The Cyber Cake

The Future of Department of the Air Force Cybersecurity

Publication Date: 1 May 2025
Office of Primary Responsibility: SAF/CNZ

Table of Contents

Introduction

In a world increasingly reliant on digital infrastructure, the present approach to cybersecurity and its many management responsibilities poses significant national security risks, particularly as we strive to secure information ecosystems from emerging threats. The cyber cake draws upon known standards of excellence and required activities to ensure that our Airman and Guardians can govern, identify, protect, detect, respond, recover, and defend from all adversaries in the cyber domain.

Cake making, once a complicated process, is now simplified and accessible to everyone, typically involving common ingredients like flour, sugar, and eggs, with additional options like fruit and extracts, but requiring adherence to recipes to produce a desired outcome. A complete cake typically consists of multiple elements, including a sturdy base or foundation, a decorative serving plate or platter, one or more layers of cake itself, and a final topping, which can range from a simple dusting of powdered sugar to an elaborate frosting or decorative design.

Much like baking an actual cake, baking a cyber cake follows the same concepts: there are ingredients that must be used, processes that must be followed, and variations that can be used to yield a desired outcome. Similarly, this process requires a solid foundation, a well-presented framework, multiple layers of depth, and a visually appealing finish. In a cyber cake, each layer acts as a "check and balance" approach for cybersecurity and is mapped to specific assessment modalities required to validate that all steps were properly performed.

Although the cyber domain continues to evolve, the basic approach is to build a base of foundational knowledge and remove the concept of compliance for compliance's sake, often associated with cyber. The result of the cyber cake concept is to "bake in cybersecurity" and compliance becomes a strategy to measure for resilience. The foundation of a cyber cake starts with the Federal Information Processing Standards (FIPS). NIST's Risk Management Framework (RMF) serves as the platter and serving plate on which the rest of the cyber cake sits. The layers of the cyber cake are Supply Chain Risk Management (SCRM), Cyber Supply Chain Risk Management (C-SCRM), the Cyber Resilience Engineering Framework (CREF), the MITRE ATT&CK Framework, and Zero Trust. Each layer comprises a set of strategies, assessments, and governance methods that work together to establish a robust cybersecurity posture, enabling organizations to effectively mitigate cyber threats and maintain resilient cybersecurity in the face of fragile governance standards in a rapidly evolving cyber landscape.

Critical concepts like Artificial Intelligence, Privacy, Controlled Unclassified Information, and the Secure Software Development Framework represent the frosting and candles.

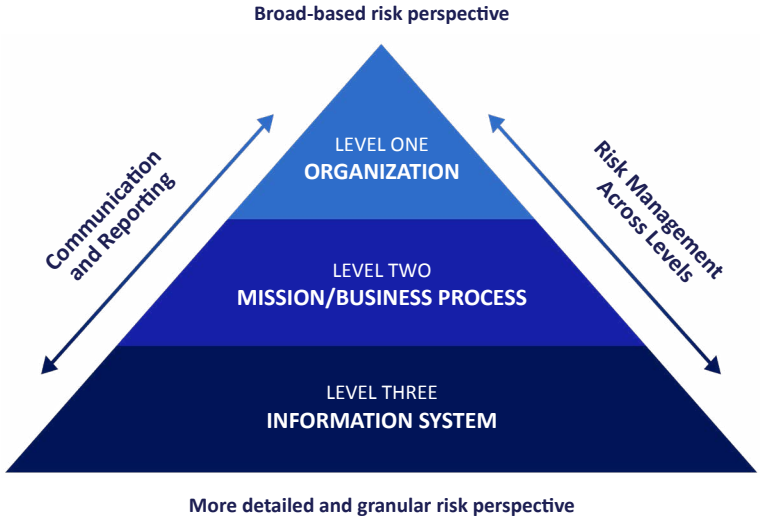


Figure 1: Organizational Risk Management Approach

Finally, the NIST CSF 2.0 represents the cake slice. With the CSF 2.0 an organization can assess how the base, layers, and toppings of its cybersecurity posture interact and work together and evaluate how well the cybersecurity measures are integrated into the it's systems and processes (see Figure 1). Every cyber cake is different, and the CSF 2.0 allows an organization to taste test how well it followed its recipe.

The Challenge

Cyberspace is a complex, multidimensional domain that encompasses not only conflict, but also communication, commerce, and societal development, as depicted in Figure 2. The knowledge base is inherently fragmented, as no single individual can master all the diverse areas represented—ranging from systems administration and information security to social, political, and economic dimensions. This highlights the reality that there is no true "cyberspace expert"; rather, it is a domain that demands collaboration across disciplines and expertise. This intricate interplay of disciplines is further complicated by the numerous governing directives that dictate how these various aspects must operate in concert. This inherent complexity often leads to a fragmented approach to cybersecurity, where individual security measures are implemented in isolation, leaving gaps that attackers can exploit.

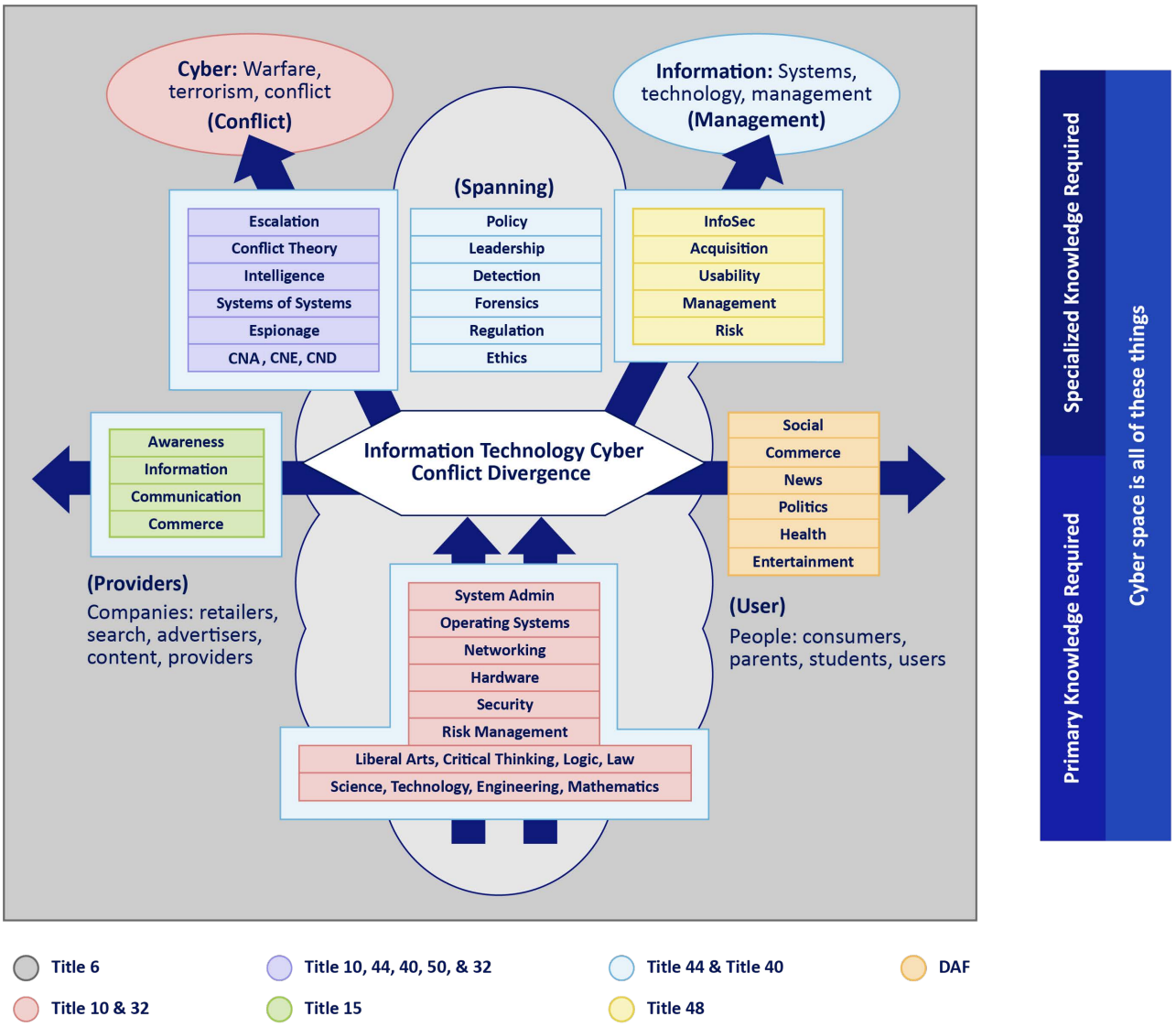


Figure 2: The Cyber Paradigm

The Challenge

Professionals, overwhelmed by the sheer vastness and intricacy of the cybersecurity landscape, find themselves seeking a clear path and reliable tools to achieve a truly resilient cybersecurity posture. However, this quest is often hindered by the fragmented approach itself. Instead of addressing cybersecurity holistically, crucial elements are often overlooked or implemented in isolation. Each neglected component—from inadequate technical controls to insufficient risk management practices—weakens the overall structure, making defenses crumble under pressure and leaving critical missions vulnerable to cyber attacks.

Organizations may believe they are protected because they have implemented some security measures, but without a holistic approach, they are still at risk, their defenses plagued by weaknesses that adversaries can readily exploit. Trying to fix cybersecurity shortcomings after the fact is like trying to frost a cake that's already collapsing, its foundation crumbling on a cracked plate. You can try to mask the damage, but the integrity of the entire structure is compromised, rendering the final product unreliable and prone to further disaster. Similarly, in cybersecurity, neglecting the fundamentals can undermine even the most advanced technologies—no amount of sophistication can compensate for a weak core. It's significantly harder—and far more costly—to try to salvage a crumbling cybersecurity posture than it is to build a strong foundation from the start.

Imagine the impact of a compromised air traffic control system, the inability to deploy troops due to a network outage, or the loss of classified information vital to national security. In today's contested environment, these threats are all too real, demanding a fundamentally different approach to cybersecurity—one that provides a robust framework and proven strategies for professionals to navigate this complex landscape.

The Cyber Cake concept addresses this challenge by providing a structured, transparent framework that demystifies cybersecurity, making it more accessible and achievable for everyone. Through the Cyber Cake, organizations can replace ambiguity with clarity, transforming cybersecurity from a daunting obstacle course into a series of manageable steps toward a more secure and resilient future. This layered approach acts as a detailed recipe for success, guiding organizations through each critical stage of building and measuring a strong security program. Each layer of the cake represents a foundational element, offering tangible steps and proven strategies that empower professionals at all levels to not only grasp the "why" behind essential security measures but also to confidently implement and assess them. By meticulously following the Cyber Cake recipe, organizations gain both a clear understanding of their implemented security measures and a roadmap for prioritizing future efforts, ultimately establishing a stronger, more informed cybersecurity posture.

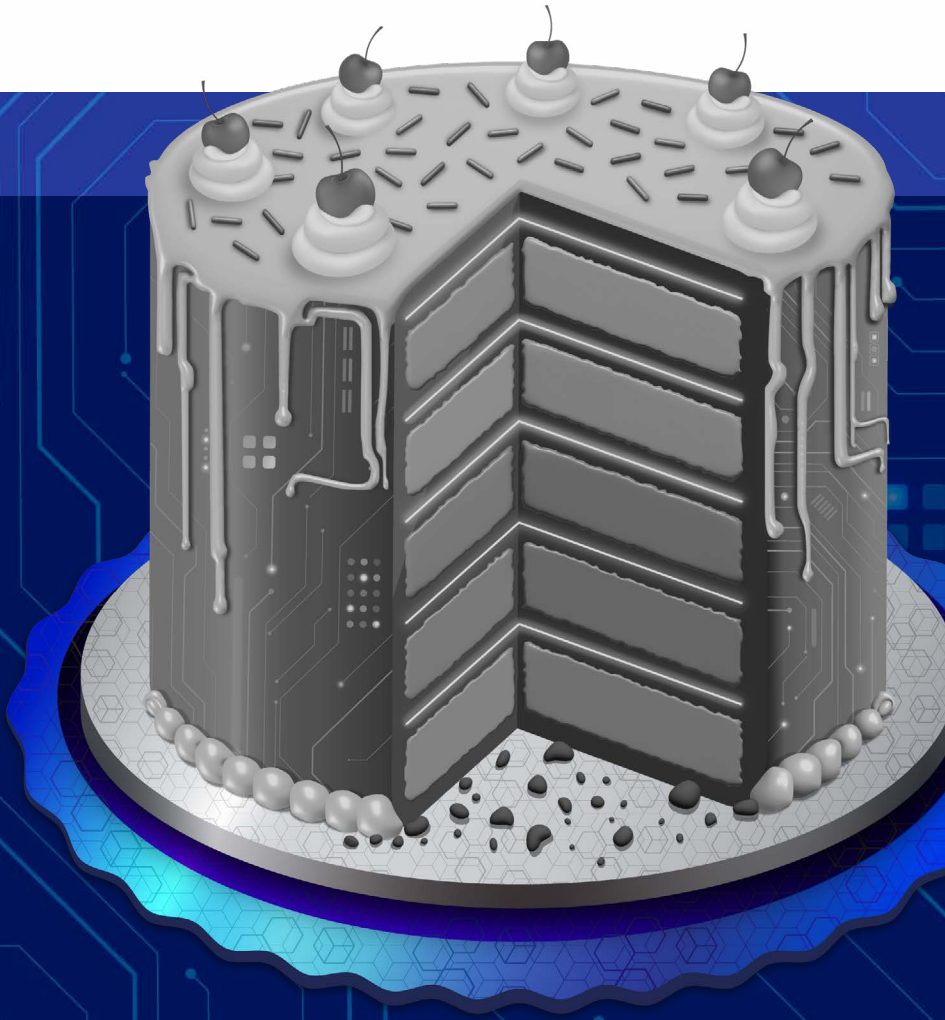
The Base: FIPS Strategy

*The base of a cyber cake starts with the **Federal Information Processing Standards (FIPS)** and is the base that supports and enables the presentation of the cake platter. FIPS are standards for federal computer systems that are developed by the National Institute of Standards and Technology (NIST) and approved by the Secretary of Commerce in accordance with the Information Technology Management Reform Act of 1996 and Computer Security Act of 1987.*

These standards are developed when there are no acceptable industry standards or solutions for a particular government requirement. FIPS standards provide a framework for secure practices, such as encryption, authentication, and access control. Familiarity with FIPS helps practitioners implement robust security controls for attaining a robust cybersecurity posture. It is important to remember that 6 USC § 1500(g)(1) defines cybersecurity posture as the ability to identify, to protect against, to detect, to respond to, and to recover from an intrusion in an information system the compromise of which could constitute a cyber attack or cyber campaign of significant consequence. FIPS also provides guidelines for risk management, including risk assessment, mitigation, and monitoring, and although FIPS are developed for use by the Federal Government, many in the private sector voluntarily use these standards.

Core FIPS Cookbooks

1. **FIPS 199, Standards for Security Categorization of Federal Information and Information Systems,** ***https://csrc.nist.gov/pubs/fips/199/final***
2. **FIPS 200, Minimum Security Requirements for Federal Information and Information Systems,** ***https://csrc.nist.gov/pubs/fips/200/final***
3. **FIPS 140-3, Security Requirements for Cryptographic Modules,** ***https://csrc.nist.gov/pubs/fips/140-3/final***
4. **FIPS 201-3, Personal Identity Verification (PIV) of Federal Employees and Contractors** ***https://csrc.nist.gov/pubs/fips/201-3/final***



The Platter: RMF Strategy

*NIST's **Risk Management Framework (RMF)** serves as the platter on which the rest of the cyber cake sits. RMF is a structured approach that organizations use to identify, assess, and mitigate risks systematically and serves as a critical first step to safeguarding information and systems.*

Core RMF Cookbooks

1. NIST SP 800-30, Guide for Conducting Risk Assessments, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf
2. NIST SP 800-39, Managing Information Security Risk, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf
3. NIST SP 800-37, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, *https://csrc.nist.gov/pubs/sp/800/37/r2/final*
4. NISP SP 800-53r5, Security and Privacy Controls for Information Systems and Organizations, *https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final*
5. NIST SP 800-53a, Assessing Security and Privacy Controls in Information Systems and Organizations, *https://csrc.nist.gov/pubs/sp/800/53/a/r5/final*
6. NIST SP 800-53b, Control Baselines for Information Systems and Organizations, *https://csrc.nist.gov/pubs/sp/800/53/b/upd1/final*
7. DAFI 17-101, Risk Management Framework (RMF) for Department of the Air Force (DAF) Information Technology (IT), *https://static.e-publishing.af.mil/production/1/saf_cn/publication/afi17-101/afi17-101.pdf*

Federal law and DoD and DAF policies emphasize a risk-based approach to cybersecurity (see Figure 3), and the RMF helps agencies identify, prioritize, and manage cybersecurity risks effectively. The RMF assigns responsibilities and prescribes procedures for executing and maintaining cybersecurity risk management within the Department of Defense (DoD). The RMF is technology neutral and is applicable to any type of information system without modification and users can tailor controls, control implementation details, and control assessment methods to accommodate various types of IT resources. The RMF at its core provides a dynamic and flexible approach to effectively manage security and privacy risks, the RMF complements an organization's risk management process and cybersecurity program, emphasizing collaboration and informed decision-making. The RMF is used to authorize the operation of information systems, which involves assessing the security controls and risks associated with the system. Practitioners who know the RMF can ensure that their systems are properly authorized and that security controls are in place to mitigate risks. The RMF also takes a lifecycle approach to risk management, which means that risk is managed throughout the entire lifecycle of the system, from design to disposal. Practitioners who understand the RMF can ensure that risk is managed at every stage of the system's life cycle.

- **Prepare:** Essential activities to prepare the organization to manage security and privacy risks.
- **Categorize:** Categorize the system and information processed, stored, and transmitted based on an impact analysis.
- **Select:** Select the set of NIST SP 800-53 controls to protect the systems based on risk assessment(s).
- **Implement:** Implement the controls and document how controls are deployed.
- **Assess:** Assess to determine if the controls are in place, operating as intended, and producing the desired results.
- **Authorize:** A senior official makes a risk-based decision to authorize the system (to operate).
- **Monitor:** Continuously monitor control implementation and risks to the system.

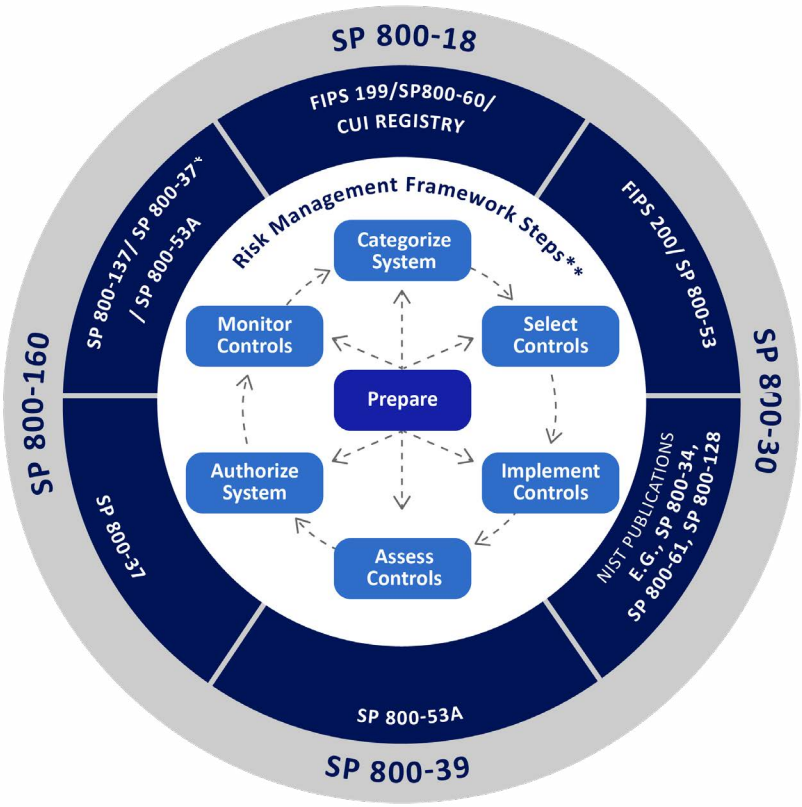


Figure 3: Risk-Based Approach

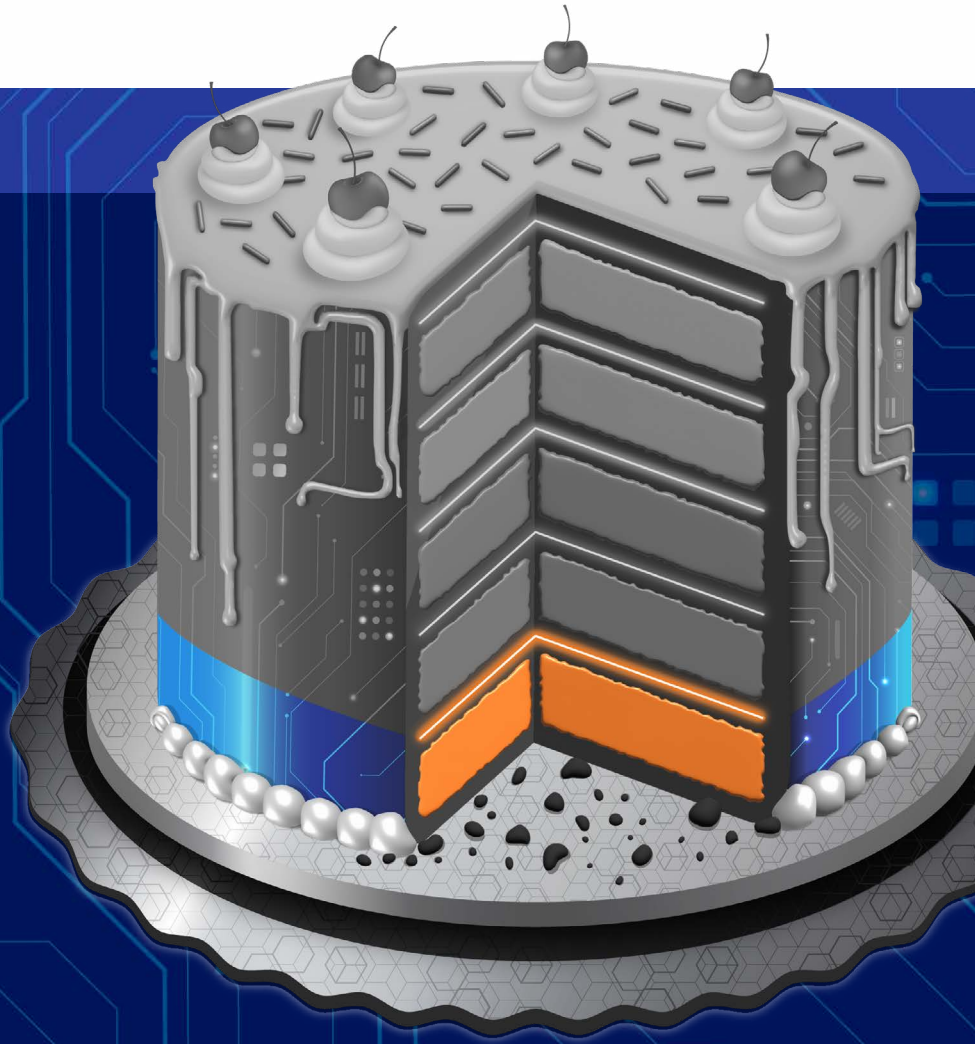
Just as the RMF is the platter for the Cyber Cake, the Prepare step is the foundation of the RMF. A well-executed Prepare step ensures that organizations fully understand their systems, data, and operational context, enabling them to make informed risk management decisions throughout the remaining RMF lifecycle. By thoroughly defining the scope and boundaries of their systems, organizations gain the clarity needed to effectively assess risks, select appropriate controls, and ultimately attain a resilient cybersecurity posture. Neglecting preparation, however, can lead to misaligned controls, ineffective security measures, and an ultimately weaker cybersecurity posture. Investing the time and effort upfront to get the Prepare step right is an investment in the long-term security and resilience of the entire organization.

Layer One: SCRM Strategy

*The first layer of the cyber cake is **Supply Chain Risk Management (SCRM)**. SCRM is a systematic process for managing supply chain risk by identifying susceptibilities, vulnerabilities, and threats throughout the supply chain and developing mitigation strategies to combat those threats, whether presented by the supplier, the supply product and its subcomponents, or the supply chain itself. The supply chain refers to the network of organizations, people, and activities involved in the production and delivery of a product or service.*

Core SCRM Cookbooks

1. **Title 10 USC Section 3252, Requirements for Information Relating to Supply Chain Risk, *https://www.govinfo.gov/content/pkg/USCODE-2023-title10/pdf/USCODE-2023-title10-subtitleA-partV-subpartB-chap223-sec3252.pdf***
2. **DoDI 5200.44, Protection of Mission Critical Functions to Achieve Trusted Systems and Networks, *https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodi/520044p.pdf***
3. **DFARS Subpart 239.73, Requirements for Information Relating to Supply Chain Risk, *https://www.acquisition.gov/dfars/subpart-239.73-requirements-information-relating-supply-chain-risk***



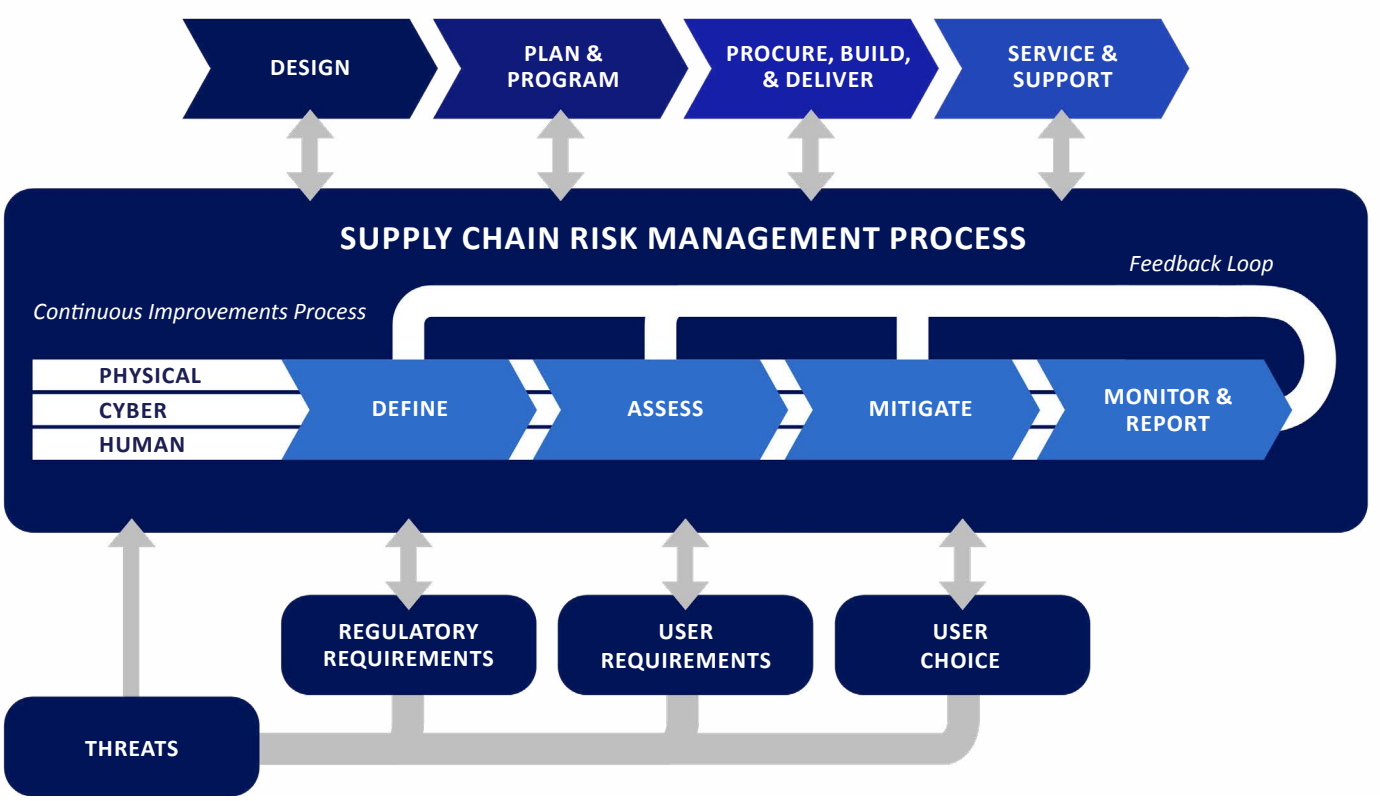


Figure 4: Supply Chain Risk Management

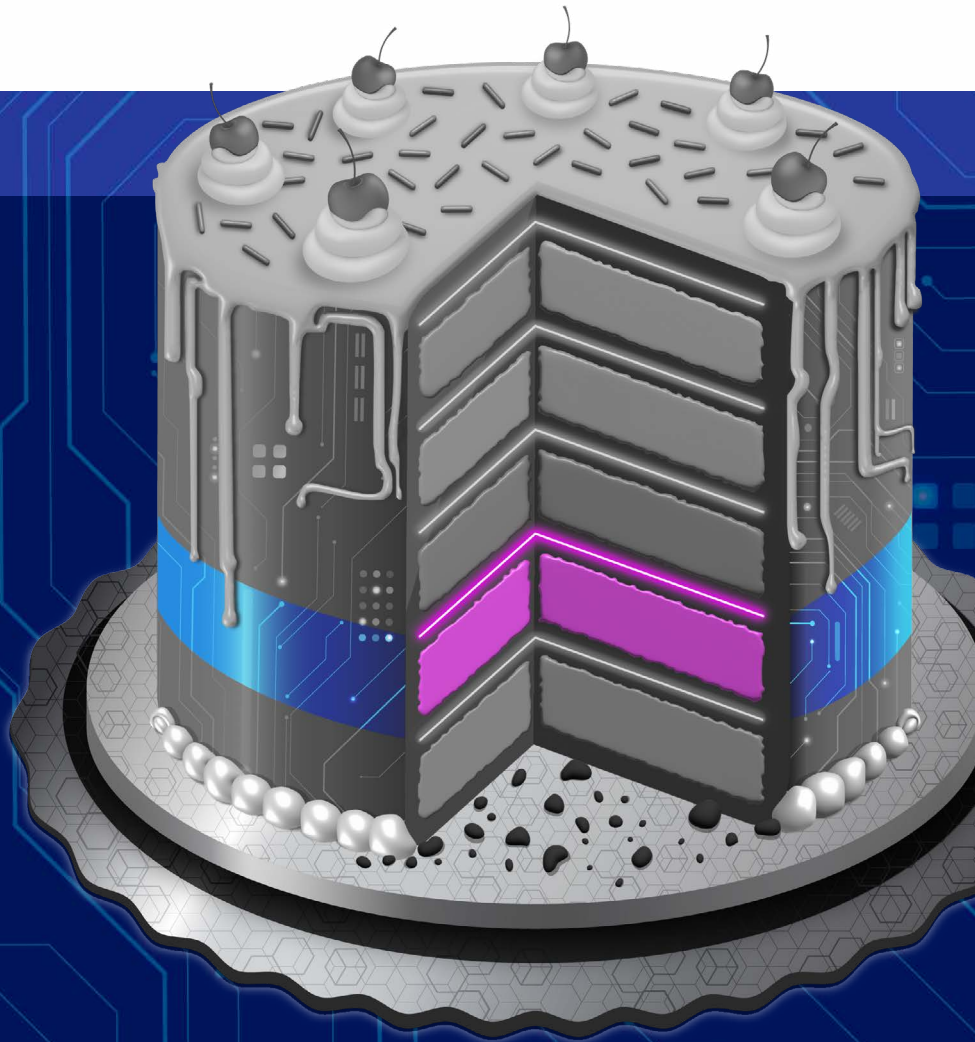
The Supply Chain Risk Management (SCRM) process is an essential component of overall risk management and helps organizations to define potential risks and vulnerabilities in the supply chain, assess the likelihood and impact of these risks, develop strategies to mitigate or manage these risks, and monitor and review the effectiveness of these strategies, as seen in Figure 4.

The figure also illustrates how the process is influenced by various external factors such as threats, legislative requirements, voluntary compliance to environmental risks, user requirements and choices. After defining, assessing, and mitigating risks across the physical, cyber, and human aspects of the supply chain, the process involves a feedback loop for continuous improvement ensuring resilience and minimizing potential disruptions. To be most effective, this approach should be integrated into the asset's lifecycle which begins in the design stage and follows through to service & support.

SCRM is important to protect United States' national security interests and minimize disruptions to military operations by ensuring the integrity and reliability of critical systems and components. By doing so, organizations can safeguard sensitive technologies and intellectual property, and enhance the resilience of global logistics and supply chains.

Layer Two: C-SCRM Strategy

Cybersecurity Supply Chain Risk Management (C-SCRM) *is the next layer in the cyber cake and complements the flavors of the below layer, SCRM. In today's digital landscape, C-SCRM is a critical subset of SCRM that specifically focuses on managing the cyber-related risks and threats associated with the supply chain, such as data breaches, malware, and other cyber attacks.*



Core C-SCRM Cookbooks

1. **NIST SP 800-161, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations,** ***https://csrc.nist.gov/pubs/sp/800/161/r1/upd1/final***
2. **NIST SP 1326, NIST Cybersecurity Supply Chain Risk Management: Due Diligence Assessment Quick-Start Guide,** ***https://csrc.nist.gov/pubs/sp/1326/ipd***
3. **NIST SP 1305, NIST Cybersecurity Framework 2.0: Quick-Start Guide for Cybersecurity Supply Chain Risk Management (C-SCRM),** ***https://csrc.nist.gov/pubs/sp/1305/final***
4. **DoD Strategy and Implementation Plan for ICT and Services Supply Chain Risk Management Assurance,** ***https://dodcio.defense.gov/Portals/0/Documents/Library/ICT-ServicesSupplyChain-RMA.pdf***
5. **DoD Information and Communications Technology Supply Chain Risk Management Home Page,** ***https://cyber.mil/ict-scrm***

It is essential to understand that SCRM encompasses a broad range of risks and threats related to the entire supply chain, including physical, logistical, and other operational risks. Fundamental performance of C-SCRM is built upon the principles and processes established by the RMF, which provides a structured and comprehensive approach to identifying, assessing, and managing risks applied to cybersecurity. C-SCRM is a systematic process for managing exposure to cybersecurity risks throughout the supply chain and developing appropriate response strategies, policies, processes, and procedures at all levels of the organization. Cybersecurity risks throughout the supply chain refer to the potential for harm or compromise that may arise from suppliers, their supply chains, their products, their services, or their use of Information and Communications Technology (ICT) and Operational Technology (OT). C-SCRM is focused on managing the risks introduced by cyber threats to the supply chain by conducting a threat analysis and vulnerability assessment to determine the likelihood and impact of the event at all levels of the organization.

Quality C-SCRM strategies foster a culture of awareness across all organizational levels to highlight its importance and the potential consequences of failure. C-SCRM ensures security by maintaining the confidentiality, integrity, and availability of supply chain information and participants, while also emphasizing the suitability, safety, reliability, and quality of products and services, as depicted in Figure 5, to meet enterprise needs and adapt to changing conditions. These dimensions are essential factors that should be considered when adopting C-SCRM.

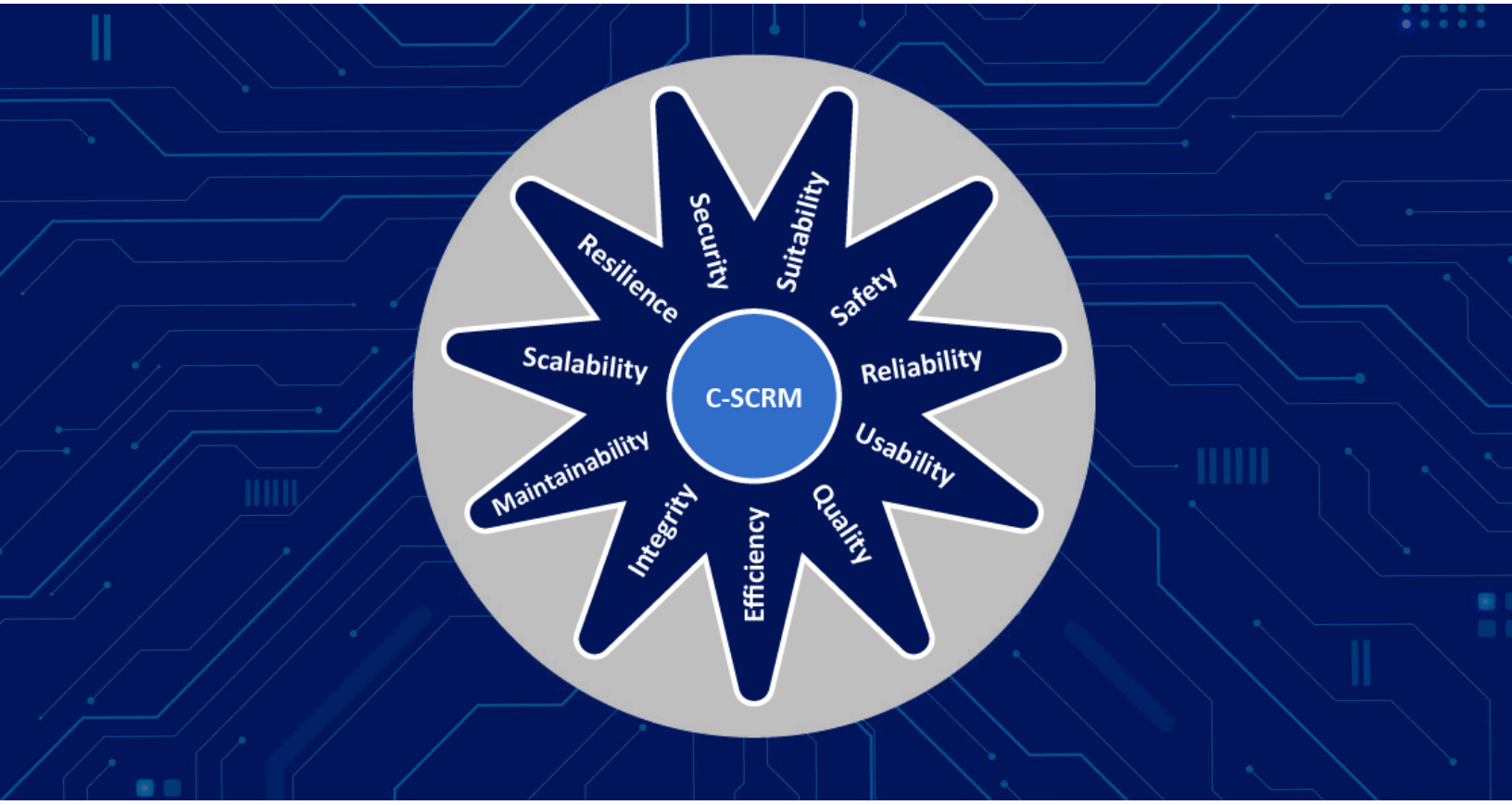


Figure 5: Lenses of C-SCRM

Much like traditional risk management practices, C-SCRM is a critical process that involves a thorough threat analysis, vulnerability assessment, likelihood assessment, and impact analysis to identify and mitigate cyber threats to an organization's supply chain, as depicted in Figure 6.

- **Threat Analysis:** C-SCRM begins with a thorough threat analysis, identifying potential threats that could impact the supply chain. This includes understanding the sources of threats, and their possible effects on the supply chain. Threats can be adversarial (e.g., insertion of malware, industrial espionage) or non-adversarial (e.g., natural disasters, poor quality products/services).
- **Vulnerability Assessment:** Following threat analysis, C-SCRM conducts a vulnerability assessment to identify weaknesses within the supply chain that could be exploited by identified threats. Vulnerabilities can be external (e.g., part of an organization's supply chain) or internal (e.g., organizational procedures).
- **Likelihood Assessment:** C-SCRM then assesses the likelihood of identified threats exploiting vulnerabilities. For adversarial threats, this involves evaluating the capability and intent of potential attackers. For non-adversarial threats, it involves analyzing the historical rate of occurrence.
- **Impact Analysis:** The final step in the C-SCRM process is impact analysis, which evaluates the potential consequences of a threat exploiting a vulnerability. This includes assessing the potential damage to organizational operations, assets, and individuals. Examples of impacts include loss of user and public trust, loss of classified information, production delays, and loss of intellectual property.

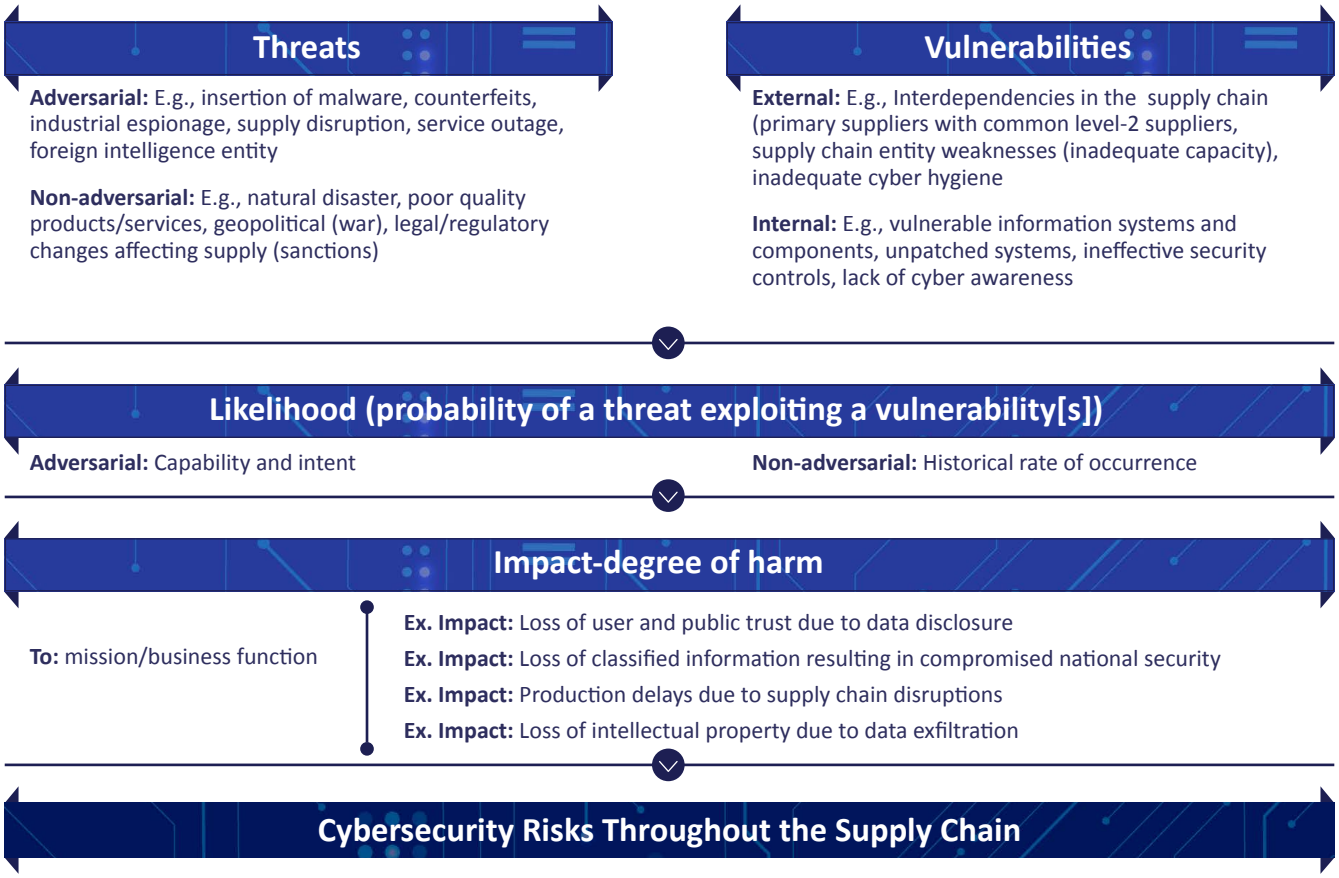


Figure 6: Cybersecurity Risks in the Supply Chain

C-SCRM Applies to All Levels of the Organization

C-SCRM plays a crucial role in protecting organizations by addressing risks introduced through external suppliers, vendors, etc. across three levels of the organization: the enterprise level, the mission/business level, and the operational level.

At each level, C-SCRM aligns its strategy, policies, and implementation plans to establish an enterprise-wide strategy that aligns security measures with key missions and business processes and embeds tactical actions into daily operational activities, as depicted in Figure 7. This top-down approach makes sure that the enterprise strategy is translated into specific goals and plans for individual units, which in turn are translated into actionable tasks and day-today operations within departments. This hierarchical structure ensures alignment and effective implementation of CSCRM practices across all levels of the organization, with a shared responsibility at each level.

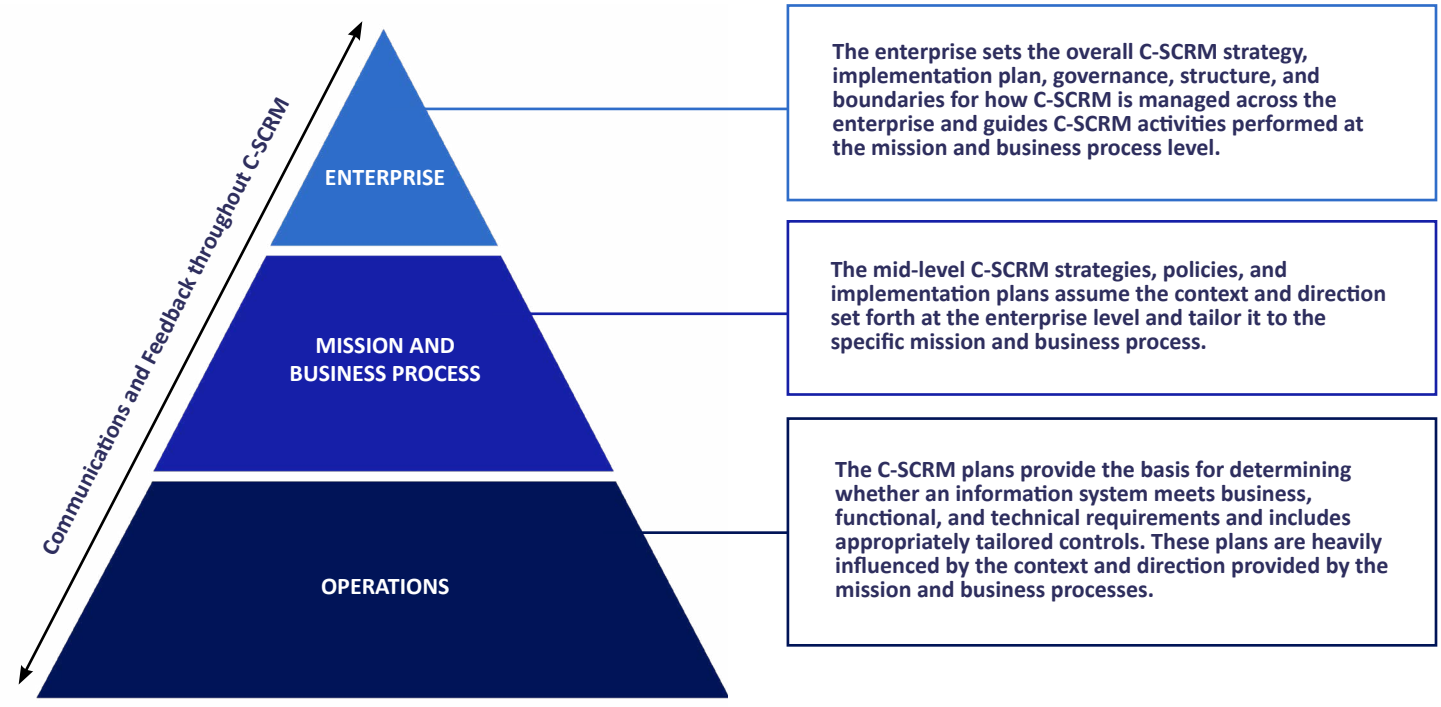


Figure 7: Tiered C-SCRM Approach

Layer Three: CREF Strategy

The Cyber Resilience Engineering Framework (CREF) *is a structured approach that strengthens an organization's ability to maintain essential functions and adapt during cyber disruptions. It combines elements of cybersecurity, business continuity, and systems engineering to build robust systems that can handle unexpected challenges.*

The CREF focuses on:

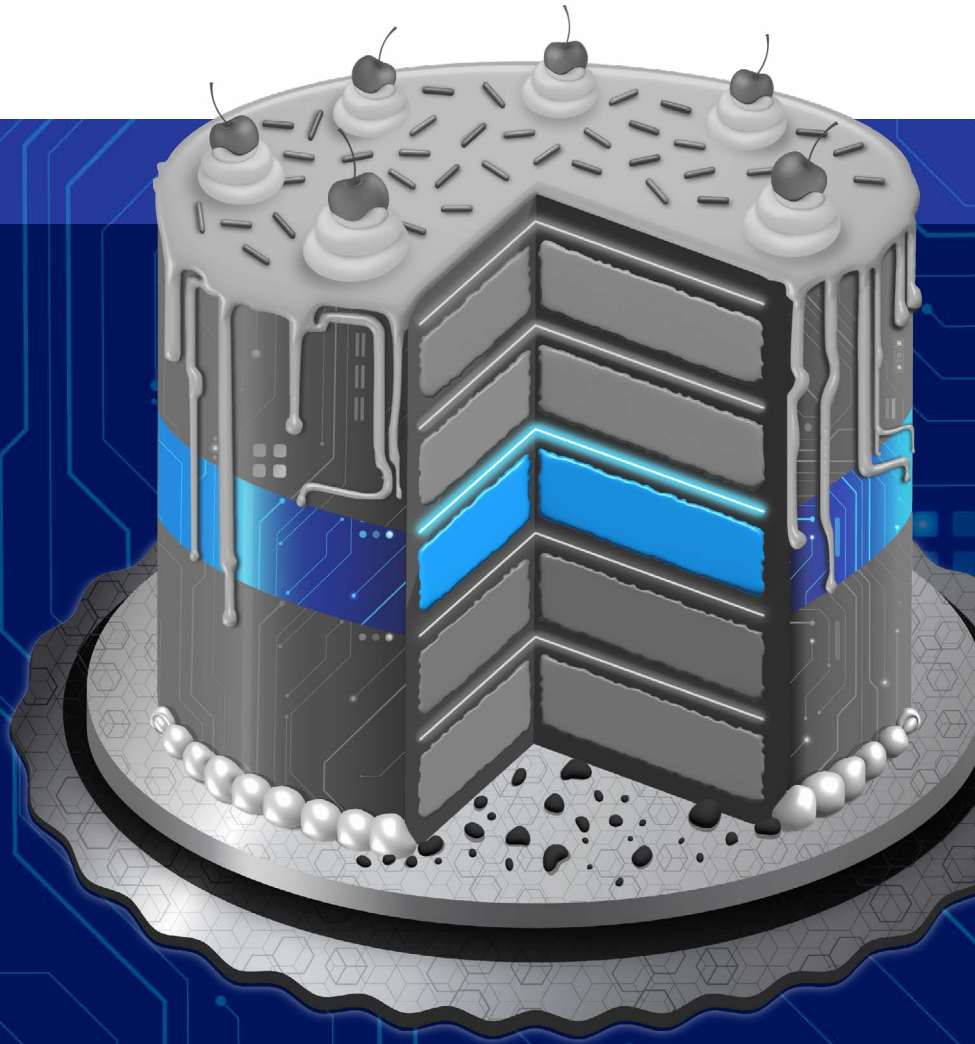
- Continuing operations even when an adversary has established a foothold in the organization's systems and cyber infrastructure, minimizing downtime and economic loss threats.
- Becoming more robust over time against emerging threats.

The CREF Process

The CREF process starts by defining strategies at the organizational, mission/business process, and operational/system levels to manage risks effectively, which helps interpret and determine priorities for achieving resilience goals.

Core CREF Cookbooks

1. **NIST Special Publication 800-160 Volume 1 Revision 1, Engineering Trustworthy Secure Systems,** ***https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v1r1.pdf***
2. **NIST Special Publication 800-160, Volume 2 Revision 1, Developing Cyber-Resilient Systems: A Systems Security Engineering Approach,** ***https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2r1.pdf***



- **CREF goals** guide the overall resilience strategy at each level to assure systems are better prepared to handle adverse conditions and maintain operational integrity.
- **Cyber resiliency objectives** are specific statements of what capabilities a system is intended to achieve in its operational environment (e.g., the measures to prevent or avoid cyber threat, the readiness to respond and manage the threat, maintain essential functions, etc.). The objectives facilitate prioritization and assessment, and enable development of questions such as:
  - To what degree can each cyber resiliency objective be achieved?
  - How quickly and cost-effectively can each cyber resiliency objective be achieved?
  - With what degree of confidence or trust can each cyber resiliency objective be achieved?
- **Cyber resiliency techniques** are a set of practical methods and tools used to implement the selected approaches to maintain resilience. The cyber resiliency techniques reflect an understanding of the threats as well as the technologies, processes, and concepts related to improving cyber resiliency to address the threats to maintain its goal and objective.
- **Strategic Design Principles** guide design decisions and describe how the concept applies to system design, which includes operational processes and procedures and may also include development and maintenance environments.

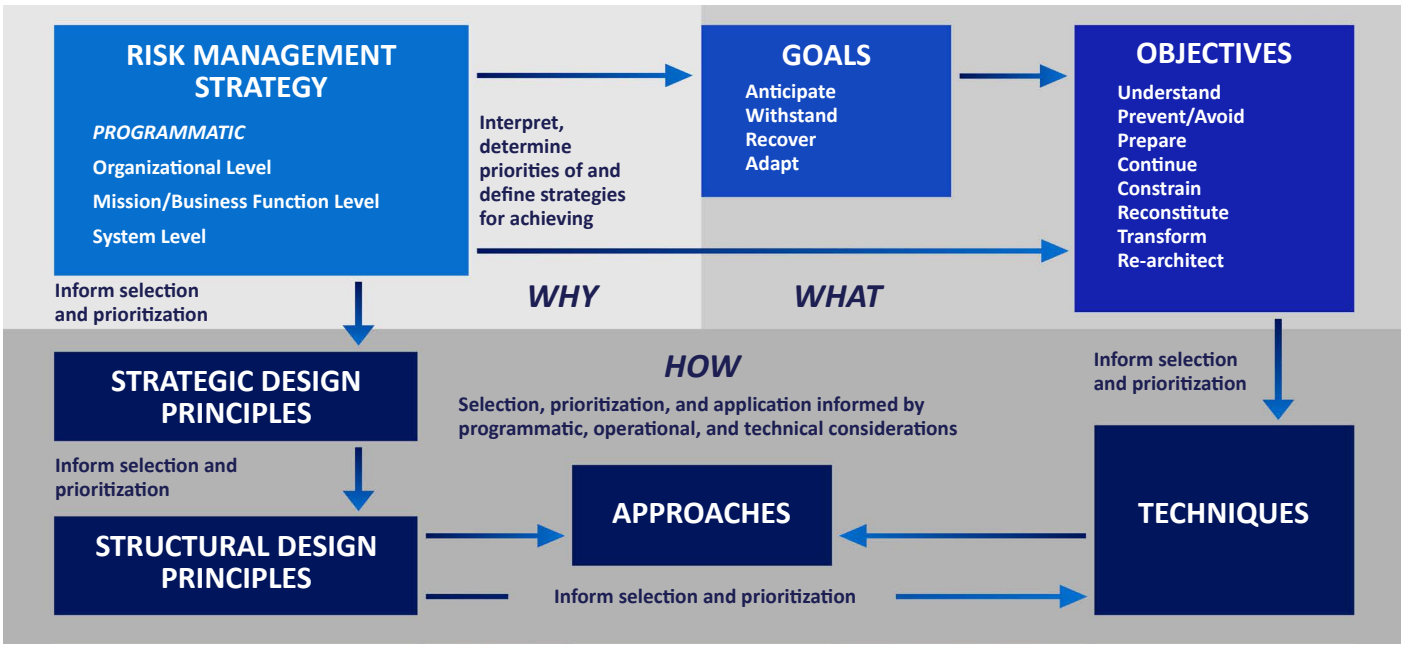


Figure 8: The Cyber Resilience Engineering Framework Process

Interim Summary

Completed Layers:

- Federal Information Processing Standards (FIPS)
- Risk Management Framework (RMF)
- Supply Chain Risk Management (SCRM)
- Cyber Supply Chain Risk Management (C-SCRM)
- Cyber Resilience Engineering Framework (CREF)

Summary

1. **Establish Baseline Security with Federal Information Processing Standards (FIPS)**
   - Begin with FIPS to set mandatory security standards for federal information systems.
   - Ensure a consistent baseline of security to support broader cybersecurity strategies.
2. **Setup the Platter: Integrate the Risk Management Framework (RMF)**
   - Incorporate cybersecurity and risk management into the system development life cycle.
   - Follow each step of the RMF Process to ensure all your cybersecurity basics are covered.
3. **Manage Supply Chain Risks**
   - Add Supply Chain Risk Management (SCRM) to address a broad range of risks, including physical, financial, and operational.
   - Provide resilience into your operations starting before a system is built.
4. **Layer on Cybersecurity Supply Chain Risk Management (C-SCRM)**
   - Ensure that vulnerabilities within the supply chain are identified, assessed, and mitigated, complementing RMF's detailed controls.
   - Enhance awareness of risks throughout an IT System's lifecycle and throughout its cyberspace components.
5. **Integrate the Cyber Resilience Engineering Framework (CREF)**
   - Ensure that critical operations can continue during cyber incidents.
   - Emphasize resilience in cybersecurity strategies, enhancing overall security, cyber survivability, and organizational resilience.

How the RMF, SCRM, C-SCRM and CREF layers fit together

RMF and SCRM serve as the baseline frameworks, providing the essential structure for the risk management and supply chain risk management practices that C-SCRM and CREF expand upon to address cybersecurity and resilience comprehensively.

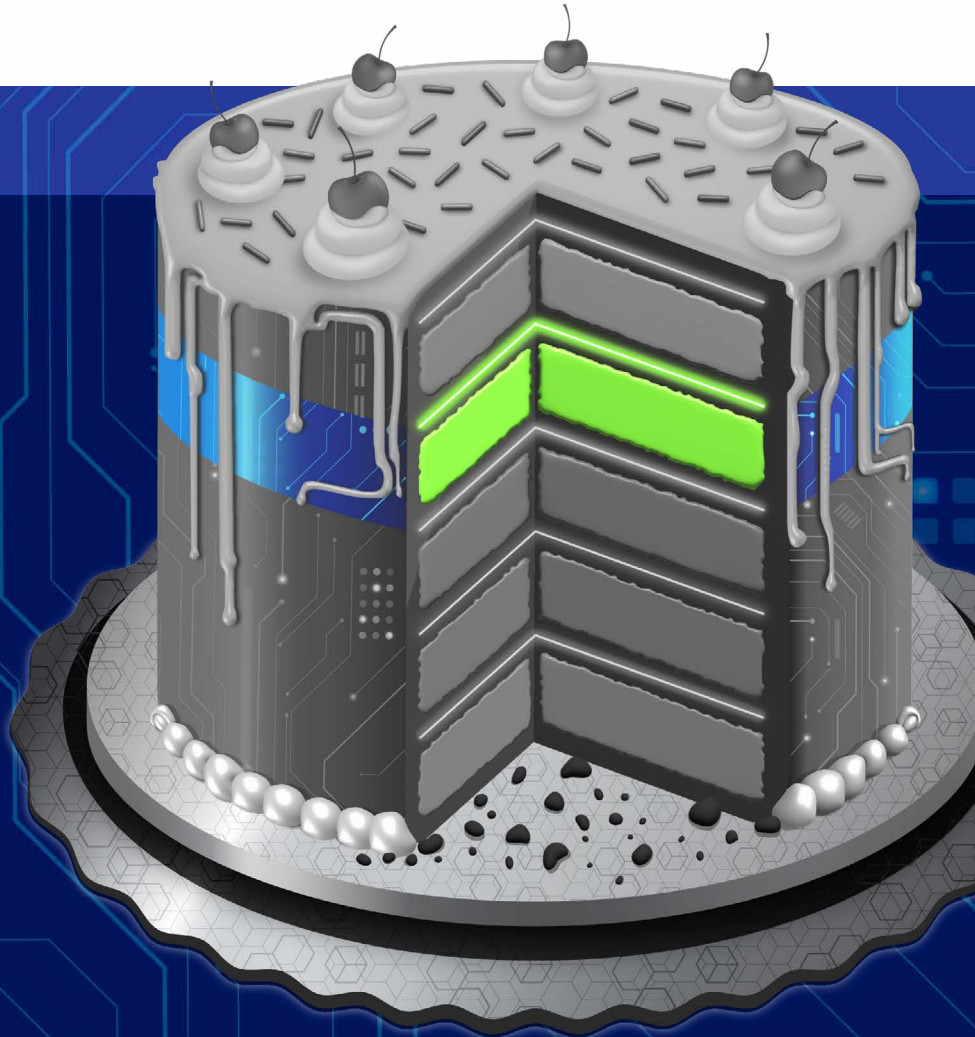
- C-SCRM is the ingredient that builds upon RMF and SCRM by specifically focusing on the cybersecurity aspects, ensuring that risks associated with the supply chain's cyber components are effectively managed.
- CREF integrates principles from RMF and SCRM to enhance an organization's ability to withstand and recover from cyber incidents, emphasizing resilience in both operational and supply chain contexts.

Layer Four: Zero Trust Strategy

Zero Trust (ZT) *is designed to enable access enhancing the operational experience of Airmen and Guardians. Facilitating direct access to protected resources simplifies digital access without sacrificing security, enabling warfighters with greater freedom of maneuver. The ZT architecture provides a digital advantage over cyber threats, enhancing the cybersecurity posture of the DAF, and better enabling Airmen and Guardians to execute their missions securely.*

Core Zero Trust Cookbooks

1. **NIST Special Publication 800-207, Zero Trust Architecture,** ***https://www.nist.gov/publications/zero-trust-architecture***
2. **DoD Zero Trust Strategy,** ***https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-ZTStrategy.pdf***
3. **DAF Zero Trust Strategy v1.0,** ***https://www.safcn.af.mil/Portals/64/Documents/Strategy/DAF%20Zero%20Trust%20Strategy%20v1.0%20(002).pdf***



Zero Trust Tenets

- **Assume a Hostile Environment:** There are malicious personas both inside and outside the environment. All users, devices, applications, environments, and all other NPEs are treated as untrusted.
- **Presume Breach:** There are hundreds of thousands of attempted cybersecurity attacks against DoD environments every day. Consciously operate and defend resources with the assumption that an adversary has presence within your environment. Enhanced scrutiny of access and authorization decisions to improve response outcomes.
- **Never Trust, Always Verify:** Deny access by default. Every device, user, application/workload, and data flow are authenticated and explicitly authorized using least privilege, multiple attributes, and dynamic cybersecurity policies.
- **Scrutinize Explicitly:** All resources are consistently accessed in a secure manner using multiple attributes (dynamic and static) to derive confidence levels for contextual access to resources. Access to resources is conditional and access can dynamically change based on action and confidence levels resulting from those actions.
- **Apply Unified Analytics:** Apply unified analytics for Data, Applications, Assets, Services (DAAS) to include behavioristics, and log each transaction.

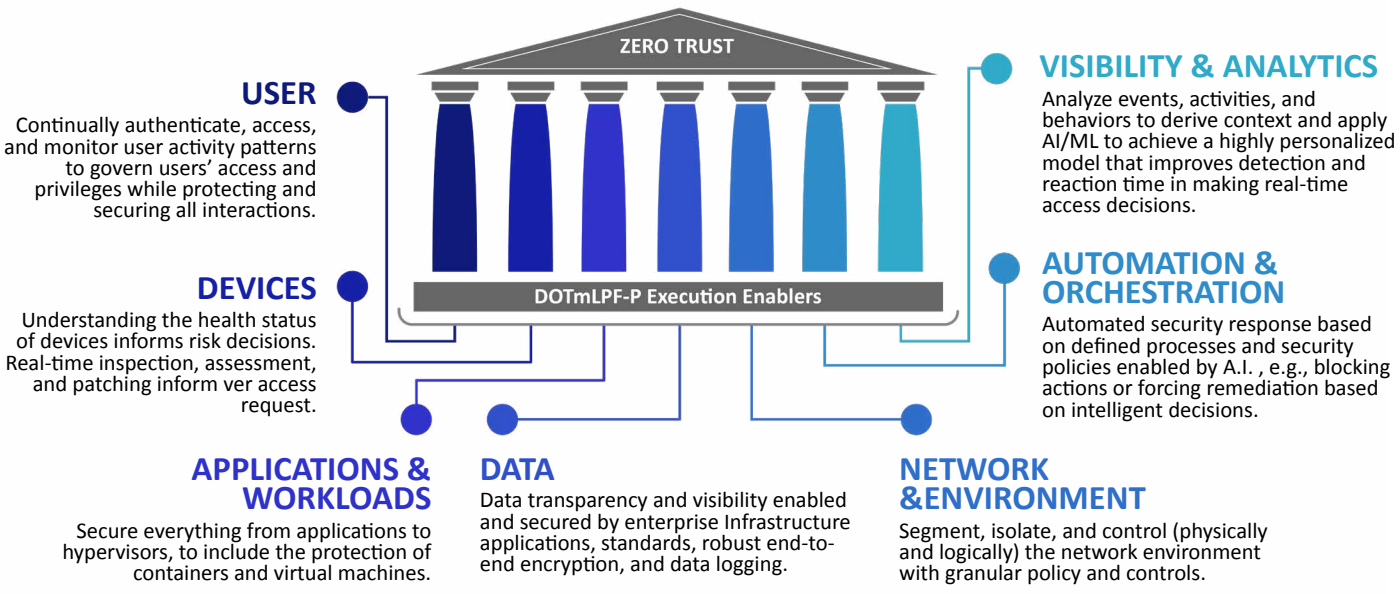


Figure 9: DoD Zero Trust Pillars

Zero Trust Pillars

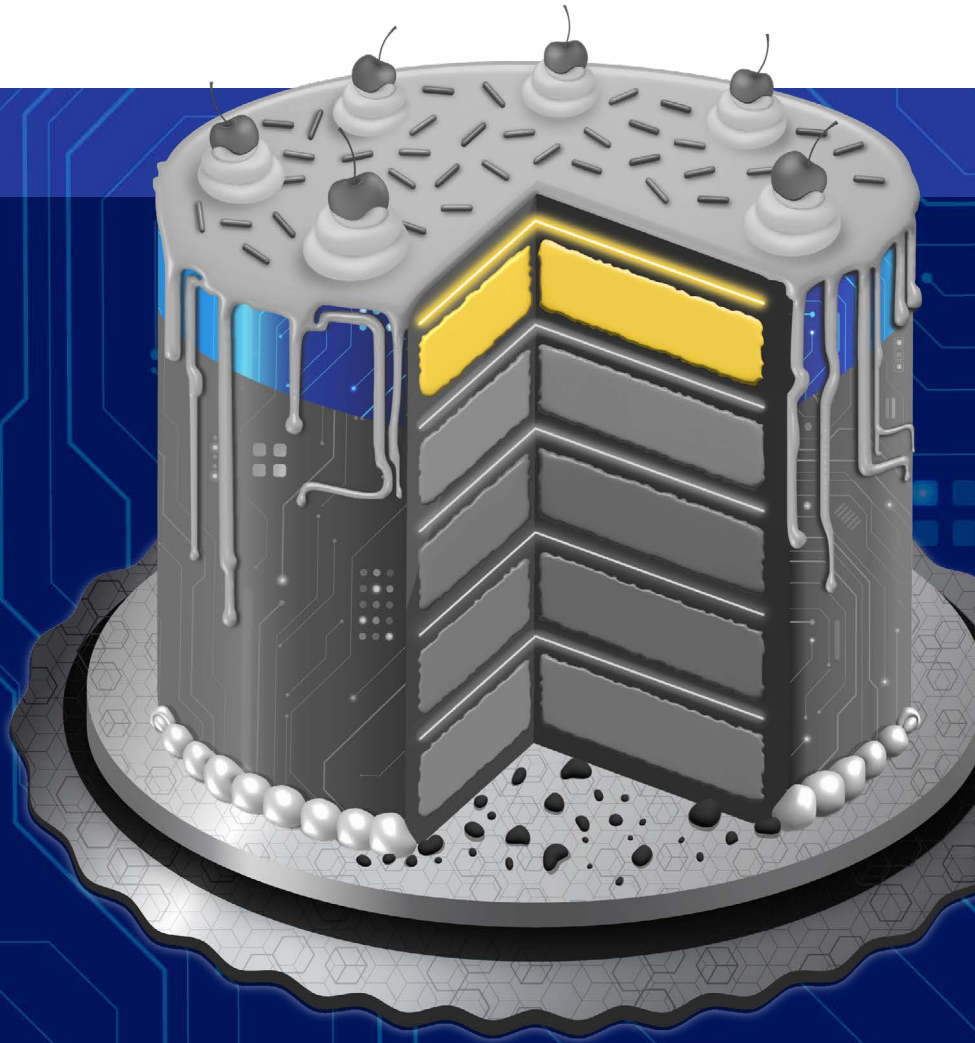
Zero Trust capabilities across the information environment must be developed, deployed, and operated within an organizing construct defined by seven DoD Zero Trust Pillars and their enablers to ensure standardization of execution. These pillars, as depicted in Figure 9, provide the foundational areas for the DoD's Zero Trust efforts. The execution enablers are cross-cutting, non-technical capabilities and activities that address culture, governance, and elements of DOTmLPF-P. This ZT model represents a state change in how the DoD implements access to resources, creating a dynamic system in which all pillars are considered to effectively enable data-centric security.

Layer Five:
MITRE ATT&CK® Framework

The MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK®) framework *is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations. ATT&CK provides details on 100+ threat actor groups, including the techniques and software they are known to use.*

Core MITRE ATT&CK Cookbooks

1. **MITRE ATT&CK,** ***https://attack.mitre.org/***
2. **MITRE ATT&CK Get Started Page,** ***https://attack.mitre.org/resources/***



Layer Five: MITRE ATT&CK® Framework

The MITRE ATT&CK framework is a comprehensive knowledge base of cyber attack tactics, techniques, and procedures (TTPs that provides a detailed understanding of the lifecycle of a cyber attack. Developed by the MITRE Corporation, a non-profit organization that operates multiple federally funded research and development centers, ATT&CK is a widely adopted framework that helps cybersecurity professionals understand the various stages of a cyber attack, from initial reconnaissance to data exfiltration, as depicted in Figure 10. By mapping the tactics and techniques used by attackers, ATT&CK enables defenders to better anticipate, detect, and respond to cyber threats. The framework is divided into 14 tactics, including Reconnaissance, Resource Development, and Impact, which are further broken down into techniques and sub-techniques, providing a granular understanding of the attack lifecycle. The following graphic illustrates the MITRE ATT&CK framework in detail, providing a visual representation of the tactics and techniques used by attackers and helping cybersecurity professionals to develop effective defense strategies

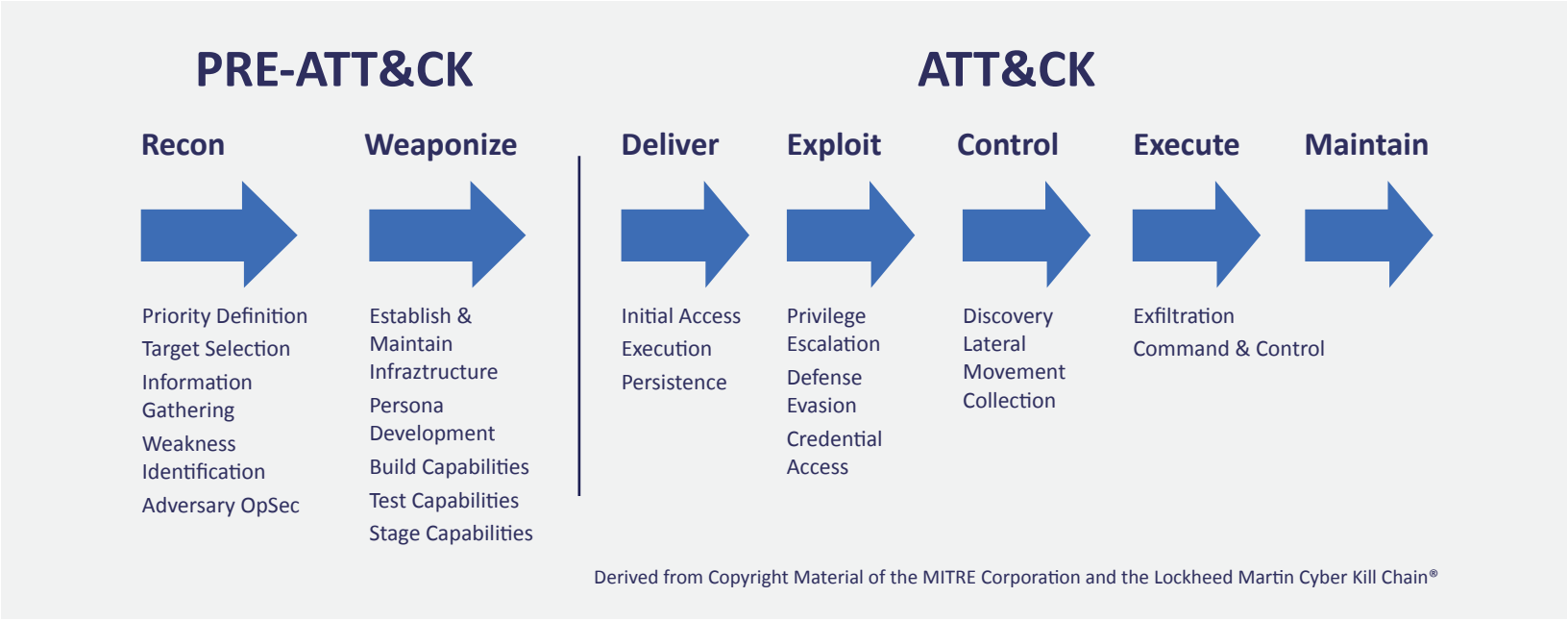


Figure 10: MITRE ATT&CK Lifecycle

Additionally, SOAR (Security Orchestration, Automation, and Response) is a cybersecurity technology that complements MITRE ATT&CK to improve threat detection and response. SOAR tools automate repetitive tasks and integrate various security tools and processes.

***ATT&CK* describes behaviors across the adversary lifecycle, commonly known as tactics, techniques, and procedures (TTPs). In ATT&CK, these behaviors correspond to four increasingly granular levels:**

Tactics

Tactics represent the "what" and "why" of an ATT&CK technique or sub-technique. They are the adversary's technical goals, the reason for performing an action, and what they are trying to achieve. For example, an adversary may want to achieve credential access in order to gain access to a target network. Each tactic contains an array of techniques that network defenders have observed being used in the wild by threat actors. Note: The ATT&CK framework is not intended to be interpreted as linear—with the adversary moving through the tactics in a straight line (i.e., left to right) in order to accomplish their goal. Additionally, an adversary does not need to use all of the ATT&CK tactics in order to achieve their operational goals.

Techniques

Techniques represent "how" an adversary achieves a tactical goal by performing an action. For example, an adversary may dump credentials to achieve credential access. Techniques may also represent what an adversary gains by performing an action. A technique is a specific behavior to achieve a goal and is often a single step in a string of activities intended to complete the adversary's overall mission. ***Note:*** many of the techniques within ATT&CK include legitimate system functions that can be used for malicious purposes (referred to as "living off the land").

Sub-techniques

Sub-Techniques provide more granular descriptions of techniques. For example, there are behaviors under the OS Credential Dumping [T1003] technique that describe specific methods to perform the technique, such as accessing LSASS Memory [T1003.001], Security Account Manager [T1003.002], or /etc/passwd and /etc/shadow [TT1003.008]. Sub-techniques are often, but not always, operating system or platform specific. Not all techniques have sub-techniques.

Procedures

Procedures are particular instances of how a technique or sub-technique has been used. They can be useful for replication of an incident with adversary emulation and for specifics on how to detect that instance in use.

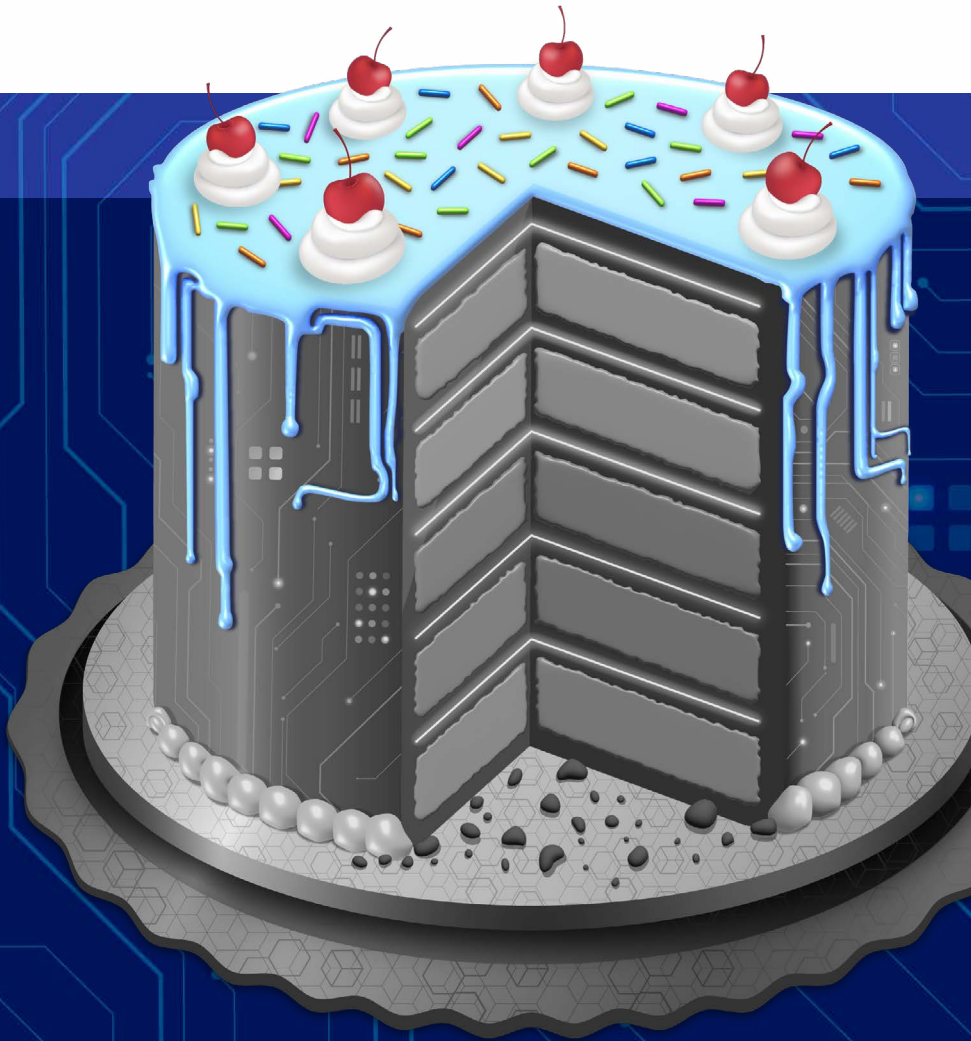
Applying MITRE ATT&CK

- **ATT&CK can be used to identify defensive gaps, assess security tool capabilities, organize detections, hunt for threats, engage in red team activities, or validate mitigation controls.**
- **The DAF uses ATT&CK as a lens to identify and analyze adversary behavior to proactively defend our assets.**
- **ATT&CK mappings can be used in design and engineering phases of the systems development lifecycle to proactively search for methods to build resilience into mission systems to prevent future attacks.**

Finally, MITRE Engage® is a framework designed to help organizations plan and implement adversary engagement strategies, including deception, denial, and adversary interaction. It provides a structured way to anticipate, detect, and counter cyber threats by actively shaping adversary behavior rather than just responding to threats. Engage is useful for threat intelligence teams, red teams, and cyber defenders looking to shift from passive defense to a more proactive and strategic cybersecurity posture.

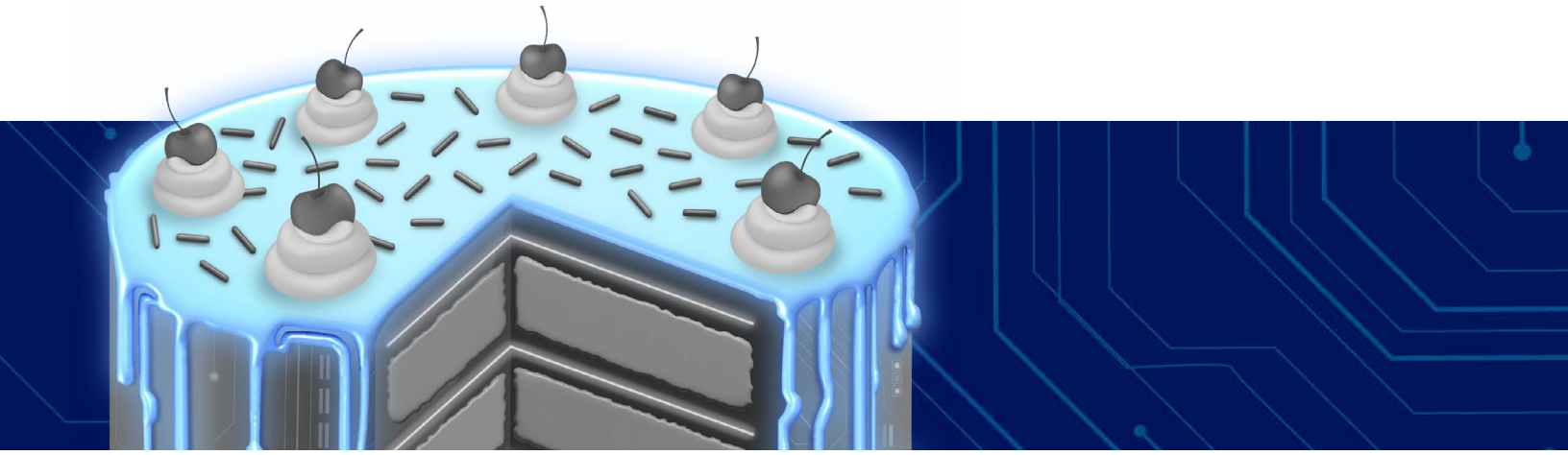
Toppings:
Privacy, SSDF, CUI, and AI Strategies

A cake is finished with the addition of frosting, sprinkles, candles, and other toppings. Critical cybersecurity concepts like ***Privacy, The NIST Secure Software Development Framework (SSDF), Controlled Unclassified Information (CUI), and Artificial Intelligence (AI)*** *represent these finishing items for a cyber cake.*



Various Cookbooks

1. NIST Privacy Framework, *https://www.nist.gov/privacy-framework/privacy-framework*
2. NIST Secure Software Development Framework (SSDF), *https://csrc.nist.gov/projects/ssdf*
3. The DoD CUI Program, *https://www.dodcui.mil/*
4. The NIST AI RMF Home Page, *https://www.nist.gov/itl/ai-risk-management-framework*
5. NIST AI 100-1, The Artificial Intelligence (AI) Risk Management Framework, *https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf*
6. DoD Data, Analytics, and Artificial Intelligence Adoption Strategy, *https://media.defense.gov/2023/Nov/02/2003333300/-1/-1/1/DOD_DATA_ANALYTICS_AI_ADOPTION_STRATEGY.pdf*



Privacy

Figure 11 shows how security and privacy are closely related, and how a breach of security can often lead to a breach of privacy. Understanding the NIST Privacy Framework can help cybersecurity practitioners identify and mitigate potential privacy risks. The Privacy Framework is a risk and outcome based approach that is flexible enough to address diverse privacy needs, enable more innovative and effective solutions that can lead to better outcomes for individuals and organizations, and stay current with technology trends, such as artificial intelligence and the Internet of Things.

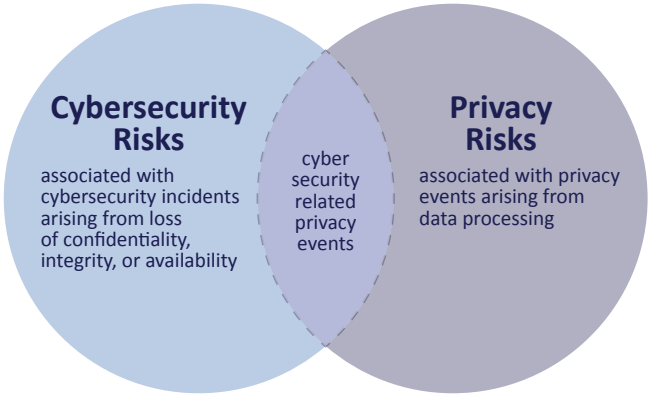
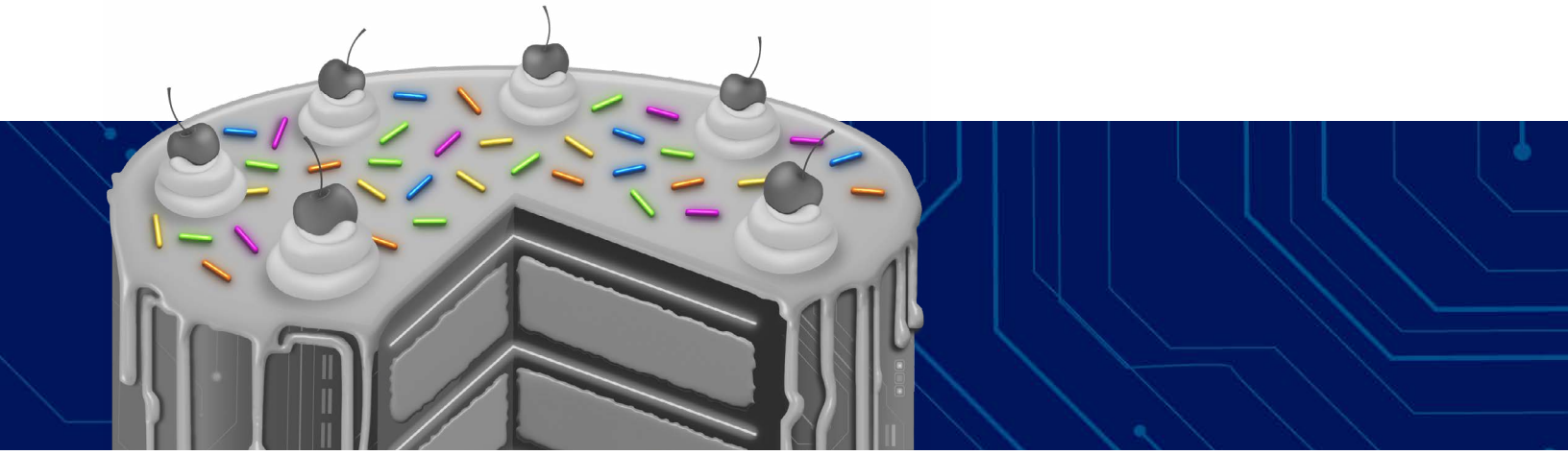


Figure 11: Cybersecurity and Privacy Risk Relationship

The NIST Privacy Framework can support organizations in:

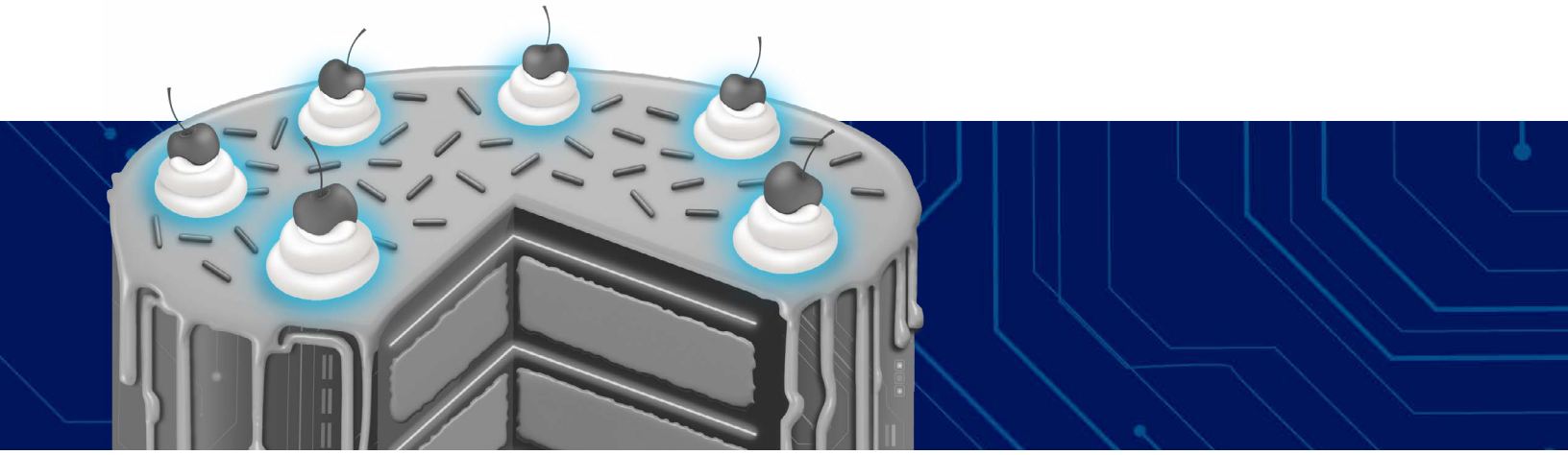
1. **Building user trust:** By supporting ethical decision-making in product and service design or deployment, organizations can optimize the beneficial uses of data while minimizing adverse consequences for individuals' privacy and society as a whole. This helps to establish trust with users, which is essential for maintaining a positive reputation and ensuring long-term success.
2. **Fulfilling compliance obligations:** The NIST Privacy Framework can help organizations fulfill their current compliance obligations, as well as future-proof their products and services to meet these obligations in a changing technological and strategic environment. This enables organizations to stay ahead of emerging regulations and standards, reducing the risk of non-compliance and associated penalties.
3. **Facilitating communication:** Facilitating communication among stakeholders, including users, employees, and regulators, about how data is collected, used, shared, and protected. This includes providing transparency into data practices, informing individuals about their privacy rights and choices, and enabling organizations to respond to privacy-related inquiries and concerns in a timely and effective manner. By facilitating open and clear communication, organizations can build trust, address privacy concerns, and demonstrate their commitment to protecting personal data.



Secure Software Development Framework (SSDF)

The NIST Secure Software Development Framework (SSDF) is a comprehensive guide that outlines the fundamental, sound, and secure practices for developing software. These practices are based on established secure software development practice documents and are designed to help organizations integrate security into every stage of the software development lifecycle. By following the SSDF, organizations can benefit from improved cybersecurity posture, which is achieved by integrating security into every stage of the software development lifecycle, thereby reducing the risk of security breaches and vulnerabilities. Additionally, the SSDF helps organizations reduce risk by identifying and mitigating potential security risks, which in turn reduces the likelihood of security incidents and data breaches. Furthermore, by demonstrating a commitment to secure software development, organizations can increase trust with their users, partners, and stakeholders. Ultimately, the SSDF can also help organizations achieve compliance with relevant security standards and regulations, reducing the risk of non-compliance and associated penalties. The practices are organized into four groups:

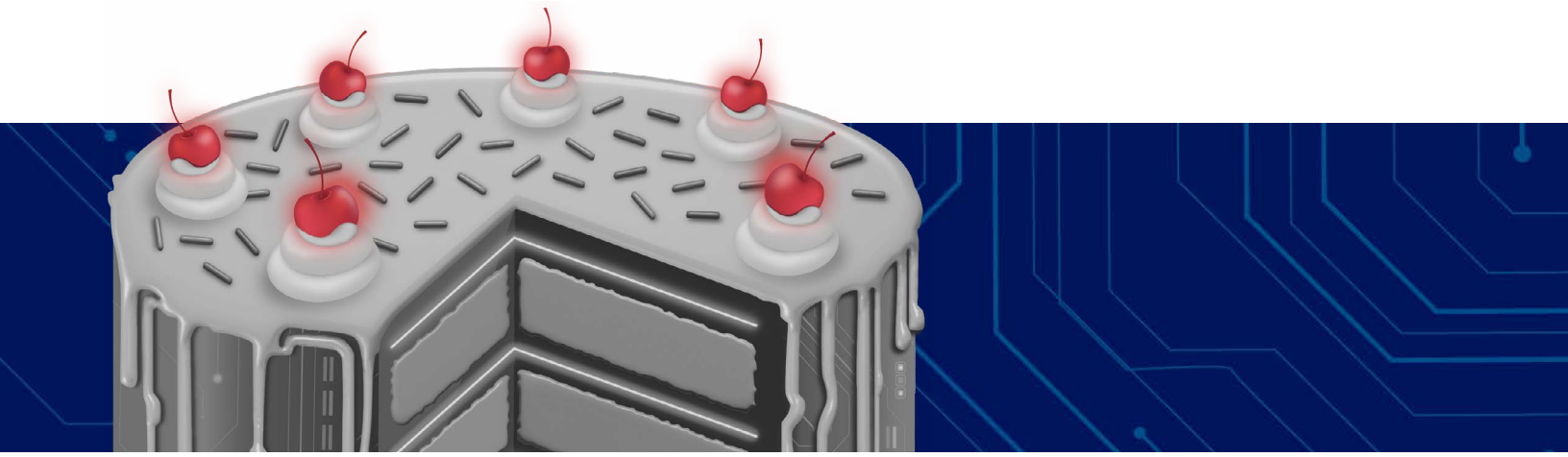
1. **Prepare the Organization (PO):** Organizations should ensure that their people, processes, and technology are prepared to perform secure software development at the organization level. Many organizations will find some PO practices to also be applicable to subsets of their software development, like individual development groups or projects.
2. **Protect the Software (PS):** Organizations should protect all components of their software from tampering and unauthorized access.
3. **Produce Well-Secured Software (PW):** Organizations should produce well-secured software with minimal security vulnerabilities in its releases.
4. **Respond to Vulnerabilities (RV):** Organizations should identify residual vulnerabilities in their software releases and respond appropriately to address those vulnerabilities and prevent similar ones from occurring in the future.



Controlled Unclassified Information (CUI)

CUI is a US government designation for sensitive information that is not classified, but still requires protection. CUI can be a high-value target for attackers, and a breach could have significant consequences, including financial loss, reputational damage, and legal liability. Government agencies, contractors, or organizations that handle CUI must comply with the CUI regulation (32 CFR Part 2002) and the National Institute of Standards and Technology (NIST) Special Publication 800-171, which provides guidelines for protecting CUI. CUI includes a wide range of sensitive information, such as financial, personal, or proprietary data, that could be damaging if compromised. Cybersecurity practitioners must ensure that CUI is handled, stored, and transmitted securely to prevent unauthorized access, theft, or exploitation.

- The DoD CUI Program standardizes the safeguarding of information across multiple categories. For example, CUI categories exist to protect Privacy Act information, attorney-client privileged information, and controlled technical information, among other. A complete list is available at the DoD CUI Registry (https://www.dodcui.mil).
- CUI markings alert recipients that special handling may be required to comply with law, regulation, or Government-wide policy.
- For DoD, CUI also enables consistent processes to safeguard information for specific national security purposes, such as physical and operations security.



Artificial Intelligence and Machine Learning (AI/ML)

The increasing use of Artificial Intelligence (AI) and Machine Learning (ML) in various aspects of life has also led to their adoption by malicious actors, posing significant threats to cybersecurity. As a cybersecurity practitioner, it is essential to be aware of the potential risks associated with AI and ML-powered attacks.

One of the primary concerns is the use of AI-powered phishing attacks, which can mimic the tone and language of high-level executives or other legitimate individuals, making them difficult to distinguish from genuine communications. Additionally, ML algorithms can be employed to analyze network traffic and identify vulnerabilities, allowing attackers to launch targeted and effective exploits.

Furthermore, AI-powered malware has become a significant threat, as it can adapt and evolve to evade detection by traditional security systems. Once inside a network, this type of adaptive malware can spread rapidly and quietly, causing damage before detection. The widespread adoption of AI technologies has enhanced adaptive malware to become increasingly sophisticated, difficult to detect, and propagates more quickly.

In order to address these threats, it is essential to consider the role of AI and ML in cybersecurity risk management. The NIST Artificial Intelligence Risk Management Framework (AI RMF) provides a structured approach to managing AI-related risks, including those related to cybersecurity (see Figure 12).

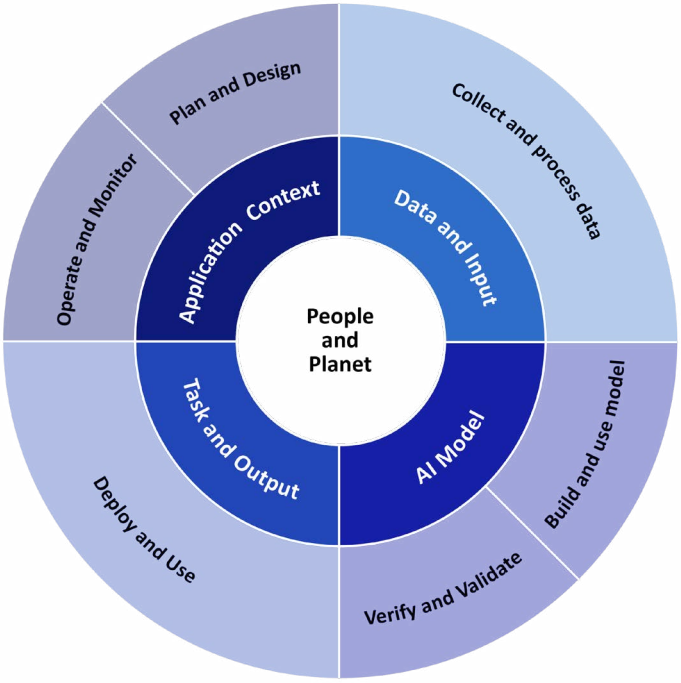


Figure 12: AI System Lifecycle

As seen in Figure 13, the AI RMF emphasizes the importance of understanding the potential risks and benefits of AI and ML, as well as identifying and mitigating potential vulnerabilities.

In the context of cybersecurity, the AI RMF highlights the need for organizations to consider the potential risks associated with AI and ML-powered threats, including the use of AI-powered phishing attacks, ML-powered malware, and other types of attacks. The framework also emphasizes the importance of implementing AI and ML-based security solutions, such as predictive analytics and anomaly detection, to improve the detection and response to cyber threats.

By prioritizing the development of AI and ML-based security solutions and incorporating them into organizational cybersecurity risk management strategies, organizations can improve defenses and stay ahead of the evolving cyber threat landscape. While the AI RMF is a voluntary documentation strategy to identify potential AI-related risks, actively implementing robust cybersecurity controls to address those risks can involve significant changes to existing systems, processes, and staff training.

Overall, the consideration of AI and ML-powered threats is a critical component of effective cybersecurity risk management, and organizations must prioritize the development of AI and ML-based security solutions to stay ahead of the evolving cyber threat landscape.

Figure 13: Risks of AI

Taking a Slice: Cybersecurity Framework 2.0

*The **NIST Cybersecurity Framework (CSF) 2.0** is used to assess the components of the cyber cake to ensure the outcome of the baking process is how the cake intended to look, smell, and taste. The CSF 2.0 is a vital tool for cybersecurity practitioners, providing a comprehensive and holistic approach to managing cybersecurity risk. As a widely adopted and widely respected framework, the CSF 2.0 offers a structured approach to identifying, protecting, detecting, responding to, and recovering from cyber threats.*

Core Cybersecurity Framework 2.0 Cookbooks

1. NIST Cybersecurity Framework (CSF) 2.0, *https://www.nist.gov/cyberframework*
2. DoDI 8500.01, Cybersecurity, *https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodi/850001_2014.pdf*
3. DAFI 17-130, Cybersecurity Program Management, *https://static.e-publishing.af.mil/production/1/saf_cn/publication/afi17-130/afi17-130.pdf*

One of the key strengths of the NIST CSF 2.0 is its ability to provide a holistic view of an organization's cybersecurity posture, considering the complex and interconnected nature of modern cybersecurity threats. By providing a framework that integrates multiple disciplines and domains, the NIST CSF 2.0 enables cybersecurity practitioners to consider the broader context of cybersecurity risk management, including the role of AI and ML in cybersecurity.

The NIST CSF 2.0 is also important because it provides a common language and set of concepts that can be used to communicate cybersecurity risk and mitigation strategies to stakeholders across the organization. This includes executives, IT personnel, and other stakeholders who may not have a deep understanding of cybersecurity technical details.

Furthermore, the NIST CSF 2.0 is designed to be flexible and adaptable, allowing organizations to tailor their cybersecurity risk management strategies to their specific needs and circumstances. This includes integrating the NIST CSF 2.0 with other frameworks and standards, such as the NIST AI Risk Management Framework, ISO 27001, and COBIT, to provide a comprehensive and integrated approach to cybersecurity risk management.

By using the NIST CSF 2.0, cybersecurity practitioners can ensure that their organization's cybersecurity risk management strategy is sound and accounts for the latest threats and vulnerabilities. The framework also provides a set of guidelines and recommendations for implementing cybersecurity controls and risk management strategies, including those related to privacy and AI/ML.

In addition, the NIST CSF 2.0 provides a framework for continuous improvement and maturity, allowing organizations to assess their current cybersecurity posture and identify areas for improvement. This includes identifying gaps in their cybersecurity controls and risk management strategies and prioritizing remediation efforts based on risk and business impact.

Overall, the NIST CSF 2.0 is an essential tool for cybersecurity practitioners, providing a comprehensive and holistic approach to managing cybersecurity risk.

Assessing the Cake Slice with CSF 2.0

The NIST CSF 2.0 provides a structured approach to managing cybersecurity risks, much like following a recipe ensures a well baked cake. By understanding and implementing the six core functions—Govern, Identify, Protect, Detect, Respond, and Recover (see Figure 14)—organizations can better prepare for, manage, and recover from cybersecurity incidents. Assessing a cyber cake according to the CSF 2.0 provides a systematic way to evaluate it according to a standardized rubric, which, if properly applied, allows for evaluating a slice of the cyber cake against cybersecurity standards.

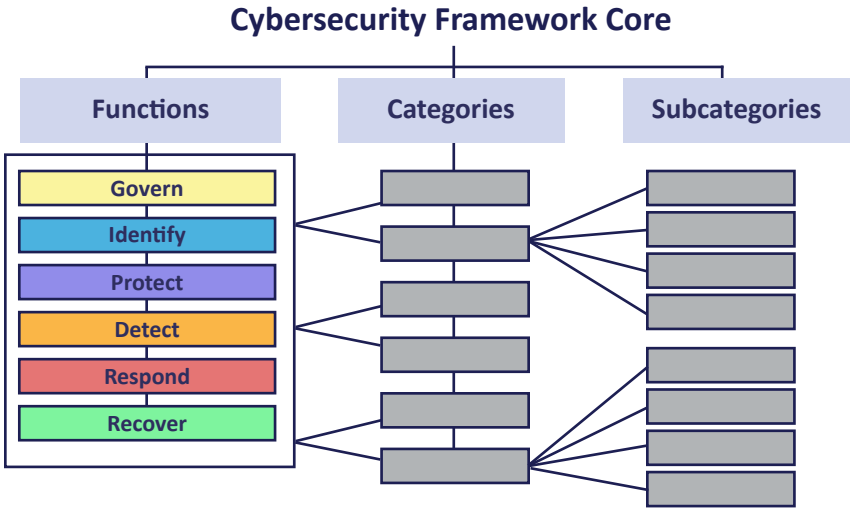


Figure 14: Cyber Security Framework 2.0 Core

The Basic Ingredient Types - Core Functions

The six core functions of the NIST CSF 2.0: Govern, Identify, Protect, Detect, Respond, and Recover represent the core cybersecurity functions and common concepts against which a cyber cake needs to be assessed. These functions are fundamental to any cybersecurity program and provide a high-level, strategic view of an organization's cybersecurity posture.

- **Govern (GV):** The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored.
- **Identify (ID):** The organization's current cybersecurity risks are understood.
- **Protect (PR):** Safeguards to manage the organization's cybersecurity risks are used.
- **Detect (DE):** Possible cybersecurity attacks and compromises are found and analyzed.
- **Respond (RS):** Actions regarding a detected cybersecurity incident are taken.
- **Recover (RC):** Assets and operations affected by a cybersecurity incident are restored.

Evaluating the Fundamentals - Categories and Subcategories

The layers of a cyber cake are assessed against the categories and subcategories within each core function. These items provide more detailed and specific aspects of cybersecurity that need to be addressed.

- **Categories:** These are subdivisions of a function into groups of cybersecurity outcomes closely tied to programmatic needs and particular activities. For example, within the Identify function, categories include Asset Management, Risk Assessment, and Improvement.
- **Subcategories:** These further divide categories into specific outcomes of technical and management activities. For instance, under the Asset Management category, there are subcategories for hardware, software, services, asset prioritization, and more.

In this fashion, the cyber cake can be addressed both at a granular level for correctness within each layer and as an entire slice to determine whether the cake came out properly according to the recipe's intent.

Evaluating the Bakery - Implementation Tiers

The implementation tiers represent how well the organization bakes its cyber cake —are they a professional baker competing on the global stage, an amateur baking a boxed cake for a birthday, or somewhere in between? Tiers characterize the rigor of an organization's cybersecurity risk governance and management practices, and they provide context for how an organization views cybersecurity risks and the processes in place to manage those risks (see Figure 15). Tiers should complement an organization's cybersecurity risk management methodology rather than replace it. For example, an organization can use the Tiers to communicate internally as a benchmark for an organization-wide approach to managing cybersecurity risks.

CSF Implementation Tiers

Tier 1	Tier 2	Tier 3	Tier 4
Partial Implementation	**Risk Informed**	**Repeatable**	**Adaptive**
Organization has an ad-hoc and reactive cybersecurity posture. Organization has little awareness of organizational risk, and any plans implemented are often done inconsistently.	Organization may be approving cybersecurity measures, but implementation is piecemeal. Organization is aware of risks, has plans, and has proper resources to protect themselves but haven't quite reached a proactive state.	Organization has implemented cybersecurity standards and are able to respond to crises. Strategies are consistently applied, and members are informed of risks.	Organization has total adoption of standards. The organization is not just prepared to respond to threats but can proactively detect threats and predict issues based on current trends and the organization's architecture.

Figure 15: CSF Implementation Tiers

Assessing the Bakery - Organizational Profiles

Organizational Profiles represent the goals of the baker producing their cyber cake, which align the organization's cybersecurity activities with its business requirements, risk tolerance, and resources. Profiles help organizations to prioritize and achieve their desired cybersecurity outcomes.

- **Current Profile:** Represents the state of the organization's cybersecurity program at the time of assessment.
- **Target Profile:** Represents the desired state of the organization's cybersecurity program.

When assessing an organization's cybersecurity program using the NIST CSF 2.0, start from the basics by understanding and evaluating the core functions, then begin assessing each layer of the cake to delve into the specific categories and subcategories, ensuring that all necessary aspects are covered. Next, assess the implementation tiers to determine the maturity of the organization's cybersecurity practices. Finally, use the profiles to align the cybersecurity activities with the organization's goals and identify gaps between the current and target states.

By using this systematic approach, much like developing a bakery business plan, organizations can systematically and comprehensively assess and improve their cybersecurity program ensuring that all critical areas are addressed and aligned with the organization's strategic objectives.

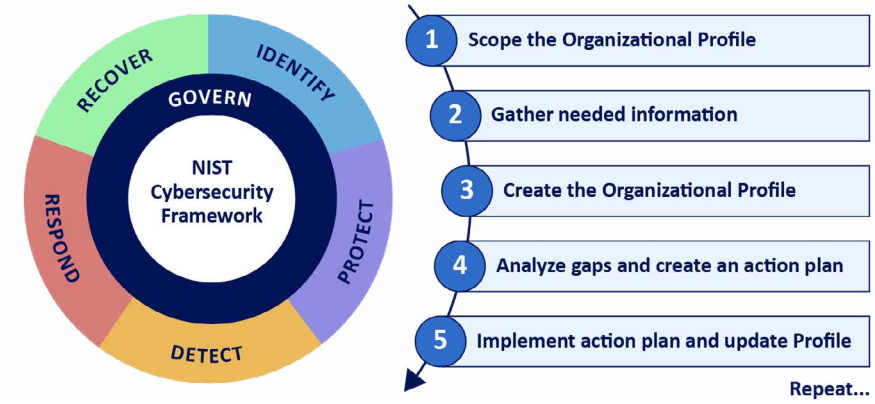


Figure 16: Creating and Using a CSF Organizational Profile

Conclusion

In the face of an increasingly complex and overwhelming cybersecurity landscape, the cyber cake concept emerges as a beacon of clarity. What began as a metaphor for a layered approach to cybersecurity, represented by the Cyber Cake, embodies the very principles essential for achieving lasting resilience. This framework, formally known as the Cyber CAKE--Continuous Assessment, Knowledge, and Education--provides a clear path for organizations to embrace those principles and build a more secure future. Airmen and Guardians need a strategy that empowers them to master the art of cyber defense operations, particularly the critical discipline of resilience—the Cyber Cake is that strategy. By embracing this structured, transparent framework we can demystify cybersecurity making it accessible and achievable for everyone. The Cyber Cake empowers organizations to replace ambiguity with clarity, transforming a daunting obstacle course into a series of manageable steps toward a more secure future.

The Cyber Cake concept also acknowledges the unpredictable nature of cyber threats, preparing organizations for the potential of "black swan" events—those rare, high-impact incidents that often defy prediction. Just as a baker might design their kitchen to withstand an earthquake, even in a low-risk area, cybersecurity professionals must anticipate and mitigate unforeseen risks. This proactive mindset, embedded within the Cyber Cake's layered approach, equips organizations with the agility and resilience to weather even the most unanticipated of these occurrences. By implementing robust security controls, fostering a culture of awareness, and maintaining flexible response plans, organizations can better position themselves to navigate the unknown and emerge stronger from even the most challenging security challenges.

Each layer of the Cyber Cake represents a critical stage in building and measuring a strong cybersecurity program, offering not just tangible steps and proven strategies but also built-in assessment modalities. These assessments, baked into each layer, provide a clear metric for gauging how effectively each element has been implemented, empowering individuals and organizations to understand their strengths and address any gaps. Just as a cake requires careful attention to detail and a precise blend of ingredients, a robust cybersecurity posture demands a thorough approach. Neglecting critical elements, misapplying security controls, or skipping crucial assessments is akin to using spoiled milk or forgetting the baking powder—the resulting outcome will be far from satisfactory.

Without a cohesive and comprehensive approach guided by the Cyber Cake, organizations leave themselves vulnerable to a host of negative consequences, jeopardizing their data, operations, and overall mission success.

By meticulously following the cyber cake recipe, organizations can break down silos and foster the cross-functional interoperability essential for effective cybersecurity while also mitigating the consequences of duplicative and manual processes. Just as a cake requires all ingredients to work together harmoniously, a robust cybersecurity posture demands a unified approach where information and expertise are freely shared. This integrated approach, eliminating cyber stovepipes, enhances threat visibility, enables swift incident response, and strengthens the overall security fabric.

The Cyber Cake concept empowers us to 'bake in' cybersecurity and become resilient by design, delivering mission capabilities at the intersection of innovative solutions and cybersecurity-aware Airmen and Guardians to compete, deter conflict, and win in and through cyberspace.

Back to Table of Contents >

This product was developed through the leadership and vision of Mr. Aaron Bishop and Dr. Merrick S. Watchorn, DMIST, whose ideas shaped its direction, and the dedicated efforts of Major Brandon Eaves, who brought it to life. Additional thanks to Col Becky Beers, Lt Col Shawn Crowe, Lt Col Eric Zymboly, Mr. William Hass, and Ms. Julienne Picot Chappell for their valuable feedback throughout the many iterations.

SAF/CNZ

OFFICE OF THE CHIEF INFORMATION SECURITY OFFICER

2025