST CSF, ISO 27002 or NIST 800-53) for due diligence work, it will most likely provide a partial picture as to the divesting entity's cybersecurity and data privacy practices. That is why the SCF-B is a bespoke set of cybersecurity and data privacy controls that was purposely built for MA&D to provide as complete a picture as possible about the divesting entity's cybersecurity and data privacy practices.

A control set questionnaire that asks for simple yes, no or not applicable answers is insufficient in MA&D due diligence. Failure to leverage maturity-based criteria will result in the inability to provide critical insights into the actual security posture of the divesting entity. The SCR-CMM can be used to obtain more nuanced answers to determine (1) if a control is implemented and (2) how mature the process behind the control is.

Considerations

Referencing back to the SCR-CMM Overview section of this document, L0-1 levels of maturity are identified as being deficient from a "reasonable person perspective" in most cases. Therefore, acquiring entities need to look at the "capability maturity sweet spot" between L2-L4 to identify the reasonable people, processes and technologies needed to demonstrate to properly protect systems, applications, services and data, regardless of where it is stored, transmitted or processed.

Areas of deficiency can be identified and remediation costs determined, which can be used to adjust valuations. Key areas that affect valuations include, but are not limited to:

- Non-compliance with statutory, regulatory and/or contractual obligations
- Data protection practices (e.g., privacy)
- IT asset lifecycle management (e.g., unsupported / legacy technologies)
- Historical cybersecurity incidents
- Risk management (e.g., open items on a risk register or Plan of Action & Milestones (POA&M)
- Situational awareness (e.g., visibility into activities on systems and networks)

[4] *SCF MADSS - https://securecontrolsframework.com/free-scf-content/mergers-acquisitions-divestitures-ma-d/*

- Software licensing (e.g., intellectual property infringement)
- Business Continuity / Disaster Recovery (BC/DR)
- IT / cybersecurity architectures (e.g., deployment of on-premises, cloud and hybrid architectures)
- IT /cybersecurity staffing competencies

IDENTIFYING A SOLUTION

The SCF did the hard work by developing the SCF-B control set. The "best practices" that comprise the SCF-B include:

- Trust Services Criteria (SOC 2)
- CIS CSC
- COBITv5
- COSO
- CSA CCM
- GAPP
- ISO 27002
- ISO 31000
- ISO 31010
- NIST 800-160
- NIST Cybersecurity Framework
- OWASP Top 10
- UL 2900-1
- EU GDPR

Understanding Key Cybersecurity Terminology

This section is intended to help standardize cybersecurity and data privacy documentation-related terminology based on definitions from leading authorities (e.g., NIST, ISO, ISACA, AICPA, etc.). In compliance operations, words have meanings. Therefore, it is important to provide examples from industry-recognized sources for the proper use of these terms that make up cybersecurity & data privacy documentation. Simply because an individual has used terminology in a specific manner for past decade (e.g., policy), that does not mean that is correct terminology usage, based on authoritative sources. ComplianceForge took the time to compile authoritative definitions from multiple sources to defend the proper usage that ComplianceForge applies to its documentation structure.

Policy / Security Policy

Policies are high-level statements of management intent from an organization's executive leadership that are designed to influence decisions and guide the organization to achieve the desired outcomes:

- Policies exist to mitigate risks to the organization, including statutory, regulatory and contractual obligations.
- Policies are enforced by standards and further implemented by procedures to establish actionable and accountable requirements.

Unfortunately, for many IT/cybersecurity professionals, when they refer to a "policy" they really mean "standard." This common misuse of critical documentation components can create a significant amount of confusion, since those are not interchangeable terms. Standards are subordinate to policies and standards address the granular requirements needed to satisfy a policy. Therefore, a 1-3 sentence policy statement is acceptable to capture a "high-level statement of management intent" for a specific domain.

- An organization is expected to have multiple policies to address cybersecurity and data privacy needs (e.g., access control, data handling, etc.).
- Policies address the strategic needs of the organization.
- There is never a justifiable reason to have an exception to a policy, since exceptions should only be at the standard or procedure level.

- **ISACA Glossary:**
  - A document that records a high-level principle or course of action that has been decided on.
  - The intended purpose is to influence and guide both present and future decision making to be in line with the philosophy, objectives and strategic plans established by the enterprise's management teams.
  - Overall intention and direction as formally expressed by management.
- **ISO 704:2009:**
  - Any general statement of direction and purpose designed to promote the coordinated planning, practical acquisition, effective development, governance, security practices, or efficient use of information technology resources.
- **ISO 27000:2016:**
  - Intention and direction of an organization as formally expressed by its top management.
- **NIST Glossary (Policy):**
  - Statements, rules or assertions that specify the correct or expected behavior of an entity.
  - A statement of objectives, rules, practices or regulations governing the activities of people within a certain context.
- **NIST Glossary (Security Policy):**
  - Security policies define the objectives and constraints for the security program. Policies are created at several levels, ranging from organization or corporate policy to specific operational constraints (e.g., remote access). In general, policies provide answers to the questions "what" and "why" without dealing with "how." Policies are normally stated in terms that are technology-independent.
  - A set of rules that governs all aspects of security-relevant system and system element behavior.
    - Note 1: System elements include technology, machine, and human elements.
    - Note 2: Rules can be stated at very high levels (e.g., an organizational policy defines acceptable behavior of employees in performing their mission/business functions) or at very low levels (e.g., an operating system policy that defines acceptable behavior of executing processes and use of resources by those processes).

Control Objective

Control Objectives are targets or desired conditions to be met.

- Control Objectives describing what is to be achieved as a result of the organization implementing a Control.
- A Standard applies organization-specific criteria to achieve a Control Objective.

Where applicable, Control Objectives are directly linked to laws, regulations and frameworks to align cybersecurity and data privacy with reasonably-expected practices. The intent is to establish sufficient evidence of due diligence and due care to withstand scrutiny (e.g., external audits/assessments) to disprove potential accusations of negligence.

- **ISACA Glossary:**
  - A statement of the desired result or purpose to be achieved by implementing control procedures in a particular process.
- **ISO 27000:2016:**
  - Statement describing what is to be achieved as a result of implementing controls.
- **AICPA SSAE No. 18, Attestation Standards Clarification and Recodification:**
  - The aim or purpose of specified controls at the organization. Control objectives address the risks that controls are intended to mitigate.

Standard

Standards are mandatory requirements regarding processes, actions and/or configurations.

- Standards are intended to be granular and prescriptive to ensure systems, applications and services are designed and operated to include appropriate cybersecurity and data privacy protections.
- Standards are designed to satisfy Controls and Control Objectives.

- **ISACA Glossary:**
  - A mandatory requirement.
- **NIST Glossary:**
  - A published statement on a topic specifying the characteristics, usually measurable, that must be satisfied or achieved to comply with the standard.
  - A rule, condition, or requirement describing the following information for products, systems, services or practices:
    - Classification of components.
    - Specification of materials, performance, or operations; or
    - Delineation of procedures.

Guideline / Supplemental Guidance

Guidelines are recommended practices that are based on industry-recognized secure practices.

- Guidelines help augment Standards when discretion is permissible.
- Unlike Standards, Guidelines allow individuals / teams to apply discretion or leeway in interpretation, implementation, or use.

- **ISACA Glossary:**
  - A description of a particular way of accomplishing something that is less prescriptive than a procedure.
- **ISO 704:2009:**
  - Recommendations suggesting, but not requiring, practices that produce similar, but not identical, results.
  - A documented recommendation of how an organization should implement something.
- **NIST Glossary:**
  - Statements used to provide additional explanatory information for security controls or security control enhancements.

CONTROL

Controls are technical, administrative or physical safeguards.

- Controls are the nexus used to manage risks through preventing, detecting or lessening the ability of a particular threat from negatively impacting business processes.
- Controls directly map to Standards, Procedures and Control Objectives.
- Control testing is designed to measure specific aspects of how Standards are actually implemented and if the Control / Control Objective is sufficiently addressed.

- **ISACA Glossary:**
  - The means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be of an administrative, technical, management, or legal nature.
- **ISO 27000:2016:**
  - The policies, procedures, practices and organizational structures designed to provide reasonable assurance that business objectives will be achieved and undesired events will be prevented or detected and corrected.
  - Measure that is modifying risk:
    - Controls include any process, policy, device, practice, or other actions which modify risk.
    - Controls may not always exert the intended or assumed modifying effect.
- **NIST Glossary:**
  - Measure that is modifying risk. (Note: controls include any process, policy, device, practice, or other actions which modify risk.)
- **NIST SP 800-53 R5:**
  - The safeguards or countermeasures prescribed for an information system or an organization to protect the confidentiality, integrity, and availability of the system and its information [security control].
  - The administrative, technical, and physical safeguards employed within an agency to ensure compliance with applicable data privacy requirements and manage data privacy risks [privacy control].

ASSESSMENT OBJECTIVE (AO)

Assessment Objectives (AOs) are a set of determination statements that express the desired outcome for the assessment of a Control.

- AOs are the authoritative source of guidance for assessing Controls to generate evidence that can support an assertion that the underlying Control has been satisfied.
- All AOs associated with a control must be satisfied to legitimately conclude a Control is properly implemented.

- **NIST Glossary:**
  - A set of determination statements that expresses the desired outcome for the assessment of a security control, privacy control, or control enhancement.

PROCEDURE

Procedures are a documented set of steps necessary to perform a specific task or process in conformance with an applicable standard.

- Procedures help address the question of how the organization actually operationalizes a Policy, Standard or Control.
- Procedures are generally the responsibility of the process owner / asset custodian to build and maintain but are expected to include stakeholder oversight to ensure applicable compliance requirements are addressed.
- Without documented procedures, there is no defendable evidence of due care practices.

The result of a procedure is intended to satisfy a specific control. Procedures are also commonly referred to as "control activities."

- **ISACA Glossary:**
  - A document containing a detailed description of the steps necessary to perform specific operations in conformance with applicable standards. Procedures are defined as part of processes.
- **ISO 704:2009:**
  - A detailed description of the steps necessary to perform specific operations in conformance with applicable standards.

  - A group of instructions in a program designed to perform a specific set of operations.
- **NIST Glossary:**
  - A set of instructions used to describe a process or procedure that performs an explicit operation or explicit reaction to a given event.

THREAT

Threats represents a person or thing likely to cause damage or danger.

Natural and man-made threats affect control execution (e.g., if the threat materializes, will the control function as expected?). Threats exist in the natural world that can be localized, regional or worldwide (e.g., tornados, earthquakes, solar flares, etc.). Threats can also be man-made (e.g., hacking, riots, theft, terrorism, war, etc.).

- **ISACA Glossary:**
  - Anything (e.g., object, substance, human) that is capable of acting against an asset in a manner that can result in harm.
- **ISO 13335-1:**
  - A potential cause of an unwanted incident.
- **NIST Glossary:**
  - Threat: Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-source to successfully exploit a particular information system vulnerability.
  - Cyberthreat: Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

RISK

Risks represents a potential exposure to danger, harm or loss.*

Risk is associated with a control deficiency (e.g., If the control fails, what risk(s) is the organization exposed to?). Risk is often calculated by a formula of the Occurrence Likelihood (**OL**) (e.g., probability of the event) x the Impact Effect (**IE**) (e.g., potential, negative consequences) in an attempt to quantify the potential magnitude of a risk instance materializing.

While it is not possible to have a totally risk-free environment, it may be possible to manage risks by avoiding, reducing, transferring, or accepting the risks.

- **ISACA Glossary:**
  - The combination of the probability of an event and its consequence.
- **ISO 704:2009:**
  - The level of impact on organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring.
- **NIST SP 800-53 R5:**
  - A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically is a function of:
    - The adverse impact, or magnitude of harm, that would arise if the circumstance or event occurs; and
    - The likelihood of occurrence.
- **NIST Glossary:**
  - A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of:
    - The adverse impacts that would arise if the circumstance or event occurs; and

- The likelihood of occurrence. Information system-related security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.

* Danger: state of possibly suffering harm or injury
* Harm: material / physical damage
* Loss: destruction, deprivation or inability to use

Metric

Metrics provide a "point in time" view of specific, discrete measurements, unlike trending and analytics that are derived by comparing a baseline of two or more measurements taken over a period of time.

Analytics are generated from the analysis of metrics. Analytics are designed to facilitate decision-making, evaluate performance and improve accountability through the collection, analysis and reporting of relevant performance related metrics.

- **ISACA Glossary:**
  - A quantifiable entity that allows the measurement of the achievement of a process goal.
- **ISO 704:2009:**
  - A thing that is measured and reported to help with the management of processes, services, or activities.
- **NIST Glossary:**
  - Tools designed to facilitate decision making and improve performance and accountability through collection, analysis, and reporting of relevant performance-related data.

Secure Baseline Configurations / Hardening Standard

Secure baseline configurations (e.g., hardening standard) are technical in nature and specify the required configuration settings for a defined technology platform.

Leading guidance on secure configurations tend to come from:

- Center for Internet Security (**CIS**) Benchmarks;
- Defense Information Systems Agency (**DISA**) Security Technical Implementation Guides (**STIGs**); and/or
- Original Equipment Manufacturer (**OEM**) recommendations.

- **NIST Glossary:**
  - A documented set of specifications for an information system, or a configuration item within a system, that has been formally reviewed and agreed on at a given point in time, and which can be changed only through change control procedures.
  - A set of specifications for a system, or Configuration Item (**CI**) within a system, that has been formally reviewed and agreed on at a given point in time, and which can be changed only through change control procedures. The baseline configuration is used as a basis for future builds, releases, and/or changes.

Risk Register / Plan of Action & Milestones (POA&M)

A POA&M is a "living document" that summarizes control deficiencies from identification through remediation. A POA&M is essentially a risk register that tracks the assignment of remediation efforts to individuals or teams, as well as identifying the tasks and resources necessary to perform the remediation.

- **NIST Glossary:**
  - Risk Register: A repository of risk information including the data understood about risks over time.
  - Risk Register: A central record of current risks, and related information, for a given scope or organization. Current risks are comprised of both accepted risks and risk that are have a planned mitigation path (e.g., risks to-be-eliminated as annotated in a POA&M).

- POA&M: A document that identifies tasks that need to be accomplished. It details resources required to accomplish the elements of the plan, milestones for meeting the tasks, and the scheduled completion dates for the milestones.

System Security Plan (SSP) / System Security & Privacy Plan (SSPP)

A SSP/SSPP is a "living document" that summarizes protection mechanisms for a system or project. It is a documentation method used to capture pertinent information in a condensed manner so that personnel can be quickly educated on the "who, what, when, where, how & why" concepts pertaining to the security of the system or project. A SSP/SSPP is meant to reference an organization's existing policies, standards and procedures and is not a substitute for that documentation.

- **NIST Glossary:**
  - Formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements.