CYBERSECURITY SUPPLY CHAIN RISK MANAGEMENT (C-SCRM)

PRACTITIONER'S GUIDE TO THE INTERSECTION OF C-SCRM, CHANGE MANAGEMENT AND ZERO TRUST (ZT)

VERSION 2025.1

Table of Contents

Executive Summary

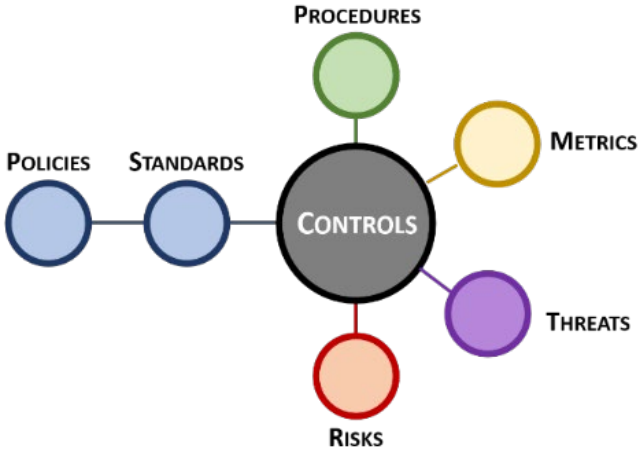
The premise of this guide is to propose an efficient way to plan out a roadmap that can successfully implement robust Cybersecurity Supply Chain Risk Management (C-SCRM) practices that focus on prevention. This guide highlights the nature of preventative cybersecurity and data protection controls as an efficient way to protect an organization from the expense and operational disruptions associated with incident response and business continuity activities. The result is a viable approach for organizations to use in order to create a prioritized project plan for C-SCRM-focused secure and compliant practices.

The concept of a " kill chain" addressed in this guide adopts the premise that it is easier to stop and prevent further damage if malicious activities are discovered earlier, rather than later. The intention of using the C-SCRM Kill Chain is:

(1) By applying a prioritized, phased approach towards C-SCRM-related activities, it is possible to avoid rework and cascading failures by addressing dependencies earlier in the process; and
(2) Focusing resources and efforts on preventative controls, rather than detective controls. Prevention, tied with automated, reactive technologies can minimize operational disruptions from either hostile or accidental incidents.

The C-SCRM Kill Chain breaks the concept of C-SCRM down into 24 major steps, which can then be translated into a project plan. This project was approached from the question of, *"If a consultant was hired to build a C-SCRM program, what would the plan be to start from nothing to get a company to where it has operational C-SCRM capabilities?"* While the C-SCRM Kill Chain maps controls from NIST SP 800-161 to the steps in the model, it is important to emphasize that the prioritization and "bucketing" of controls into phases is a subjective endeavor and not everyone may agree with this approach. If you choose to use the C-SCRM Kill Chain, you will invariably need to modify the approach to fit your organization's unique business practices and specific needs.

The C-SCRM Kill Chain leverages the principles of the Integrated Controls Management (ICM) model.[1] The premise of ICM is that controls are central to cybersecurity and data protection operations, as well as the overall business rhythm of an organization. The ICM is supported by the Cybersecurity & Data Privacy Risk Management Model (C|P-RMM)[2] that describes the central nature of controls, where beyond just policies and standards, but procedures, metrics, threats and risks map to controls, as well.



"Zero Trust Architecture (ZTA) is more than just by tying logical access to a user's identity and should take into account the validated integrity of systems, applications and services across the supply chain."

Special thanks goes to the following contributors, since this document would not exist without their applied expertise:

Tom Cornelius
Senior Partner
ComplianceForge

Mark Allers
VP, Business Development
Cimcor

Ryan Bonner
Founder & CEO
Defcert

Tim Trickett
CTO, Public Sector
BDO

[1] *ComplianceForge's Integrated Controls Management (ICM) model - https://complianceforge.com/content/pdf/complianceforge-integrated-controls-management.pdf*
[2] *SCF's Cybersecurity & Data Privacy Risk Management Model (C|P-RMM) - https://securecontrolsframework.com/risk-management-model/*

Resilient vs. Reactive Operational Mindset

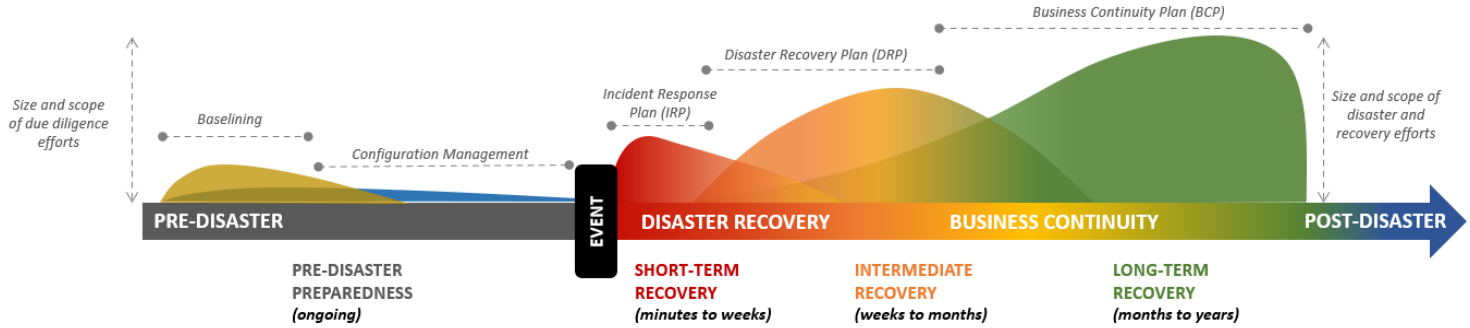
National Institute of Standards and Technology (NIST) Special Publication 800-160 focuses on "cyber resiliency engineering" and is the authoritative source for secure engineering principles within the realm of cybersecurity and data protection.[3] A common definition of *resilience* is "*the capacity to quickly recover from difficulties*." Resilience is a measure of an organization's elasticity – being able to spring back into a pre-determined operational state following an incident. Organizations should strive to be resilient to IT and cybersecurity-related incidents both internally and across the supply chain.

Traditional incident response and recovery operations are not designed with resilience in mind. Recovery is absolutely possible and Service Level Agreement (SLAs) help establish acceptable data loss parameters, maximum outages, etc. However, this is more of a way to bracket risk management decisions and while is an efficient manner to justify budgets for Continuity of Operations (COOP)-related technologies and staffing, it is not sustainable. While reactive operations are often viewed as heroic endeavors that "saved the organization from doom," it does not mean that reactive model is the best methodology or least expensive path to follow. Resiliency is.

Reactive-Focused Security Operations

If you study the graphic below, there are a few key takeaways:

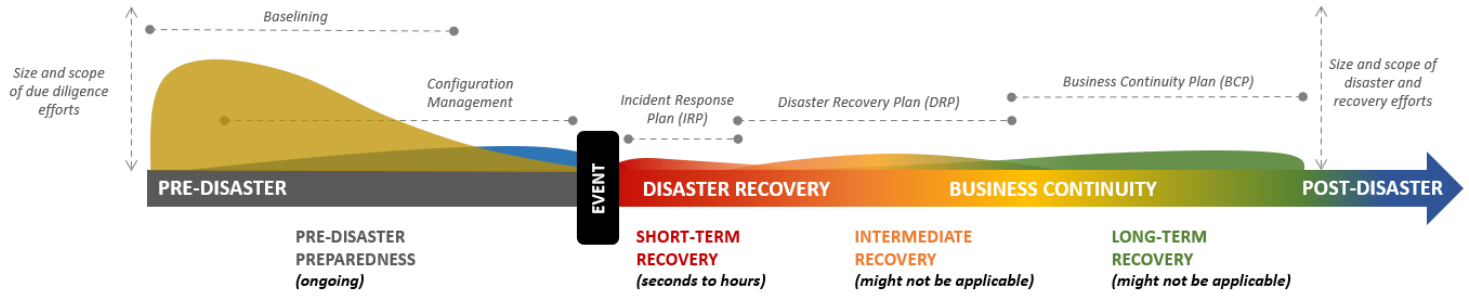
- Effort is on the "right side" of an incident or event – it is reactive. Baselining and configuration management on the "left side" of an incident or event is often compliance-focused and are not directly tied to response/recovery operations.
- The traditional, reactive model has minimal focus on baselining and configuration management.
- When an incident occurs, there are structured plans to respond that span from minutes to years in duration:
  - Incident Response Plan (IRP)
  - Disaster Recovery Plan (DRP)
  - Business Continuity Plan (BCP)
- Expense is primarily associated with event detection, response, remediation and recovery operations.



Resiliency-Focused Security Operations

If you study the graphic below, there are a few key takeaways:

- Effort is on the "left side" of an incident or event is prevention-focused. An increase in effort on the "left side", will likely result in a decreased operational impact on the "right side" of the event occurrence.
- There is significant effort placed on baselining and automating configuration management operations.
- When an incident occurs, the automated remediation actions minimize impact and the necessity to activate IRPs, DRPs and BCPs.
- Expense is primarily associated with tightly-controlled configuration management practices.

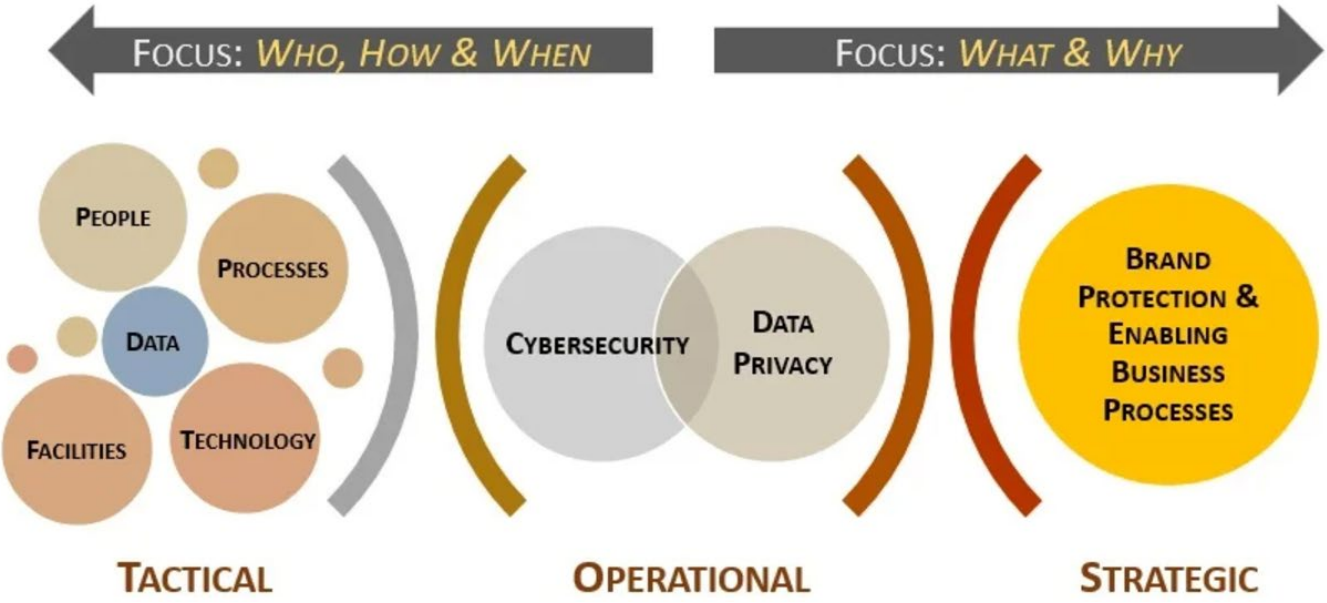


[3] *NIST SP 800-160 "Developing Cyber Resilient Systems: A Systems Security Engineering Approach" - https://csrc.nist.gov/publications/detail/sp/800-160/vol-2/final*

Understanding Necessary Building Blocks For Implementing Zero Trust & C-SCRM

If truth be told, controls exist to protect an organization's data. For instance, requirements for asset management do not *primarily* exist to protect the inherent value of the asset, but the data it contains, since assets are merely data containers. Assets, such as laptops, servers and network infrastructure are commodities that can be easily replaced, but data residing on those devices cannot.

This concept of being data-centric is crucial to understand when developing, implementing and governing a cybersecurity and data protection program that addresses Zero Trust and Cybersecurity Supply Chain Risk Management (C-SCRM) concepts. Zero Trust Architecture (ZTA) is more than just by tying logical access to a user's identity and should take into account the validated integrity of systems, applications and services ***across the supply chain***.

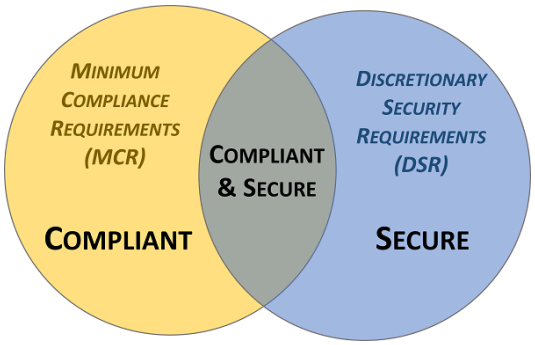


Zero Trust & C-SCRM Goals - Secure, Compliant or Both?

For C-SCRM, controls must be designed to proactively address the (1) strategic, (2) operational and (3) tactical nature of operating an organization's cybersecurity and data protection program. C-SCRM must be designed to address both internal controls that are directly under the influence of the organization, as well as third-party operated controls that directory or indirectly influence C-SCRM for the organization. Organizations need to understand and clarify the difference between "compliant" versus "secure" since that is necessary to have coherent risk management discussions with affected stakeholders.

To assist in this process, an organization's applicable controls should be categorized 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 (privacy) controls to address voluntary industry practices or internal requirements, such as findings from internal audits or risk assessments.



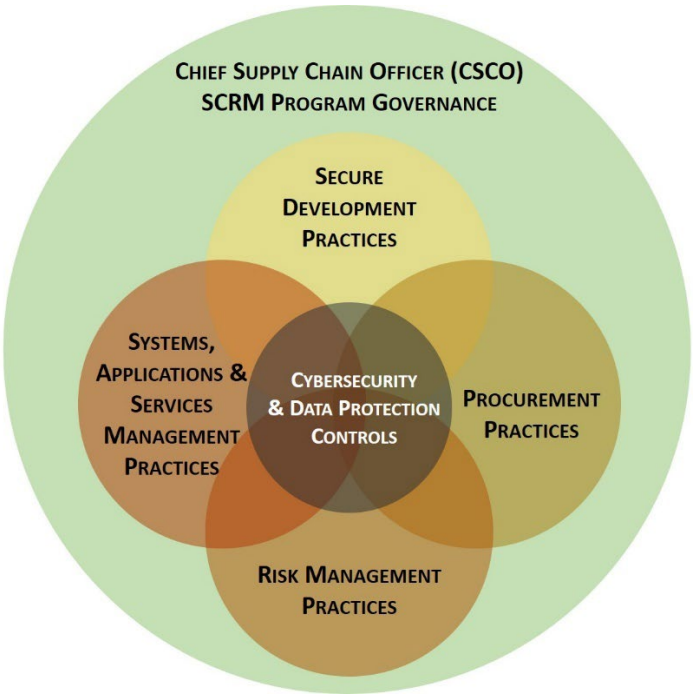
Secure and compliant operations exist when both MCR and DSR are implemented and properly governed:

- 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.

When you start looking at how you "do zero trust & supply chain risk management" in a practical manner, it is more than just a control set. In fact, a C-SCRM program needs to also have authority over several key business functions that impact supply chain security:

- Secure Development Practices
- Procurement Practices
- Risk Management Practices
- Systems, Applications & Services Management Practices

NIST SP 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*, is the "gold standard" for C-SCRM-related concepts and this guide heavily relies on that body of work.[4]



Operational Leadership

For C-SCRM to be successful, operational leadership is essential. This "active participation" by a Chief Supply Chain Officer (CSCO) and his/her staff, ensures that processes are effectively carried out on a day-to-day basis. In many industries, the CSCO is often designated as the Chief Operations Officer (COO). Regardless of the official title, the CSCO is responsible for internal and external supply chain processes. This scope ranges beyond simple logistics and manufacturing activities to include:

- Innovation and development.
- Onboarding new technologies/services.
- Business operations (e.g., manufacturing, service delivery, etc.).
- Business Continuity & Disaster Recovery (BCDR).
- Third-party relationship onboarding and management (e.g., vendors, service providers, contractors, etc.).
- Decommissioning technologies, services and third-party relationships.

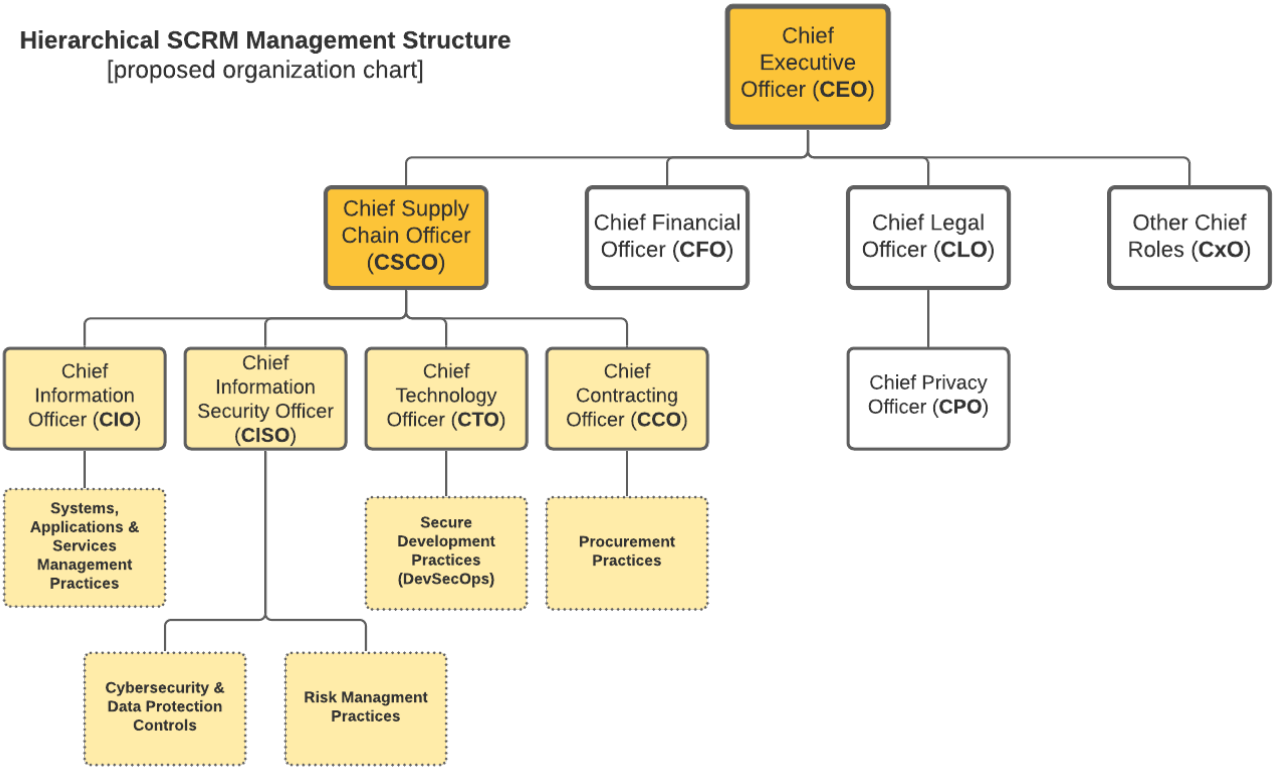
Efficient operational leadership requires the organization to structure roles that are complementary and not counterproductive. For the CSCO role to be successful in executing the organization's C-SCRM program:

- The CSCO needs to report directly to the organization's Chief Executive Officer (CEO) to eliminate conflicts of interests among leadership representing Lines of Business (LOB) within the organization.
- The CSCO must be able to influence cybersecurity and data protection controls by being part of the organization's cybersecurity steering committee.
- Due to the reliance on risk management practices and the underlying cybersecurity and data protection controls that enable a C-SCRM program to function, the Chief Information Security Officer (CISO) should directly report to the CSCO.
- Due to the supply chain nature of DevSecOps, the Chief Technology Officer (CTO) role should directly report to the CSCO.

[4] *NIST SP 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.pdf*

- Due to the external focus of the C-SCRM program, the Chief Contracting Officer (CCO) role should directly report to the CSCO to ensure contracts and procurement actions are in-line with the C-SCRM program.
- Due to how technology is so integral to business operations, the Chief Information Officer (CIO) role should directly report to the CSCO.
- The CISO, CIO, CTO and CCO need to be viewed as peers, each with an equal role of importance in the C-SCRM program, where the CSCO provides operational leadership to orchestrate C-SCRM activities across the enterprise and its supply chain.

It should be needless to say, but corporate "buy-in" is essential for the overall program to function accordingly. The "message from the top" must be from the Board of Directors (BoD) and CEO so that corporate executives (CxO) will be forced to adopt the practices within their Lines of Business (LoB) to address their inherent risk with technology and the supply chain. C-SCRM is a multi-player effort, so the organization must adopt a "One Team. One Fight" mentality that is driven by senior leadership first and foremost. Additionally, the organization's Internal Audit (IA) plays a crucial role in maintaining internal accountability, where there is a neutral system of checks and balances.



Secure Development Practices

C-SCRM is an enterprise-wide activity that is implemented throughout the System Development Life Cycle (SDLC). Within the concept of secure development practices, in order to ensure C-SCRM is operational it takes the following to exist and be functional:

- Maintain close working relationships through frequent visits and communications.
- Mentor and coach suppliers on C-SCRM and actively help suppliers improve their cybersecurity and supply chain practices.
- Invest in common solutions.
- Require the use of the same standards within the acquirer organizations and by suppliers, thereby simplifying communications about cybersecurity risk and mitigations and helping to achieve a uniform level of quality throughout the ecosystem.
- Restrict the use of open-source software to projects for which there is clear oversight and accountability. If this is not possible, then code audits/reviews should be performed for open-source project.

Resilience and improvement activities include:

- Rules and protocols for information sharing between acquirers and suppliers.
- Joint development, review and revision of incident response, business continuity and disaster recovery plans.
- Protocols for communicating vulnerabilities and incidents.

- Responsibilities for responding to cybersecurity incidents.
- Coordinated communication methods and protocols.
- Coordinated restoration and recovery procedures.
- Collaborative processes to review lessons learned.
- Updates of coordinated response and recovery plans based on lessons learned.

PROCUREMENT PRACTICES

C-SCRM lies at the intersection of cybersecurity and supply chain risk management. Existing supply chain and cybersecurity practices provide a foundation for building an effective Risk Management Program (RMP). Therefore, within the concept of procurement practices, in order to ensure C-SCRM is operational it takes the following to exist and be functional:

- Increased executive leadership or Board of Directors (BoD) involvement for establishing C-SCRM as a top business priority and to ensure proper oversight.
- C-SCRM intersects with the BoD fiduciary "duty of care" and BoD-level training should be provided to board members understand the current state and weaknesses of the organization's supply chain, including the BoD's responsibilities in executing a C-SCRM strategy.
- Clear governance of C-SCRM activities that includes cross-organizational roles and responsibilities with clear definitions and designation/distribution of these roles among enterprise risk management, supply chain, cybersecurity, product management and product security (if applicable) and other relevant functions appropriate for the organization's business.
- Leading framework-based policies, standards and procedures that provide guidance to different business units detailing their C-SCRM activities.
- Same policies used internally and with suppliers.
- Integration of cybersecurity considerations into the system and product development life cycle.
- Use of cross-functional teams to address specific, enterprise-wide risks.
- Clear definition of roles of individuals responsible for cybersecurity aspects of supplier relationships (which may be different than those responsible for procurement activities with specific suppliers).
- Establishment of Centers of Excellence (CoE) to identify and manage best practices.
- A set of measures of success used to facilitate decision-making, accountability and improvement.
- Approved and banned supplier lists.
- Use of software and hardware component inventory (e.g., bill of materials) for third-party components.
- Prioritization of suppliers based on their criticality.
- Establishment of testing procedures for the most critical components.
- Establishment of a known set of security requirements or controls for all suppliers, especially robust security requirements for critical suppliers to be used in procurement (sometimes known as master specifications).
- Service-Level Agreements (SLA) with suppliers that state the requirements for adhering to the organization's cybersecurity policy and any controls required of the supplier.
- Establishment of intellectual property rights agreements.
- Shared supplier questionnaires across like organizations, such as within the same critical infrastructure sector.
- Upstream propagation of acquirer's security requirements within the supply chain to sub-tier suppliers.
- Assurance that suppliers have only the access they need in terms of data, capability, functionality and infrastructure; bounding this access by specific time frames during which suppliers need it.
- Use of escrow services for suppliers with a questionable or risky track record.
- Provision of organization-wide training for all relevant stakeholders within the organization, such as supply chain, legal, product development and procurement; this training may also be extended to key suppliers.
- Identification of alternative sources of critical components to ensure uninterrupted production and delivery of products.
- Secure requirements guiding disposal of hardware that contains regulated data (e.g., CUI, FCI, PII, CHD, PHI, etc.) or otherwise sensitive information (e.g., Intellectual Property (IP)).
- Protocols for securely terminating supplier relationships to ensure that all hardware containing acquirer's data has been properly disposed of and that the risks of data leakage have been minimized.
- Establishment of formalized vendor management process, including a vendor management platform to track the state of C-SCRM-related controls across the supply chain.

Risk Management Practices

C-SCRM needs to be implemented as part of an organization's overall Enterprise Risk Management (ERM) activities (e.g., NIST SP 800-39 & NISTIR 8286). These risk management practices involve identifying and assessing applicable risks, determining appropriate response actions and developing a C-SCRM strategy. Within the concept of risk management practices, in order to ensure C-SCRM is operational it takes the following to exist and be functional:

- Activities should involve identifying and assessing applicable risks, as well as determining appropriate response actions.
- Developing a C-SCRM strategy and implementation plan to document selected response actions and monitoring performance against that plan.
- Manage risks. Cyber supply chain risk is associated with a lack of visibility into, understanding of and control over many of the processes and decisions involved in the development and delivery of cyber products and services.
- Manage threats and vulnerabilities. Effectively managing cyber supply chain risks requires a comprehensive view of threats and vulnerabilities.
    - Threats can be either "adversarial" (e.g., tampering, counterfeits) or "non-adversarial" (e.g., poor quality, natural disasters).
    - Vulnerabilities can be "internal" (e.g., organizational procedures) or "external" (e.g., part of an organization's supply chain).
- The C-SCRM strategy should be periodically reviewed by the BoD's risk or audit committee.

Systems, Applications & Services Management Practices

C-SCRM requires organizations to identify critical systems, applications and services, as well as sensitive data, that are most vulnerable and can cause the largest organizational impact if compromised. Within the concept of systems, applications & services management practices, in order to ensure C-SCRM is operational it takes the following to exist and be functional:

- Developing Data Flow Diagrams (DFDs) that track where regulated data (e.g., CUI, FCI, PII, CHD, PHI, etc.) or "crown jewels" IP is stored, transmitted and processed.
- Identifying suppliers that process regulated data or "crown jewels" IP.
- Developing network diagrams that identify suppliers that have access to the acquirer's system and network infrastructure.
- Threat modeling to determine whether a supplier can become an attack vector by being compromised and allowing threat actors access to the acquirer's organization.
- For technology companies, whether a supplier can become an attack vector for the technology company's products or services delivered to customers.
- Controlling the volume of data a supplier has access to or hosts.
- Controlling the physical location of data to ensure compliance with the organization's data governance requirements.
- Monitoring the revenue contribution of suppliers (e.g., criticality).

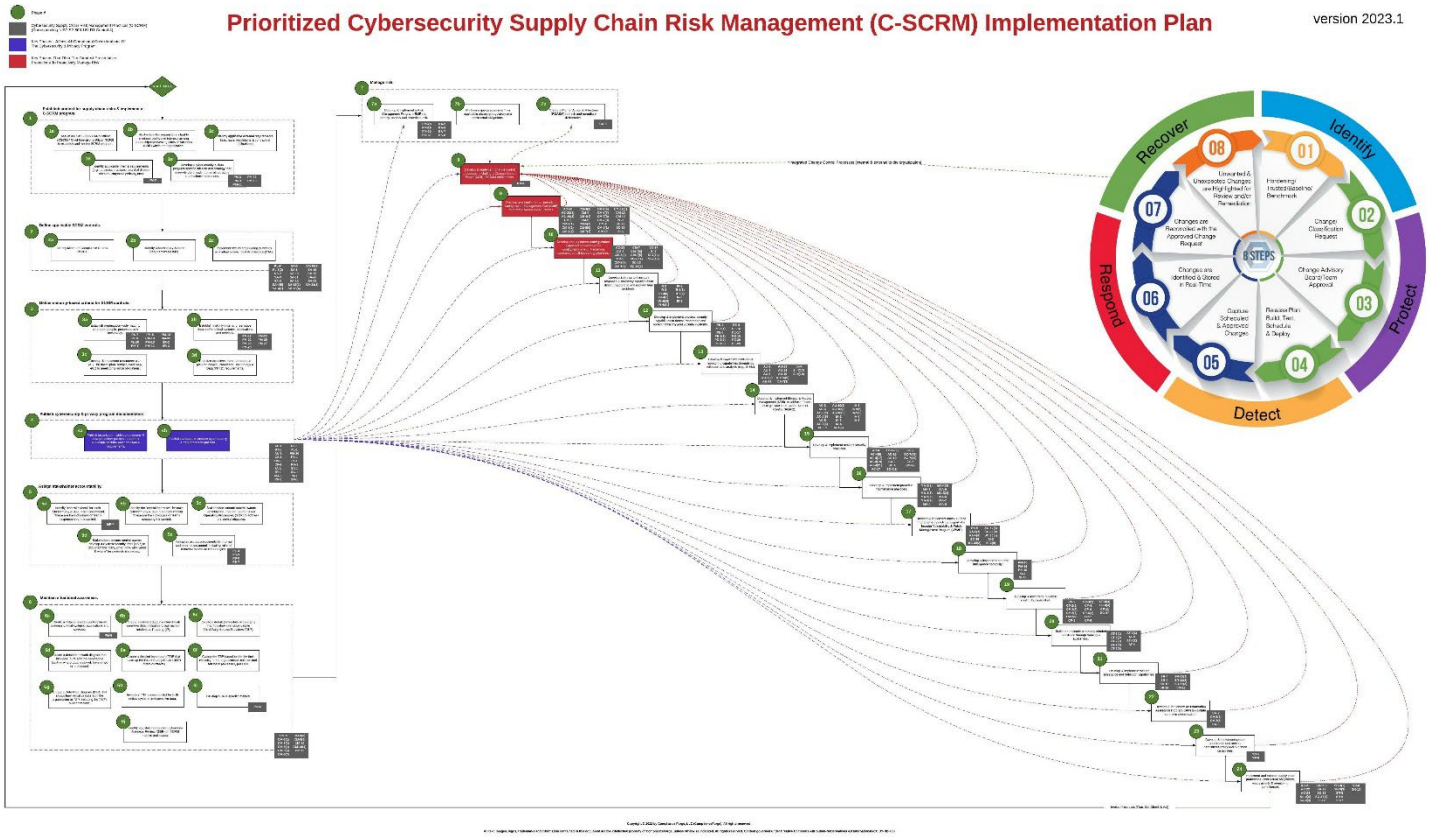
Applying The Kill Chain Model To Zero Trust & C-SCRM

You might be asking yourself how a “kill chain” model applies to C-SCRM. The root issue that is being addressed pertains to how many IT & cybersecurity professionals who are looking at the near future and beyond with dread. With C-SCRM, these front-line IT/cybersecurity practitioners currently do not know where to start, let alone what path they need to follow to align with C-SCRM. The C-SCRM Kill Chain provides a prioritized project plan approach to C-SCRM.

There is an abundance of *"What is ZT & C-SCRM?"* guidance on the Internet, but there is a lack of practical guidance of HOW you are actually supposed to "do ZT & C-SCRM" in realistic terms. The C-SCRM Kill Chain is designed to provide a roadmap that would be usable for anyone:

(1) Starting out on ZT or C-SCRM journey for their organization; or
(2) Wanting to double check their approach to implementing ZT or C-SCRM.

The graphical approach to the C-SCRM Kill Chain is shown below and is downloadable as a separate PDF for that infographic.



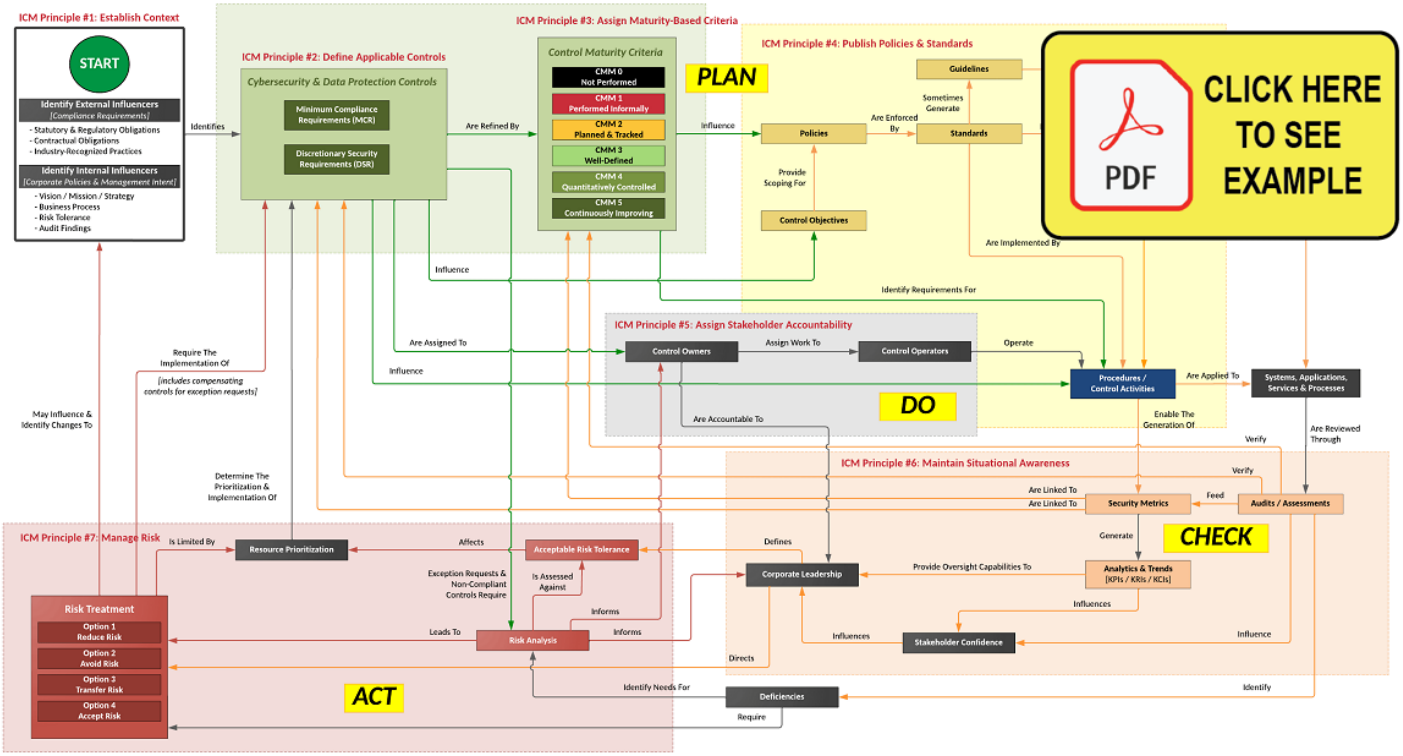
[image is downloadable from https://complianceforge.com/content/pdf/change-kill-chain-visualization.pdf]

ZERO TRUST & C-SCRM PROJECT PLANNING TOOL

The premise of the C-SCRM Kill Chain is to build viable approach for organization to use in order to create a prioritized project plan for implementing a C-SCRM program. The intention of using the C-SCRM Kill Chain is that if you apply a prioritized, phased approach towards C-SCRM-related activities, it is possible to avoid rework and cascading failures by addressing dependencies earlier in the process. The bottom line is this model breaks down C-SCRM into 24 major steps, which can then be translated into a project plan.

The C-SCRM Kill Chain leverages the principles of the Integrated Controls Management (ICM) model:[5]

(1) Establish context;
(2) Define applicable controls;
(3) Assign maturity-based criteria;
(4) Publish policies & standards;
(5) Assign stakeholder accountability;
(6) Maintain situational awareness;
(7) Manage risk; and
(8) Evolve process.



[image is downloadable from https://complianceforge.com/content/Plan-Do-Check-Act.pdf]

[5] *ComplianceForge's Integrated Controls Management (ICM) model - https://complianceforge.com/content/pdf/complianceforge-integrated-controls-management.pdf*

Background On The Logic Used In This Model To Operationalize C-SCRM

It is important to explain the thought process that went through the prioritization of the model's phases. This is a quick explanation on some of the reasoning used to determine prioritization:

1. There are fundamental steps that must occur to establish the basis to be able to implement C-SCRM-related steps. This groundwork is essentially the first 6 steps.

2. You cannot legitimately assess changes, vulnerabilities, threats, etc. without first having a handle on risk management and a defined risk threshold. Risk management is the key building block that other practices rely upon.

3. Once you have solid risk management practices, change control is the second most important phase to address, since that is needed to legitimately alter other practices and you need to be able to document your changes and track open issues in a Plan of Action & Milestones (POA&M) (e.g., evidence of due care).

4. Secure configurations and centralized configuration management (e.g., Group Policies, hardening scripts, etc.) almost go hand-in-hand, but before you can centrally manage configurations, they need to be defined and standardized. Configuration management supports steps going forward.

5. From there, the assumption is that you will discover issues so incident response capability needs to exist.

6. Since C-SCRM spans more than just cybersecurity, there is a necessity to have physical security practices in place. These physical security capabilities should support the organization's overall incident response plans.

7. Event logging (continuous monitoring) is next and needs to exist before secure configurations, since logs need to get sent somewhere. You need to have this logging infrastructure in place before you get into secure configurations.

8. Next, Identity and Access Management (IAM) needs to be locked down to ensure aspects of least privilege and Role Based Access Control (RBAC) are implemented. The reason IAM comes after secure configurations is due to troubleshooting - if you have "gold standard" secure builds to work from, it is easier to then assign permissions/RBAC that will work with those builds. The alternative is your new configurations break IAM/RBAC practices, which is something that should be avoided.

9. Network security practices are somewhat covered through secure configurations and IAM practices, but aspects such as remote access and network architecture (e.g., Zero Trust Architecture (ZTA), jump boxes, segmentation, etc.) need to be standardized and enforced uniformly.

10. You realistically can't do vulnerability management without first having solid maintenance capabilities, so maintenance needs to be formalized with change control integrations. Maintenance needs to be tied into change management, which has a risk management component to it.

11. The concept of vulnerability management is broad and is best summed up by the term "attack surface management" where you are doing what you can to minimize the ways an adversary can attack. This relies on maintenance practices and change management being in place and operating.

12. From there, the remaining phases are relatively subjective in the order the steps are implemented until you reach the step where an Information Assurance Program (IAP) will help assist the intern audit function by performing Control Validation Testing (CVT) operations. This is often done for pre-production testing, but can be done after major changes to evaluate control implementation before "go live" of the updated system, application or service.

13. Realistically, your organization needs to have the first 23 steps well-managed before actions are taken to provide stringent oversight on third-party practices. This is why supply chain protections are the 24th step in this kill chain.

Zero Trust / C-SCRM Kill Chain Phases

The C-SCRM Kill Chain is made up of twenty-four (24) phases (these correspond to those shown in the associated infographic). It is important to note that these steps can be applied both to internal practices and External Service Providers (ESP). Realistically, an organization must first "master the fundamentals" and have its own C-SCRM practices in order before proactive oversight of ESPs is feasible.

1. Establish Context For Supply Chain Risks & Implement a Zero Trust & Supply Chain Risk Management (C-SCRM) Program.

To build and maintain efficient and effective operations, a C-SCRM program must have a hierarchical vision, mission and strategy that directly supports the organization's broader strategic objectives and business processes. This process of establishing context involves identifying all applicable external compliance requirements (e.g., laws, regulations and contractual obligations), as well as internal directives (e.g., Board of Directors (BoD), corporate policies, etc.). This is a due diligence element of the C-SCRM program.

This step has 5 subcomponent steps:

- **1a.** Assign a Chief Supply Chain Officer (CSCO) to establish and run the C-SCRM program.
- **1b.** Restructure the organization chart to eliminate conflicts of interests among leadership representing Lines of Business (LOB) within the organization.
- **1c.** Identify applicable external requirements (e.g., laws, regulations & contractual obligations)
- **1d.** Identify applicable internal requirements (e.g., business practices, BoD dictates, corporate policies, etc.)
- **1e.** Develop a cybersecurity & data program-specific mission and strategy that supports the broader corporate strategy and business operations.

2. Define Applicable Zero Trust & C-SCRM Controls.

A tailored control set of cybersecurity and data protection controls must exist. This control set needs to be made of Minimum Compliance Requirements (MCR) and Discretionary Security Requirements (DSR). This blend of "must have" and "nice to have" requirements establish an organization's tailored control set to ensure both secure practices and compliance are designed for.

This step has 3 subcomponent steps:

- **2a.** Identify MCR.
- **2b.** Identify DSR.
- **2c.** Implement secure engineering principles and adopt a Zero Trust Architecture (ZTA).

3. Define Maturity-Based Criteria for C-SCRM Controls.

The cybersecurity & privacy program must assign maturity targets to define organization-specific "what right looks like" for controls. This establishes attainable criteria for People, Processes, Technologies, Data & Facilities (PPTDF) requirements. Tailored maturity level criteria can be used to plan for, budget for and assess against. Maturity targets should support the organization's need for operational resiliency.

This step has 4 subcomponent steps:

- **3a.** Establish organization-wide maturity criteria for people, processes and technology.
- **3b.** Establish maturity criteria for sensitive data and/or critical systems, applications and services.
- **3c.** Develop & implement a resource plan (e.g., business plan, budget, road map, etc.) to meet compliance obligations.
- **3d.** Prioritize objectives from the resource plan for PPTD requirements.

4. Publish Policies & Standards for C-SCRM.

Documentation must exist, otherwise an organization's cybersecurity and data protection practices are unenforceable. Formalizing organization-specific requirements via policies and standards are necessary to operationalize controls. Documented policies and standards provide evidence of due diligence that the organization identified and implemented reasonable steps to address its applicable requirements.

This step has 2 subcomponent steps:

- **4a.** Publish organization-wide cybersecurity and data protection policies to address applicable security and data protection requirements.
- **4b.** Publish standards to enforce cybersecurity and data protection policies.

5. Assign Stakeholder Accountability.

Controls must be assigned to stakeholders to ensure accountability (e.g., business units, teams and/or individuals). These "control owners" may assign the task of executing controls to "control operators" at the Individual Contributors (IC)-level. Stakeholders utilize the prescriptive requirements from policies and standards to develop Standardized Operating Procedures (SOP) that enable ICs to execute those controls. The documented execution of procedures provides evidence of due care that reasonable practices are being performed.

This step has 5 subcomponent steps:

- **5a.** Identify "control owners" for all applicable cybersecurity and data protection controls. These are the individuals or teams responsible for the control.
- **5b.** Identify the "control operators" for all applicable cybersecurity and data protection controls. These are the individuals or teams executing the control.
- **5c.** Stakeholders ensure control owners develop documented SOP to address the control objective(s).
- **5d.** Stakeholders ensure control owners develop a System Security Plan (SSP) to document the "who, what, how, why, when & where" for products & services.
- **5e.** Formalize access agreements for internal and external personnel, including rules of behavior for critical technologies.

6. Maintain Situational Awareness - Establish An Internal Audit (IA) Capability

Situational awareness must involve more than merely "monitoring controls" (e.g., metrics). While metrics are a point-in-time snapshot into discrete controls' performance, the broader view of metrics leads to a longer-term trend analysis. When properly tied in with current risk, threat and vulnerability information, this insight provides "situational awareness" that is necessary for organizational leadership to adjust plans to operate within the organization's risk threshold.

An organization's Internal Audit (IA) function provides quality control. This function can help validate the scope and impact of risk, which stakeholders may be unaware of. IA practices generate evidence of due care that reasonable steps are in place to validate stakeholder claims and assumptions.

This step has 10 subcomponent steps:

- **6a.** Create a detailed asset inventory for all business-critical systems, applications and services (internally hosted as well as those hosted by third-parties).
- **6b.** Create a detailed data inventory for all sensitive data, including "crown jewels" Intellectual Property (IP).
- **6c.** Create a detailed inventory of contracts that flow-down sensitive data to External Service Providers (ESP).
- **6d.** Create a detailed network diagram that includes ESPs and the geographic location where data is stored, transmitted and/or processed.
- **6e.** Create a detailed inventory of ESP that make up the Direct Supply Chain (DSP) (e.g., direct contracts).
- **6f.** Categorize ESP based to identify their criticality to the organization's mission and business processes, per LOB
- **6g.** Create a Data Flow Diagram (DFD) that shows how sensitive data from the organization to ESP, including the ESP's subcontractors.
- **6h.** Inventory ESP access control for both critical systems and sensitive data.
- **6i.** Develop C-SCRM -specific metrics.
- **6j.** Identify key stakeholders for a Quarterly Business Review (QBR) on C-SCRM metrics and issues.

7. Manage Risk.

Proactive risk management processes must exist across all phases of development/information/system life cycles to address confidentiality, integrity, availability and safety aspects. Risk management must address internal and external factors, including cybersecurity, privacy and C-SCRM considerations. To manage risk, it requires the organization to enforce a clearly defined risk threshold and ensure reasonably-expected secure practices are operational.

This step has 3 subcomponent steps:

- **7a.** Develop & implement a Risk Management Program (RMP) to identify, assess and remediate risk.
- **7b.** Perform a gap assessment from applicable statutory, regulatory and contractual obligations.
- **7c.** Create a Plan of Action & Milestone (POA&M) to track and remediate deficiencies.

8. Change Control.

Develop & implement change control processes and workflows, including a Change Control Board (CCB) that is technically competent to evaluate security ramifications for baseline security configuration deviations.

9. Centralized Configuration Management Plan (CMP).
Develop and implement a centralized Configuration Management Plan (CMP) to enforce secure configurations.

10. System Hardening.
Identify, build & implement secure baseline configurations (e.g., hardening standards) for all technology platforms.

11. Incident Response.
Develop & implement incident response capabilities to detect, respond to and recover from incidents.

12. Physical Security.
Develop & implement physical security capabilities to detect, respond to and recover from physical security incidents.

13. Continuous Monitoring.
Develop & implement continuous monitoring capabilities through log collection and analysis (e.g., SIEM).

14. Identity & Access Management (IAM).
Develop & implement Identity & Access Management (**IAM**) to address "least privilege" and Role-Based Access Control (RBAC).

15. Network Security.
Develop & implement network security practices.

16. Maintenance.
Develop & implement proactive maintenance practices.

17. Attack Surface Management (ASM).
Develop & implement Attack Surface Management (**ASM**) practices as part of a broader Vulnerability & Patch Management Program (VPMP).

18. Threat Intelligence.
Develop & implement a threat intelligence capability.

19. Business Continuity.
Develop & implement business continuity capabilities (e.g., Disaster Recovery (DR), Business Continuity (BC), Continuity of Operations (COOP), etc.).

20. Security Awareness Training.
Build and maintain a security-minded workforce through training & awareness.

21. Tamper Resistance & Detection.
Develop & implement tamper resistance and detection capabilities.

22. Information Assurance Program (IAP).
Develop & implement an Information Assurance Program (IAP) to validate control implementation.

23. Decommissioning & Migration.
Develop & implement system application and service decommissioning and migration capabilities.

24. Supply Chain Protections.
Implement and monitor supply chain protections (contractual obligations, assessments & monitoring compliance).

APPENDIX A: DOCUMENTATION TO SUPPORT ZERO TRUST & SUPPLY CHAIN RISK MANAGEMENT

The purpose of a company's cybersecurity documentation is to prescribe a comprehensive framework for:

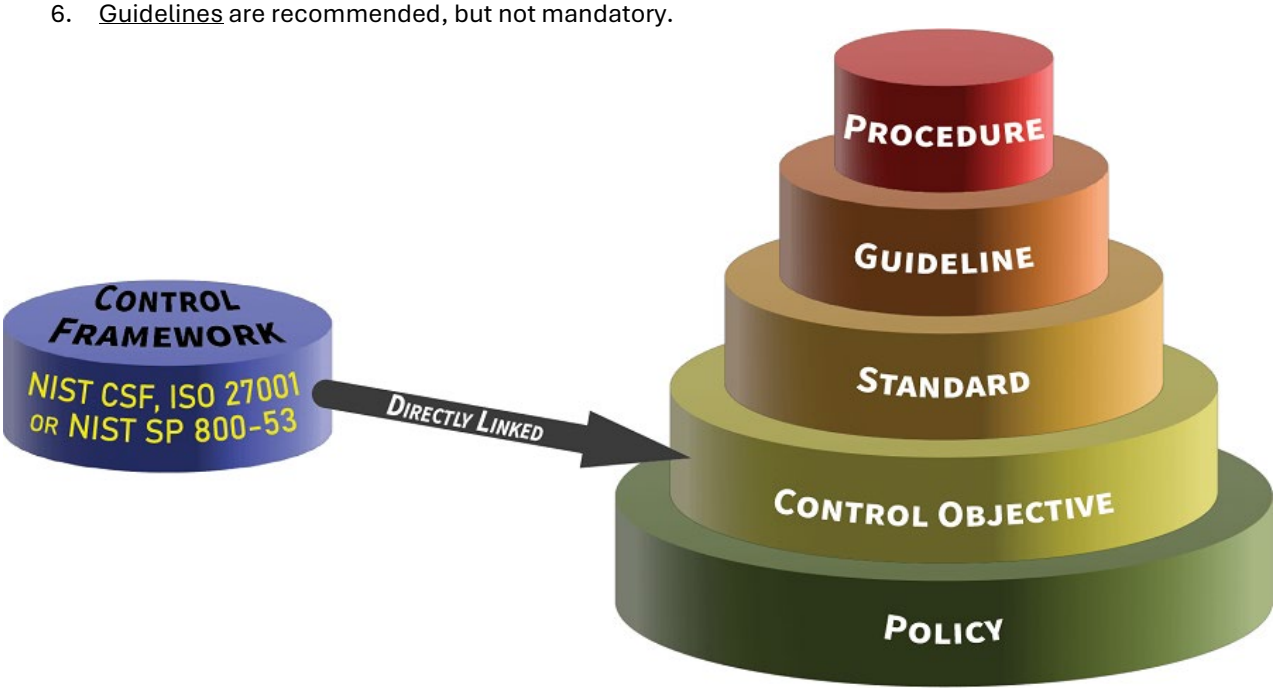
- Creating a clearly-articulated approach to how your organization handles cybersecurity and data protection practices.
- Protecting the confidentiality, integrity, availability and safety of data and systems across the enterprise.
- Providing guidance to help ensure the effectiveness of cybersecurity and data protection controls that are put in place to support your company's operations.
- Helping an organization's users recognize the highly-networked nature of the current computing environment to provide effective organization-wide management and oversight of those related cybersecurity and data protection controls.

Documentation works best when it is simple and concise. Conversely, documentation fails when it is overly wordy, complex or difficult for users to find the information they are seeking. When you picture this from a hierarchical perspective, everything builds off of the policy and all of the components of cybersecurity and data protection documentation building off each other to make a cohesive approach to addressing applicable requirements:

CYBERSECURITY DOCUMENTATION COMPONENTS

In the context of good cybersecurity documentation, components are hierarchical and build on each other to build a strong governance structure that utilizes an integrated approach to managing requirements. 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.

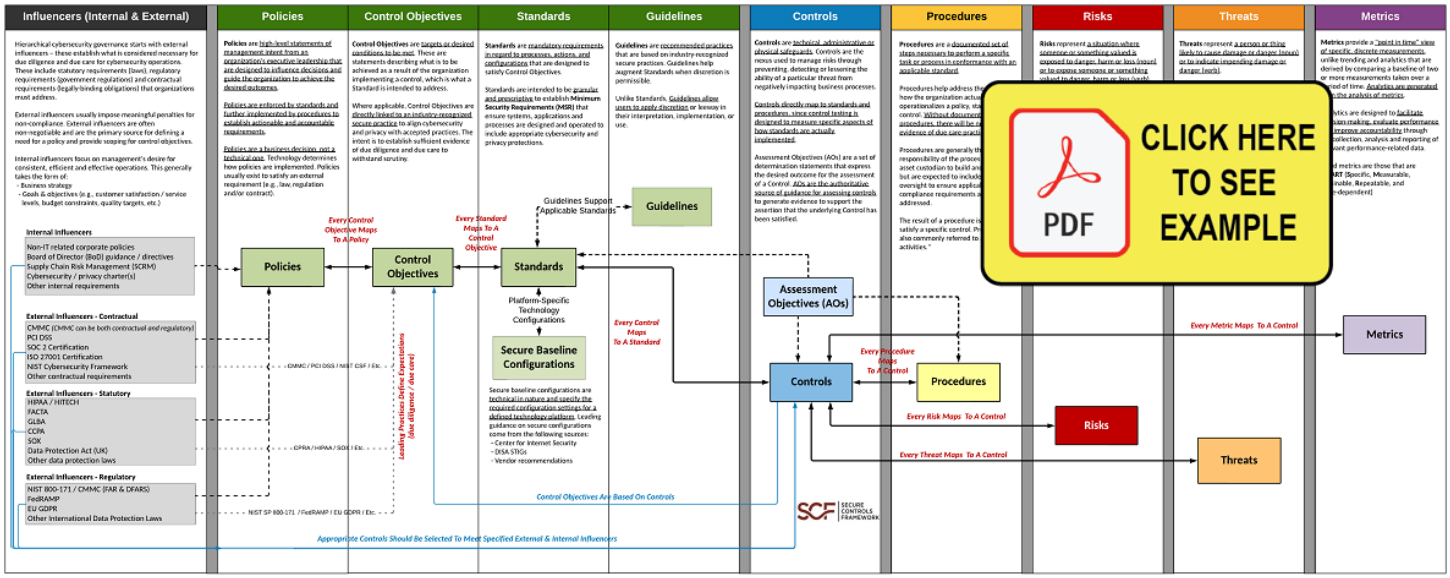


Cybersecurity Documentation Hierarchy – Understanding How Cybersecurity Documentation Is Connected

When you look at establishing cybersecurity and data protection documentation, it all starts with influencers – these influencers set the tone and establish what is considered to be due care for cybersecurity and data protection practices:

- External Influencers - This includes a wide-range of compliance obligations that an organization has to address:
  - Statutory requirements (laws);
  - Regulatory requirements (government regulations); and
  - Contractual requirements (legally-binding agreements); and
- Internal Influencers - These are business-driven and the focus is more on executive management's desire for consistent, efficient and effective operations.

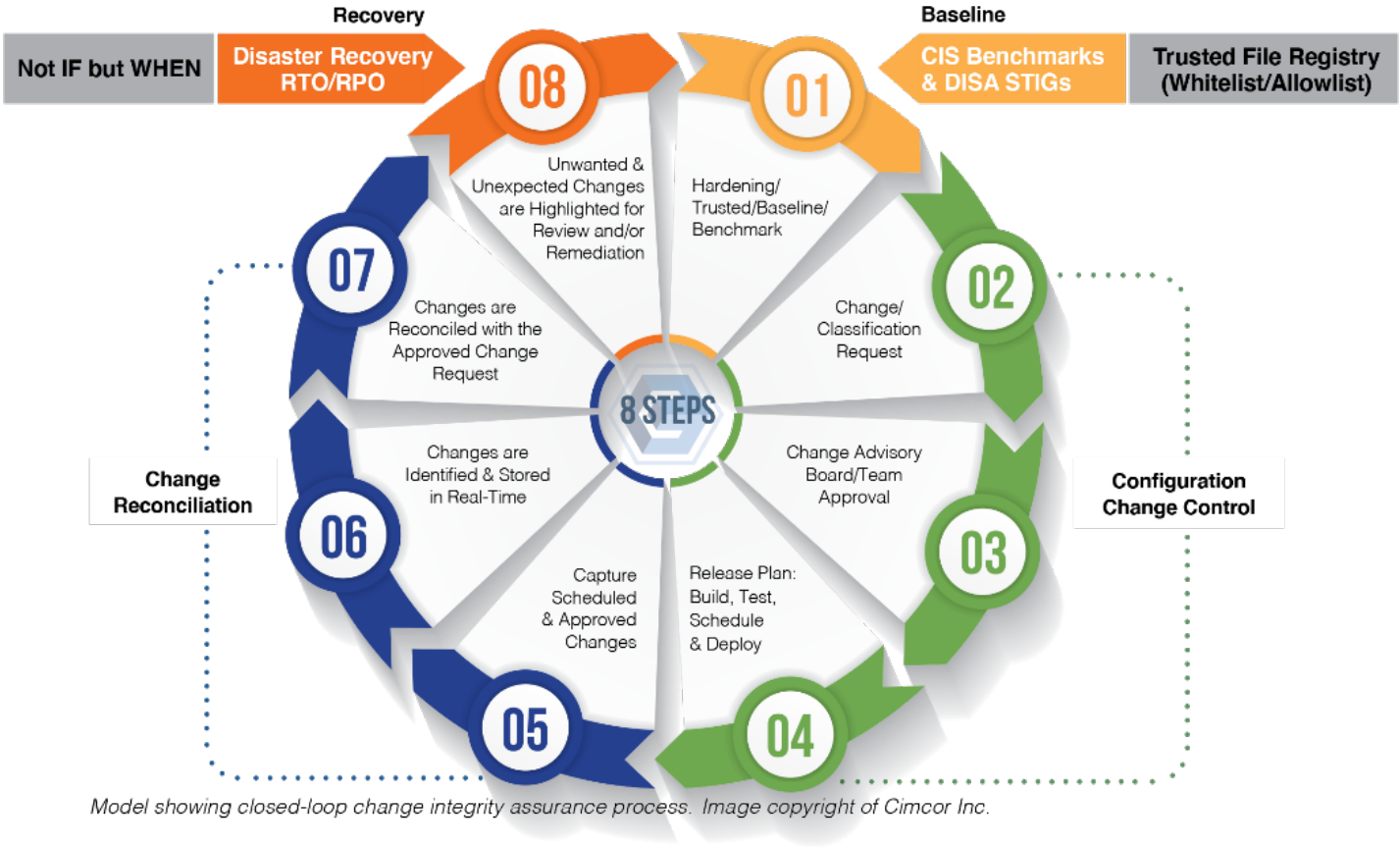
ComplianceForge developed the Hierarchical Cybersecurity Governance Framework (HCGF) to help visualize this. When documentation is all laid out properly, your company's cybersecurity documentation show flow like this where your policies are linked all the way down to metrics:



[image is downloadable from: https://complianceforge.com/content/pdf/complianceforge-hierarchical-cybersecurity-governance-framework.pdf]

Appendix B: Baselines, Configuration Change Control, Change Reconciliation & Recovery

What baselines (secure baseline configurations / hardening), configuration change control, change reconciliation and recovery have in common is these controls are requirements in almost all major security frameworks. Cimcor, Inc. developed an 8-step, closed-loop workflow that emphasizes detective controls and assembles those them into an industry-leading, practices-based process. When paired with automation, this workflow enables an unprecedented ability to identify unknown, unwanted and unauthorized changes to your IT and cloud assets in real-time and provides facilities to remediate either manually or automatically.



Model showing closed-loop change integrity assurance process. Image copyright of Cimcor Inc.

Four key areas where Cimcor's model supports the C-SCRM Kill Chain model includes:

(1) **Baselines (Secure Baseline Configurations / Hardening).** Validate and verify that your infrastructure is hardened and secure with industry-recognized security baselines as a mechanism to establish a trusted baseline configuration. Couple this with a whitelist/allowlist database that can verify the authenticity and integrity of the individual files provides additional assurances of system integrity.

(2) **Configuration Change Control**. The process of regulating and approving changes throughout the entire operational life cycle of an information system from an authoritative baseline. This is traditionally accomplished through traditional IT Service Management (ITSM) products. However, ideally, this functionality should also be included in security platforms or at a minimum, security platforms should be integrated in a manner to support the ticketing process.

(3) **Change Reconciliation**. Highlight, curate and triage observed changes against expected and authorized changes to create a closed-loop change control process. This best practice can drives Mean-Time-To-Identify (MTTI) breaches and Mean-Time-To-Detect (MTTD) breaches down to seconds. Real-time change detection is essential but having the functionality to rapidly respond and remediate those changes is what will ultimately help you achieve and maintain continuous integrity.

(4) **Recovery**. The ability to roll-back and remediate to a last know trusted baseline is a core function that will allows Mean-Time-To-Restore (MTTR) and Mean-Time-To Contain (MTTC) to be measured in seconds. Recovery should be configurable, in a matter that will allow the user to maintain a history of trusted baselines and to roll-back to the most appropriate baseline which will enable full recovery.

The reasons why this is important is straightforward:

(1) Cost. It is generally less expensive to prevent an incident (e.g., ransomware outbreak) that it is to respond to it; and

(2) Time. Automating response processes can both minimize impact and decrease the time associated with the incident, which can help mitigate associated costs.

BASELINES (SECURE BASELINE CONFIGURATIONS / HARDENING)

"Hardening" is the process of securing an asset by reducing its attack surface. That means configuring the asset in a way that reduces the number of tools, techniques and tactics that an attacker can utilize to gain access to it. Once an asset has been hardened, it becomes a trusted reference point from which to manage deviations from to ensure that only expected changes occur. These authorized changes are often referred to as configuration drift or infrastructure drift.

It is important for organizations to integrate CIS Benchmarks, DISA STIGs and Original Equipment Manufacturer (OEM) recommended security practices as a reference point to establish a "hardened" Secure Baseline Configuration (SBC). This reference point can be used to create a chain of evidence which can be produced to validate and verify the expected changes to the hardened state of an asset, system or device. This is where automation is crucial to leverage some form of "Trusted File Registry" database of known and trusted software. This database can be used to validate and verify the authenticity and integrity of the software files themselves through a chain of custody back to the software vendor that published the software.

CONFIGURATION CHANGE CONTROL

The management and control of configurations and baselines for systems, applications and services to enable security and facilitate the management of risk. Any and all deviations from a baseline configuration should be triaged and evaluated via an authorized change management process.

Automated tools, such as CimTrak, can ensure the security and integrity of your critical IT assets by detecting changes to your applications and infrastructure in real-time. When a change is detected, automated processes should provide a detailed audit trail of the incident, including a appropriate forensic information, including but not limited to:

- Who made the change?
- What was changed?
- Where the change was made?
- When the change took place?
- How the change was made?

CHANGE RECONCILIATION

The process of regulating and approving changes throughout the entire operational life cycle of an information system. The workflow process outlined above will be able to highlight and compare observed changes against expected/authorized changes. In the event of an unexpected, unauthorized and unwanted change, it should be immediately highlighted for analysis and remediated if necessary to create a trusted and resilient infrastructure. In the absence of this process, integrity, configuration drift, or infrastructure drift is inevitable!

Without a built-in ticketing system (which is also the integration mechanism to traditional ITSM products if deployed) to manage the process of classifying and approving change, it is nearly impossible to perform change reconciliation activities. This process provides the unique ability to capture the expected changes and reconcile/curate those changes with observed changes to then highlight everything that is unauthorized change on critical systems within your environment. Automated tools, such as CimTrak, should be configured to prevent changes entirely for those files and directories that should never change.

When changes to a system happen, those changes must be considered untrustworthy until a workflow process validates and verifies the integrity of those changes by determining if they were approved and authorized by an authoritative person or Change Advisory Board (CAB). Only until this happens will we be able to identify Zero Day Attacks and fulfill the concept of Zero Trust become a reality.

RESILIENCY / RECOVERY

Often, security professionals will remark, "It's not a matter of if, but when" a security event will occur. With this inevitability in mind, it is extremely important to ensure that the recovery is integrated into your security program. Recovery is the process of mitigating the scenario where the chain of trust is broken for some unforeseen reason. When this happens, having a defined process to ensure the trust and resiliency of the data and infrastructure is paramount. Traditional ITSM products implement recovery functionality for purposes of operational up-time and availability. The terminology of Recovery Time Objective (RTO) and Recovery Point Objective (RPO) are closely aligned with security objectives of Mean-Time-To-Contain (MTTC) as statistics show "change" is the most common cause of both operational downtime and security incidents.

- Recovery Time Objective (RTO): The maximum amount of time that should pass before your IT systems recover.

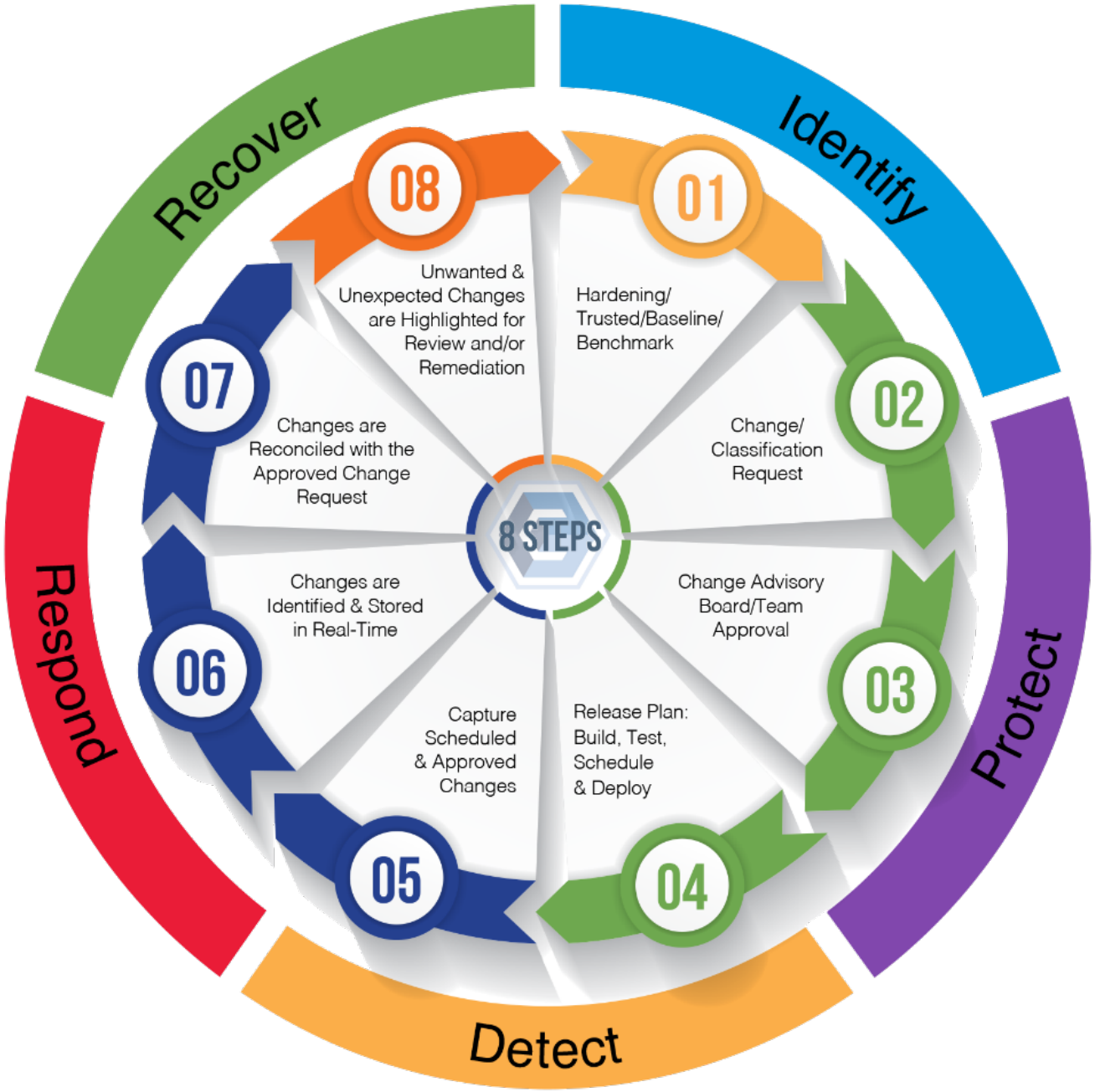
- Recovery Point Objective (RPO): The maximum amount of time permissible since the most recent data backup in order for your IT systems to recover.

Automated tools, such as CimTrak, can restore and recover from unwanted change is measured in seconds which differs from traditional ITSM back-up and restoration functionality of reprovisioning. It is necessary to have the ability to discreetly identify and restore the necessary files from any number of previously trusted baselines to avoid the costly time and effort of reprovisioning an entire system. Automated tools should be configured to roll-back and remediate changes if and when necessary (manually or automatically), to any previous trusted state(s) as it securely stores the previous files associated with that state of operation in a compressed and encrypted format.

APPENDIX C: NIST CYBERSECURITY FRAMEWORK ALIGNMENT

Cimcor's 8-step, closed-loop security workflow also aligns effectively with the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF). The NIST CSF's five functional requirements of (1) Identity, (2) Protect, (3) Detect, (4) Respond and (5) Recover overlay onto this model, which further supports the C-SCRM Kill Chain approach to prioritizing cybersecurity controls.

When viewed through against the NIST CSF, the C-SCRM Kill Chain, along with Cimcor's security workflow model, focus on the "Identify" and "Protect" nature of cybersecurity controls. The reason for this is it is more cost-effective in the long-term to perform due diligence steps that enact and enforce secure baseline configurations, rather than focusing efforts on "Detect" and "Respond" cybersecurity controls. While this approach does rely upon automated technologies to enforce configurations and revert unapproved changes, the focus on prevention is aimed at implementing and maintaining a sustainable approach to securing an organization's enterprise, regardless of the geographic location of the system, application or service.



APPENDIX D: CRITICAL RESOURCES & ACQUISITION PATH

The premise of the C-SCRM Kill Chain model was to create a proof of concept for an efficient way to plan out a roadmap to successfully implement robust Zero Trust and Cybersecurity Supply Chain Risk Management (C-SCRM) cybersecurity and data protection practices that focus on prevention and automated remediation. The end result is a viable approach for organizations to use in order to create a prioritized project plan for C-SCRM-focused secure practices. This requires taking the organization's critical resources and the acquisition path (e.g., business processes) into consideration.

THEORY OF CONSTRAINTS

As with any process, an organization's cybersecurity & privacy compliance program is always vulnerable due to the ability of the "weakest link" (e.g., person, part, supplier and/or process) to cause damage and adversely affect the overall cybersecurity & privacy compliance program. The theory of constraints (TOC) is a management paradigm that views any manageable system as being limited in achieving more of its goals by a very small number of constraints. There is always at least one constraint in a project/initiative and TOC utilizes a process to identify the constraint(s) and restructure the rest of the organization/processes around it.

MANAGEMENT FOCUS

At the management level, TOC focuses on:

- Define business processes;
- Establish minimum quality requirements for people, processes and technologies;
- Establish, review and enforce contract requirements;
- Appropriately resource technical requirements; and
- Maintain situational awareness.

TECHNICAL FOCUS

At the individual contributor level (e.g., analyst, engineer, technician, etc.), TOC focuses on:

- Define technical requirements;
- Identify and implement "industry recognized practices" to design, build and maintain systems, applications and services; and
- Provide metrics to management to maintain situational awareness.

CHANGE MANAGEMENT WITHIN C-SCRM

As you work through security and privacy controls, it is common that new technology solutions are necessary. This is inevitable and your organization may need to re-factor the C-SCRM Kill Chain as guidance for time and resource constraints.

There are several factors that need to be considered when incorporating new technologies:

1. Define the appropriate technology solution(s) by identifying necessary People, Processes, Technologies, Data & Facilities (PPTDF) (**step 3a**).
2. Identify suitable vendors based on the organization's:
    a. Knowledge of your organization's statutory, regulatory and contractual obligations (**step 2a**);
    b. Ability to fill gaps related to those obligations (**step 5**); and
    c. Ability to perform as expected (e.g., you want to avoid paying someone to be their "Guinea pig" to learn how to implement technologies and/or processes through on-the-job training).
3. Without exception, leverage your organization's change control processes to ensure the technology solutions are documented, reviewed and approved.
    a. Leverage the C-SCRM Kill Chain phases to identify where you will implement and operate the new technology solution to understand possible "cascading effects" of new technologies on other phases.
4. Whenever multiple technology implementations overlap in a C-SCRM Kill Chain phase, be aware of time and resource constraints.
    a. Add time allowances for the procurement, training, configuration and ongoing operation of the new technology solution;
    b. Plan for the possibility that overlapping implementations may:
        i. Extend the time spent in a particular phase of the C-SCRM Kill Chain; and
        ii. Increase labor-related expenses:
            1. Professional services from the vendor or managed IT service providers familiar with the solution; and/or
            2. Technical staff support from another internal team.

5. Integrate new technologies into internal audit practices (**phase 22**) to maintain your Information Assurance (IA) capability and controls governance.
    a. This is the optimal time to develop performance measures (e.g., metrics) for assessing the continued effectiveness of your newly-implemented technology solutions.

APPENDIX E: A CASE FOR ZERO TRUST CONTINUOUS CONFIGURATION ENFORCEMENT

The analogies between traditional supply chain functions (e.g., production, services, value delivery, etc.) and cybersecurity operations (e.g., confidentiality, integrity, availability and safety) may not be immediately apparent. However, as cybersecurity threats continue to disrupt supply chains and critical infrastructure, organizations may soon find the need to apply robust Supply Chain Risk Management (SCRM) practices as part of an overall business survival and resiliency strategy that leverages existing lean manufacturing principles.

In support of the concept of C-SCRM Kill Chain, Toyota operates a supply chain management system designed with monitoring and risk management at its core. The automaker's lean "4P" model (*Philosophy, Process, People and Partners and Problem Solving*) results in a resilient supplier base that is less-affected by trends and short-term disruptions.

Toyota views its suppliers' challenges as its own challenges, since it impacts Toyota's own ability to produce. Toyota fully appreciates the concept that any challenge to Toyota's supply chain is inherently a Toyota problem. Toyota's model often leads to "joint improvement" activities where the automaker practices *genchi genbutsu*. *Note - It may be worthwhile to research the Toyota Production System for yourself to understand the challenge and difficulties Toyota faces, since that may be applicable to your specific business model.*

To help with problem-solving and continuous improvement, Toyota actively involves itself in its suppliers' operations to create a mutually-beneficial outcome. Toyota's involvement to directly monitor its supply chain allows it to understand whether those third-party suppliers can meet Toyota's production needs and that insight empowers Toyota to make adjustments, as necessary. Therefore, rather than being surprised by sudden shortages or disruptions, Toyota's supply chain acts as a sensor to allow it to detect trends well before becoming issues that crest the global horizon.

As with any supply chain, organizations can expect some suppliers to possess fewer resources, expertise and organizational maturity, based on the organization's size and industry. Therefore, during the C-SCRM Kill Chain process, organizations have an opportunity to propagate new competencies and best practices throughout its supply chain. However, deciding to "find out for yourself" where suppliers struggle with cybersecurity is an unsettling proposition: "*What if I discover that my suppliers are less secure than anticipated?"* For the Toyota analogy, the worse option for the automaker is, "*What if I remain blind to supplier shortcomings*?" Toyota's model is aggressively proactive and that has served the organization extremely well. By teaching Toyota's philosophy and processes to its suppliers, Toyota developed more consistent practices among their disparate supply chain and identified threats before realizing those risks upstream.

Reasons why C-SCRM Kill Chain implications from downstream suppliers matter include, but are not limited to:

- Software Bill of Materials (SBOM) security concerns (e.g., insecure protocols)
- Hardware Bill of Materials (HBOM) security concerns (e.g., alternate computer chips due to supply constraints)
- Covered telecommunications equipment or services (e.g., FAR 52.204-25 violation[6])
- Foreign ownership or knowledge-sharing agreements (e.g., intellectual property theft)
- Cross-border data transmission, processing and/or storage (e.g., compliance violation)
- Insecure data governance practices (e.g., compliance violation)
- Data sovereignty (data localization) requirements (e.g., compliance violation)

[6] *FAR52.204-25: Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment - https://www.acquisition.gov/far/52.204-25*