The Cyber Cake

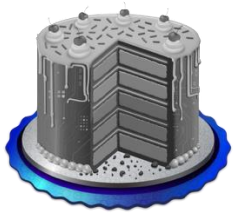
The Future of Department of the Air Force Cybersecurity

Mr. Aaron Bishop

SAF/CNZ

DAFITC 2025

Introduction



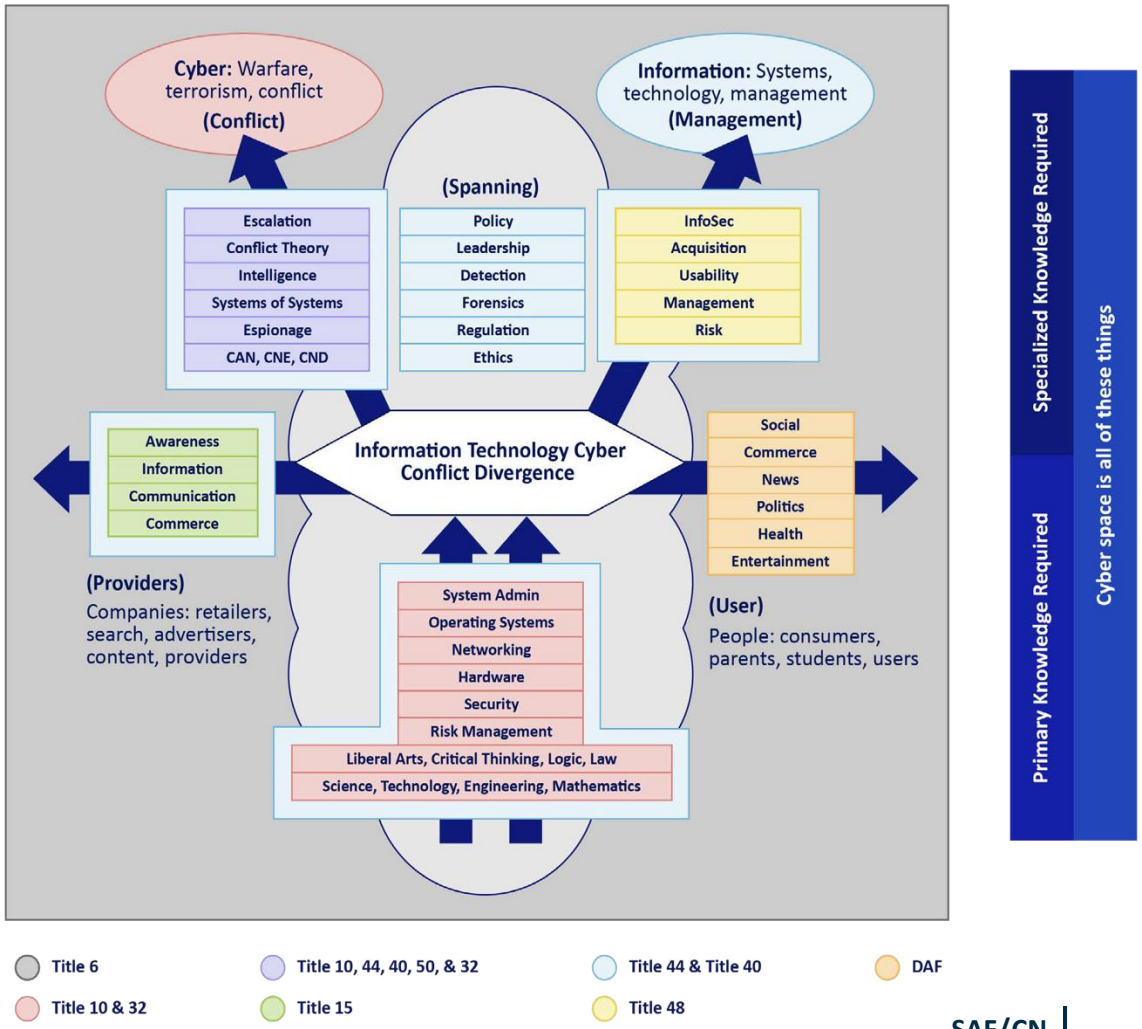
In a world increasingly reliant on digital infrastructure, the present approach to cybersecurity and its many management responsibilities poses significant national security risks, particularly as we strive to secure information ecosystems from emerging threats. The cyber cake draws upon known standards 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.

The Cyber Paradigm: What is Cyberspace?

- **Complex, Multidimensional Domain**: Cyberspace encompasses conflict, communication, commerce, and societal development.
- **Fragmented Knowledge Base:** No single individual can master all diverse areas, from systems administration to social, political, and economic dimensions.
- **Collaboration Across Disciplines:** Professionals from various fields must work together to grasp the nuances of cyberspace.
- **Perceived Complexity:** The cybersecurity landscape is often seen as complex and overwhelming.
- **Need for Clear Path and Reliable Tools:** Professionals seek a clear path and reliable tools to achieve a resilient cybersecurity posture.

The Solution: How the Cyber Cake Addresses the Paradigm

- **Structured, Transparent Framework:** The Cyber Cake provides a structured, transparent framework that demystifies cybersecurity.
- **Accessible and Achievable:** Makes cybersecurity more accessible and achievable for everyone.
- **Manageable Steps:** Transforms cybersecurity from a daunting obstacle course into a series of manageable steps.
- **Layered Approach:** Each layer of the cake represents a foundational element, guiding professionals through critical stages.
- **Clear Understanding and Roadmap:** Offers a clear understanding of security measures and a roadmap for prioritizing future efforts.

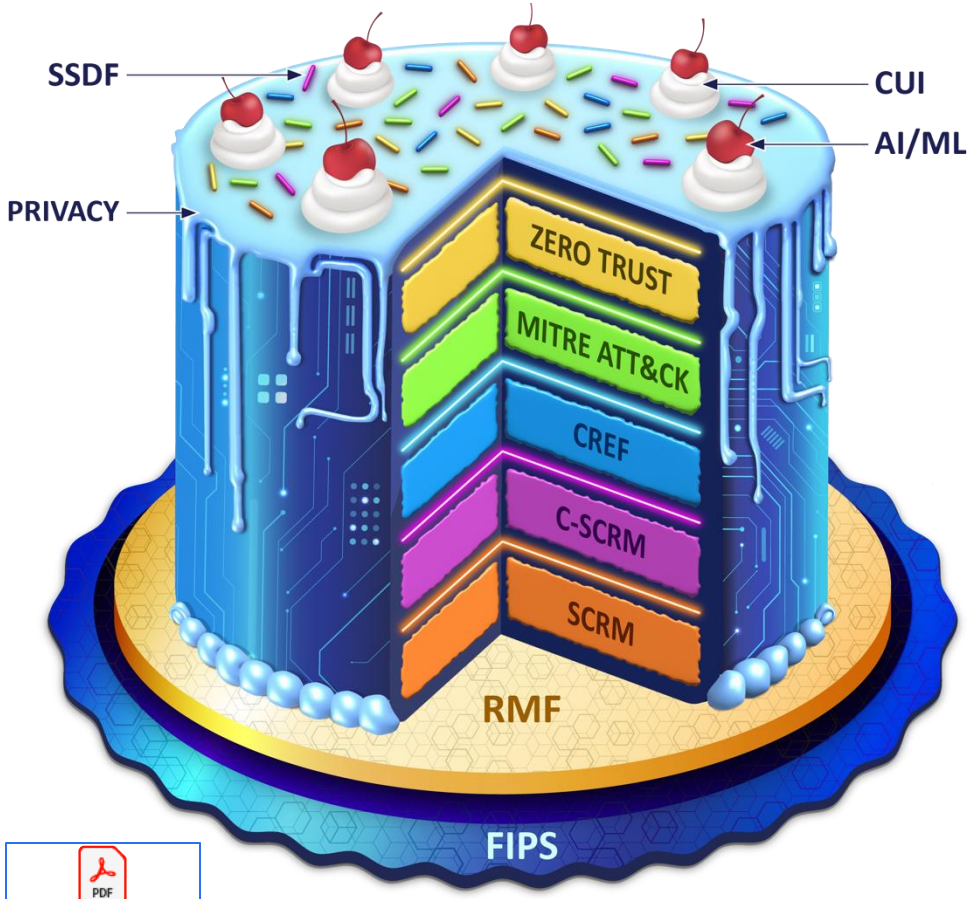


The Cyber CAKE : Continuous Assessment, Knowledge, and Education

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.

The Concept

- The **Base** of the Cyber Cake is the Federal Information Processing Standards (FIPS).
- NIST's Risk Management Framework (RMF) serves as the **Platter** 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 and assessments that work together to enable organizations to effectively mitigate cyber threats and maintain a resilient cybersecurity posture in a rapidly evolving cyber landscape.
- **The Toppings** are represented by critical concepts including Artificial Intelligence (AI), Privacy, Controlled Unclassified Information (CUI), and the Secure Software Development Framework (SSDF).
- The **Cake Slice** represents the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) 2.0 and is used to assess how the base, layers, and toppings interact and work together and evaluate how well cybersecurity measures are integrated into the organization's systems and processes.



The Cookbooks

Every layer of the Cyber Cake has a box at the bottom left that will take you to the core "Cookbooks" (references) that will help you for each topic discussed in the layer. It is important to remember that the listed Cookbooks are only the core references of the referenced subject. The "Cookbooks" box here below will take you to a listing of all the references.

DAF Cyber Cake, May 2025

Cyber Cake Cookbooks

The Base: Federal Information Processing Standards

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. The FIPS were created by NIST in accordance with the Information Technology Management Reform Act of 1996 and Computer Security Act of 1987 to be the standards used by the Federal Government and the DoD.

FIPS are security standards for federal and defense cybersecurity compliance, specifically focusing on data encryption. FIPS standards are developed when there are no acceptable industry standards or solutions for a particular government requirement.

The FIPS:

- Provide a framework for secure practices, such as encryption, authentication, and access control.
- Helps practitioners implement robust security controls for attaining a robust cybersecurity posture.
- Provides guidelines for risk management, including risk assessment, mitigation, and monitoring.
- Are developed for use by the Federal Government, many in the private sector voluntarily use these standards.

FIPS Examples

FIPS 199
Standards for Security Categorization of Federal Information and Information Systems

FIPS 200
Minimum Security Requirements for Federal Information and Information Systems

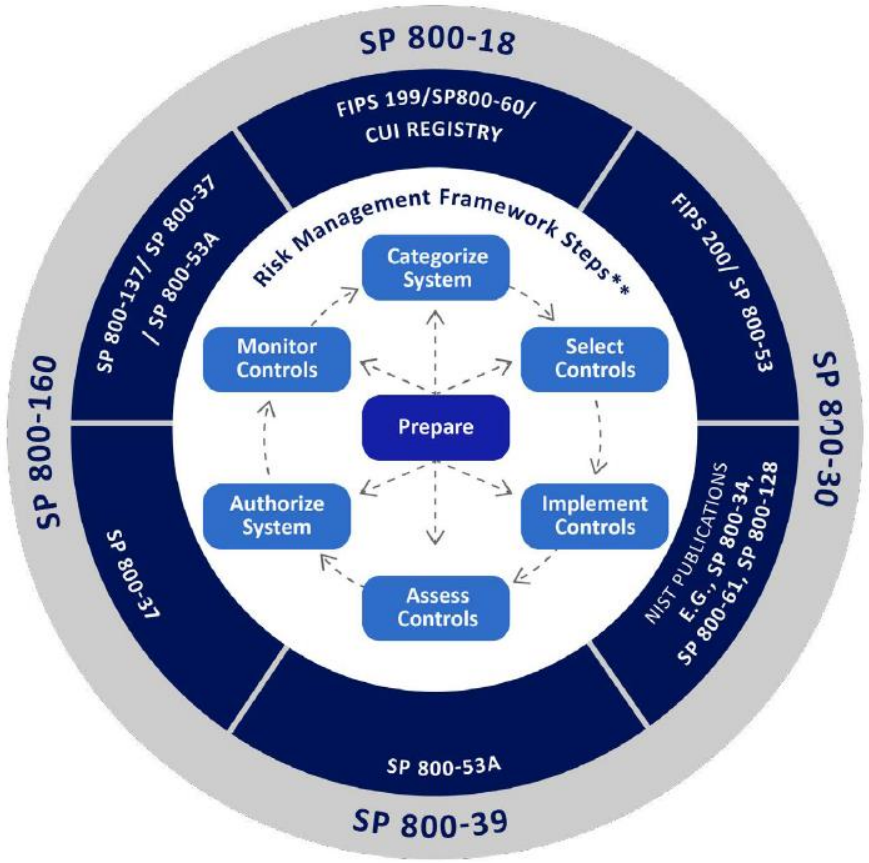
FIPS 140-3
Security Requirements for Cryptographic Modules

FIPS 201-3
Personal Identity Verification (PIV) of Federal Employees and Contractors

Core FIPS Cookbooks

The Platter: Risk Management Framework 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. RMF is used to authorize the operation of information systems, which involves assessing the security controls and risk management throughout the entire lifecycle of the systems from design to disposal.



- **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.

A well-executed Prepare step ensures that organizations fully understand their systems, data, and operational context, enabling them to make informed risk management decisions. Defining the scope and boundaries of their systems, organizations gain the clarity needed to effectively assess risks, select controls, and attain a resilient cybersecurity posture. Neglecting preparation, however, can lead to misaligned controls, ineffective security measures, and an ultimately weaker cybersecurity posture.

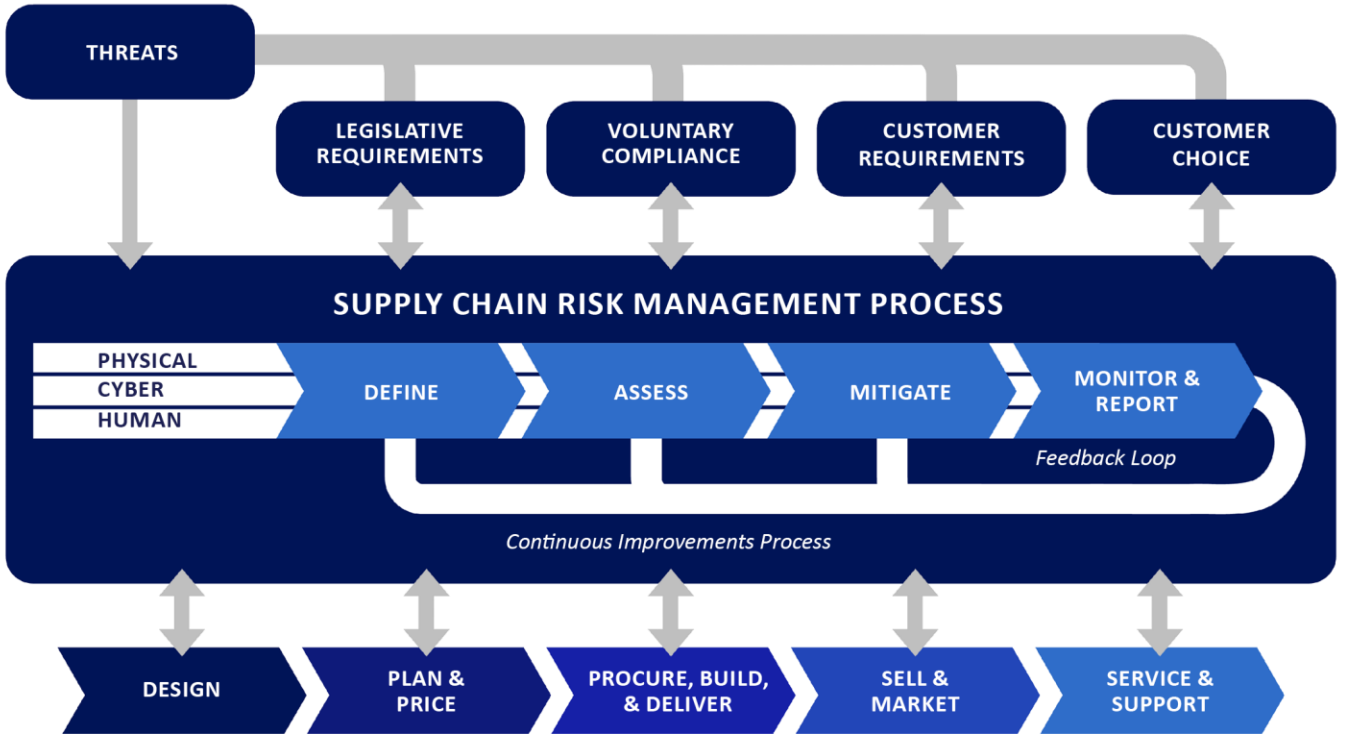
Core RMF Cookbooks

Layer One: Supply Chain Risk Management Strategies

Supply Chain Risk Management (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.

The Supply Chain Risk Management (SCRM) process is an essential component of overall risk management and helps organizations to:

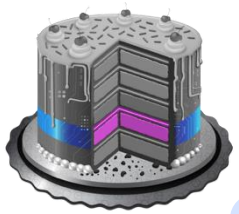
- **Define** potential risks and vulnerabilities in the supply chain
- **Assess** the likelihood and impact of these risks
- **Mitigate** risk by developing strategies to manage and prepare for possible risks
- **Monitor and Report** the effectiveness of risk response measures, and identify risk impacting change to information systems



The figure above illustrates how the process is influenced by various external factors such as threats, legislative requirements, voluntary compliance to environmental risks, customer 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.

Core SCRM Cookbooks

Layer Two: Cybersecurity Supply Chain Risk Management



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.

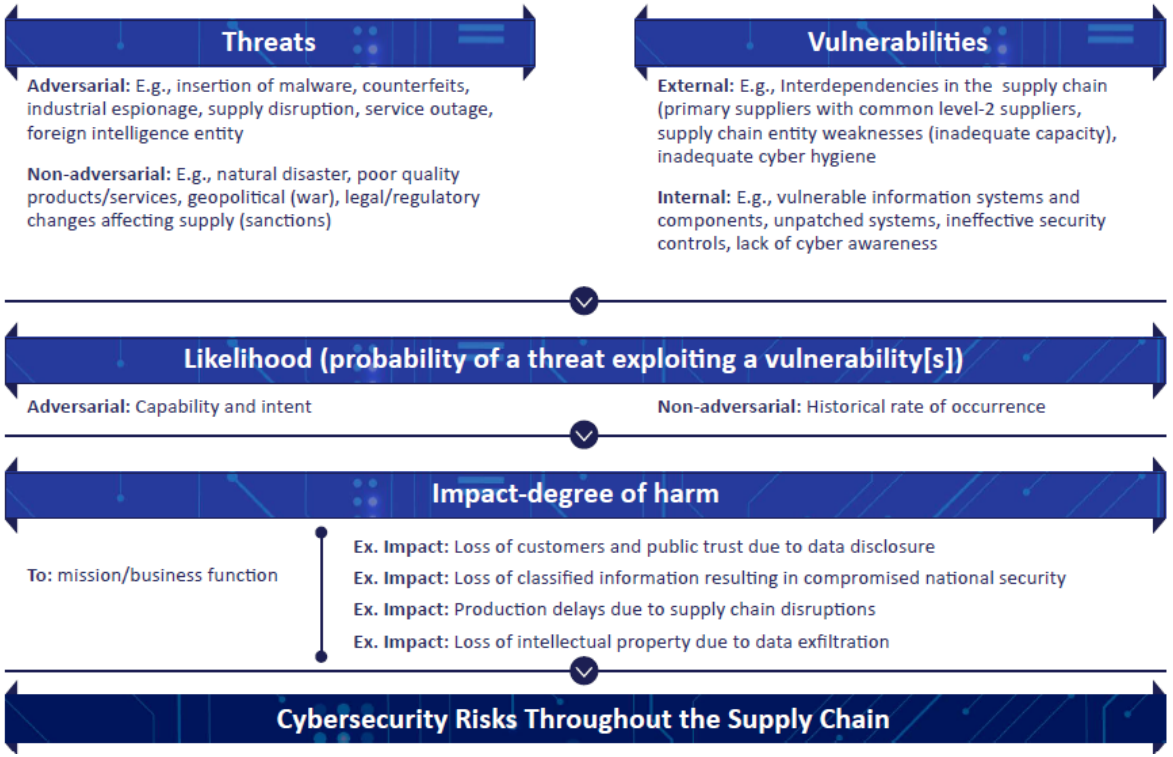
C-SCRM is a critical process that involves a thorough threat analysis, vulnerability assessment, likelihood assessment, and impact analysis to identify and mitigate cyber threats to an organization's supply chain.

Threat Analysis: Identifies 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: Identifies weaknesses within the supply chain that could be exploited by identified threats. Vulnerabilities can be external.

Likelihood Assessment: 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: Evaluates the potential consequences of a threat exploiting a vulnerability. This includes assessing the potential consequences of a threat exploiting a vulnerability. Examples of impacts include loss of customers and public trust, loss of classified information, production delays, and loss of intellectual property.



Core C-SCRM Cookbooks

Layer Three: Cyber Resilience Engineering Framework

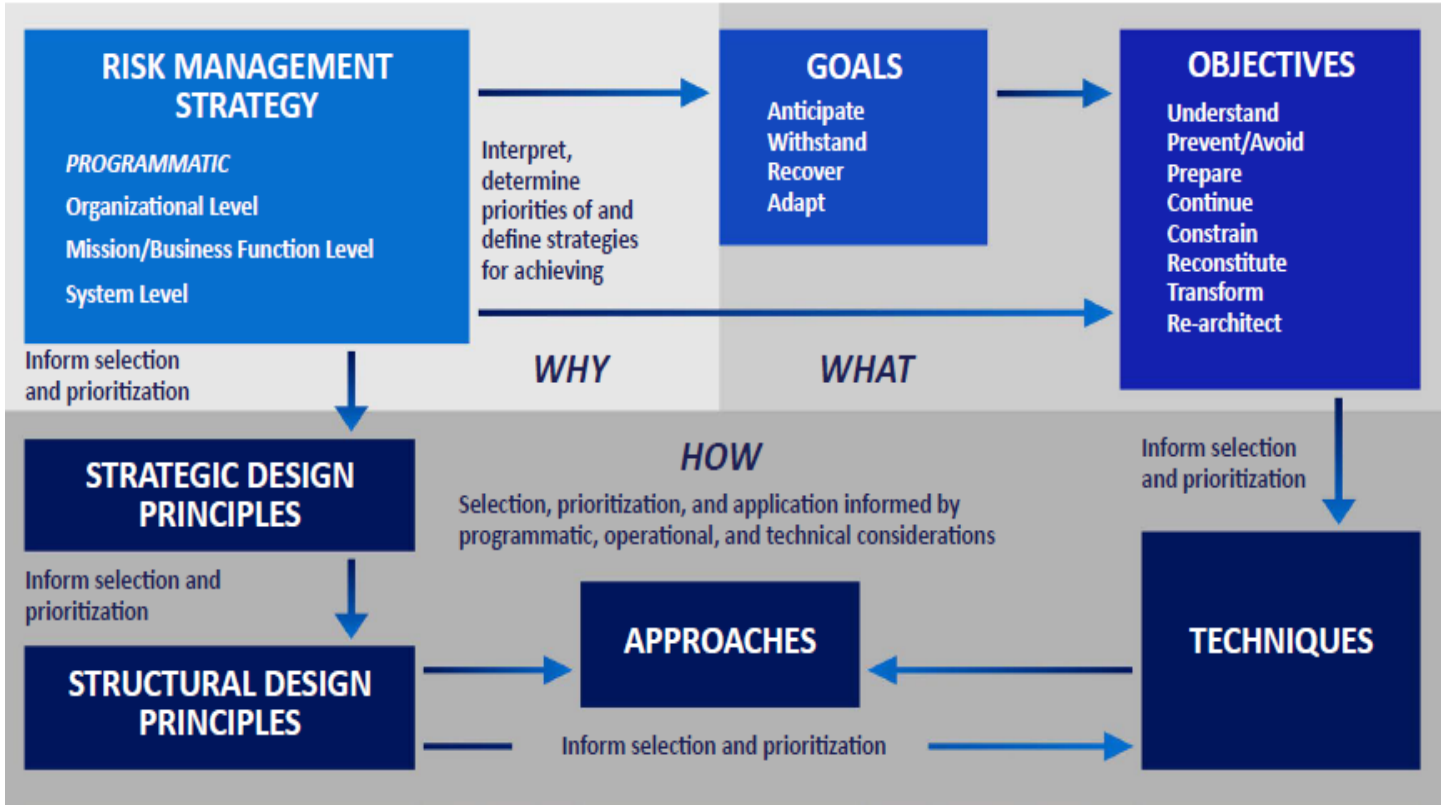
The Cyber Resilience Engineering Framework (CREF) is a structured approach that strengthens an organization's ability to maintain essential functions and adapt during cyber disruptions. It combines elements of cybersecurity, business continuity, and systems engineering to build robust systems that can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

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 that will enable the development of questions.

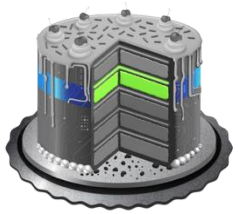
Cyber resiliency techniques are a set of practical methods and tools used to implement the selected approaches to maintain resilience. The cyber resiliency techniques reflect an understanding of the threats as well as the technologies, processes, and concepts related to improving cyber resiliency to 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.



Core CREF Cookbooks

Layer Four: Zero Trust



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.

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.

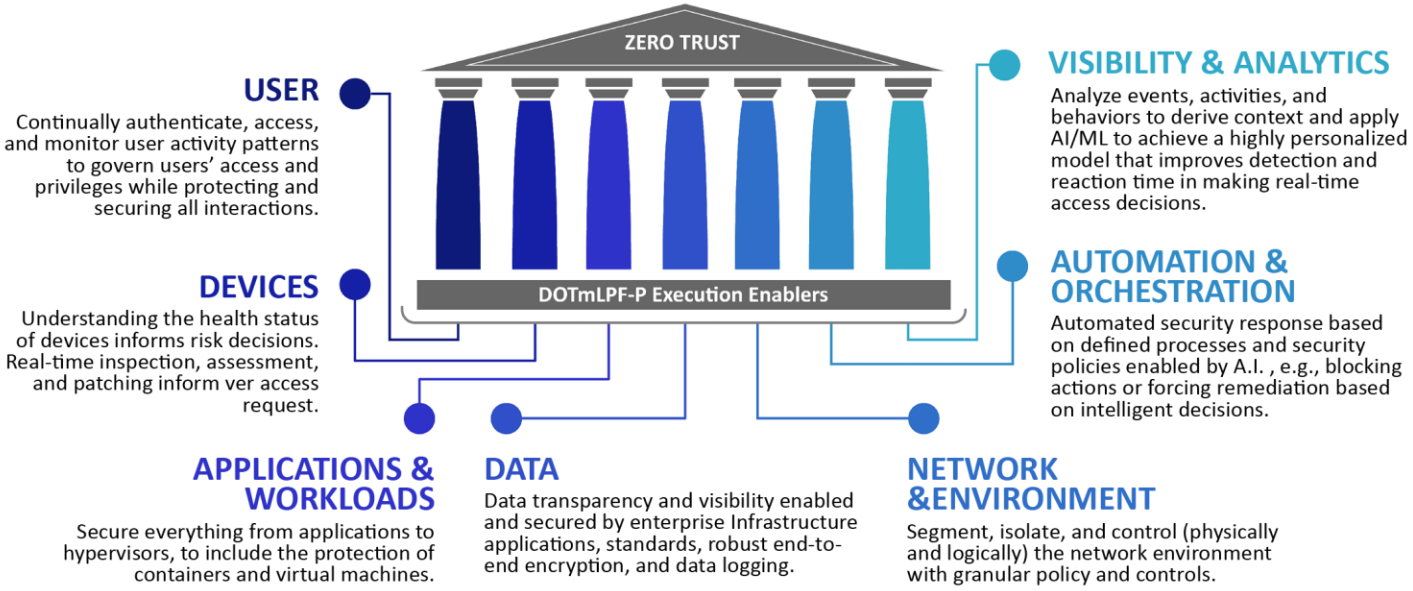
Presume Breach: There are hundreds of thousands of attempted cybersecurity attacks against DoD environments every day. Consciously operate and defend resources with the assumption that an adversary has presence within your environment. Enhanced scrutiny of access and authorization decisions to improve 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.

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.



Core Zero Trust Cookbooks

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.

The MITRE ATT&CK Framework Categorization of Cyber Attacks

Tactics

Tactics represent the "what" and "why" of an ATT&CK technique or sub-technique. Each tactic contains an array of techniques that network defenders have observed being used in the wild by threat actors.

Techniques

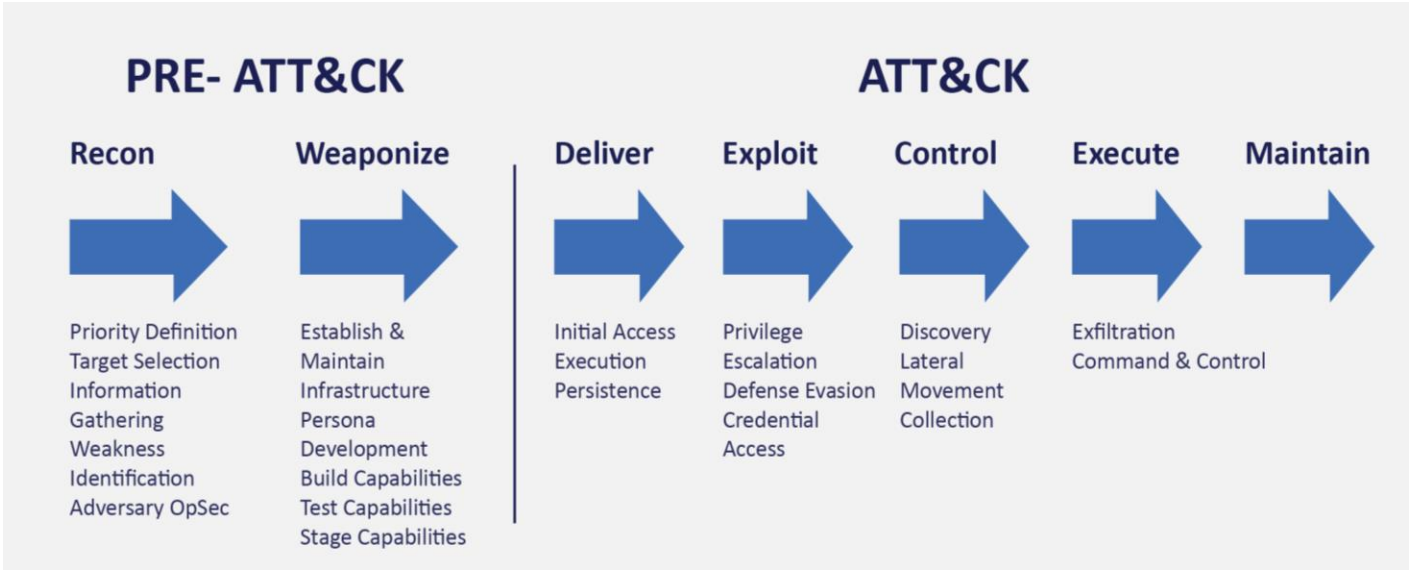
Techniques represent "how" an adversary achieves a tactical goal by performing an action. Techniques may also represent what an adversary gains by performing an action. A technique is a specific behavior to achieve a goal and is often a single step in a string of activities intended to complete the adversary's overall mission.

Sub-techniques

Sub-Techniques provide more granular descriptions of techniques. For example, there are behaviors under the OS Credential Dumping technique that describe specific methods to perform the technique. Sub-techniques are often, but not always, operating system or platform specific.

Procedures

Procedures are 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.



Core ATT&CK Cookbooks

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)/Machine Learning (ML) represents these finishing items for a cyber cake.

Privacy

Building Customers' 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.

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.

Facilitating Communication:
Facilitating communication among stakeholders, including customers, employees, and regulators, about how data is collected, used, shared, and protected.

SSDF

Prepare the Organization (PO):
Organizations should ensure that their people, processes, and technology are prepared to perform secure software development at the organization level.

Protect the Software (PS):
Organizations should protect all components of their software from tampering and unauthorized access.

Produce Well-Secured Software (PW):
Organizations should produce well-secured software with minimal security vulnerabilities in its releases.

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.

CUI

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.

CUI Markings:
Alert recipients that special handling may be required to comply with law, regulation, or Government-wide policy.

DoD/CUI:
Enables consistent processes to safeguard information for specific national security purposes, such as physical and operations security.

AI/ML

Cybersecurity Threats:
The increasing use of AI and ML in various aspects of life has also led to their adoption by malicious actors, posing significant threats to cybersecurity.

Phishing Attacks:
Can mimic the tone and language of high-level executives or other legitimate individuals, making them difficult to distinguish from genuine communications.

Malware:
Can adapt and evolve to evade detection by traditional security systems and can rapidly and quietly spread causing damage before detection.

The NIST AI RMF:
Provides a structured approach to managing AI-related risks, including those related to cyber security.

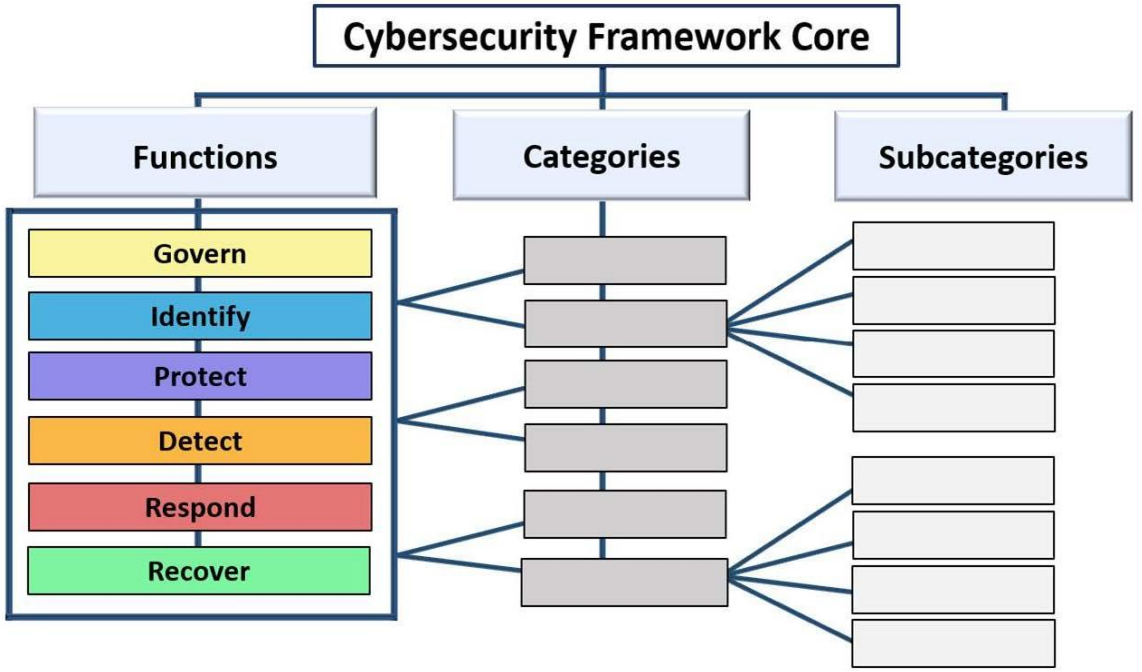
Core Toppings Cookbooks

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.

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. Each Function is divided into Categories, which are related cybersecurity outcomes that collectively comprise the Function. Subcategories further divide each Category into more specific outcomes of technical and management activities.

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



Core CSF 2.0 Cookbooks

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, now embodies the very principles essential for achieving lasting resilience. This framework 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.

Cyber Cake: Resilient by Design

The Cyber Cake concept 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. This proactive mindset equips organizations with the agility and resilience to weather even the most unanticipated occurrences. Cyber Cake's additional characteristics that underscore the essential features required for a resilient cybersecurity posture include:

- **Structure and Transparency:** The Cyber Cake concept is a structured and transparent framework that simplifies cybersecurity, providing a practical path to achieving a resilient cybersecurity posture that is accessible and attainable for everyone.
- **Comprehensive Layered Approach:** 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.
- **Baked-in Assessments:** The framework delivers baked-in assessment modalities into each layer that provides a clear metric for gauging how effectively each element has been implemented, empowering individuals and organizations to understand their strengths and address any gaps.
- **Cross-Functional Interoperability**: 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.
- **Promotes a unified approach:** The strategy empowers us to become resilient by fostering an environment where information and expertise are freely shared, enhancing threat visibility, enabling swift incident response, and strengthening 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.

Core Cookbooks: References

Core Federal Information Processing Standards (FIPS)

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

RMF

- 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
- NISP SP 800-53r5, Security and Privacy Controls for Information Systems and Organizations, https://csrc.nist.gov/pubs/ sp/800/53/r5/upd1/final
- 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
- NIST SP 800-53b, Control Baselines for Information Systems and Organizations, https://csrc.nist.gov/pubs/ sp/800/53/b/upd1/final
- 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

SCRM

- 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
- 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
- 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

C-SCRM

- NIST SP 800-161r1-upd1, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations, https://csrc.nist.gov/pubs/ sp/800/161/r1/upd1/final
- NIST SP 1326, NIST Cybersecurity Supply Chain Risk Management: Due Diligence Assessment Quick-Start Guide, https://csrc.nist.gov/pubs/sp/1326/ipd
- 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
- 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
- DoD Information and Communications Technology Supply Chain Risk Management Home Page, https://www.denix.osd.mil/ict-scrm/

CREF

- NIST Special Publication 800-160 Volume 1 Revision 1, Engineering Trustworthy Secure Systems, https://nvlpubs.nist.gov/nistpubs/ SpecialPublications/NIST.SP.800- 160v1r1.pdf
- 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

Zero Trust

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

MITRE ATT&CK

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

Privacy, SSDF, CUI, and AI Strategies

- NIST Privacy Framework, https://www.nist.gov/privacy-framework/privacy-framework
- NIST Secure Software Development Framework (SSDF), https://csrc.nist.gov/projects/ssdf
- The DoD CUI Program, https://www.dodcui.mil/
- The NIST AI RMF Home Page, https://www.nist.gov/itl/ai-risk-management-framework
- NIST AI 100-1, The Artificial Intelligence (AI) Risk Management Framework, https://nvlpubs.nist.gov/nistpubs/ ai/NIST.AI.100-1.pdf
- 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

Cybersecurity Framework 2.0

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

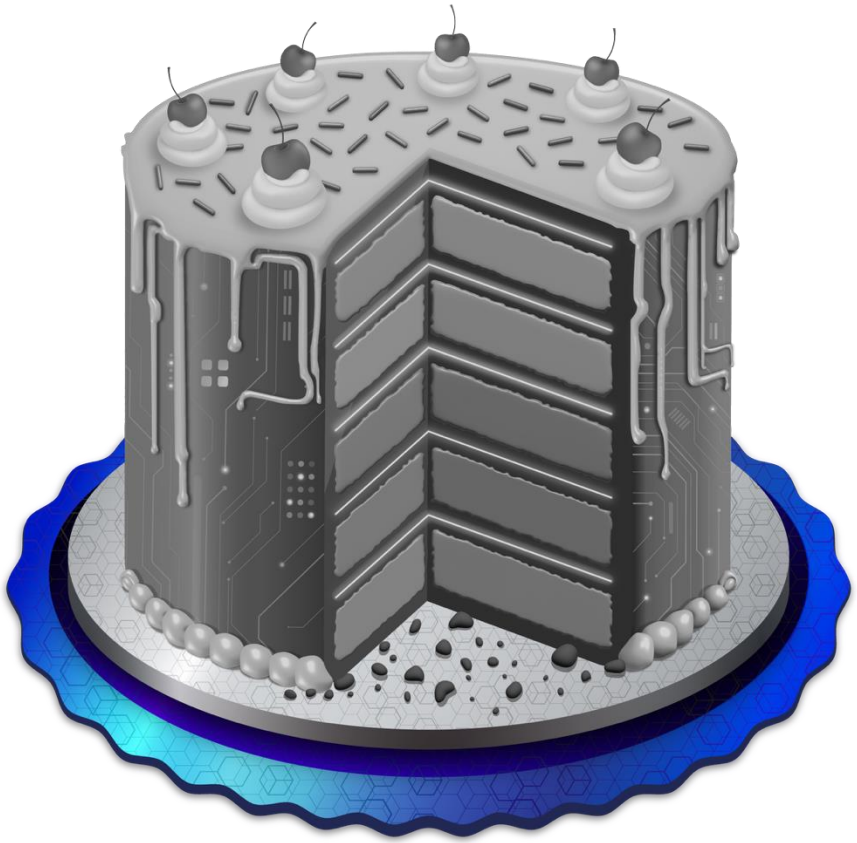
Core Cookbooks: FIPS

FIPS 199, Standards for Security Categorization of Federal Information and Information Systems,
https://csrc.nist.gov/pubs/fips/199/final

FIPS 200, Minimum Security Requirements for Federal Information and Information Systems,
https://csrc.nist.gov/pubs/fips/200/final

FIPS 140-3, Security Requirements for Cryptographic Modules,
https://csrc.nist.gov/pubs/fips/140-3/final

FIPS 201-3, Personal Identity Verification (PIV) of Federal Employees and Contractors
https://csrc.nist.gov/pubs/fips/201-3/final



Back to FIPS

Core Cookbooks: RMF

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

NISP SP 800-53r5, Security and Privacy Controls for Information Systems and Organizations,
https://csrc.nist.gov/pubs/ sp/800/53/r5/upd1/final

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

NIST SP 800-53b, Control Baselines for Information Systems and Organizations,
https://csrc.nist.gov/pubs/ sp/800/53/b/upd1/final

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

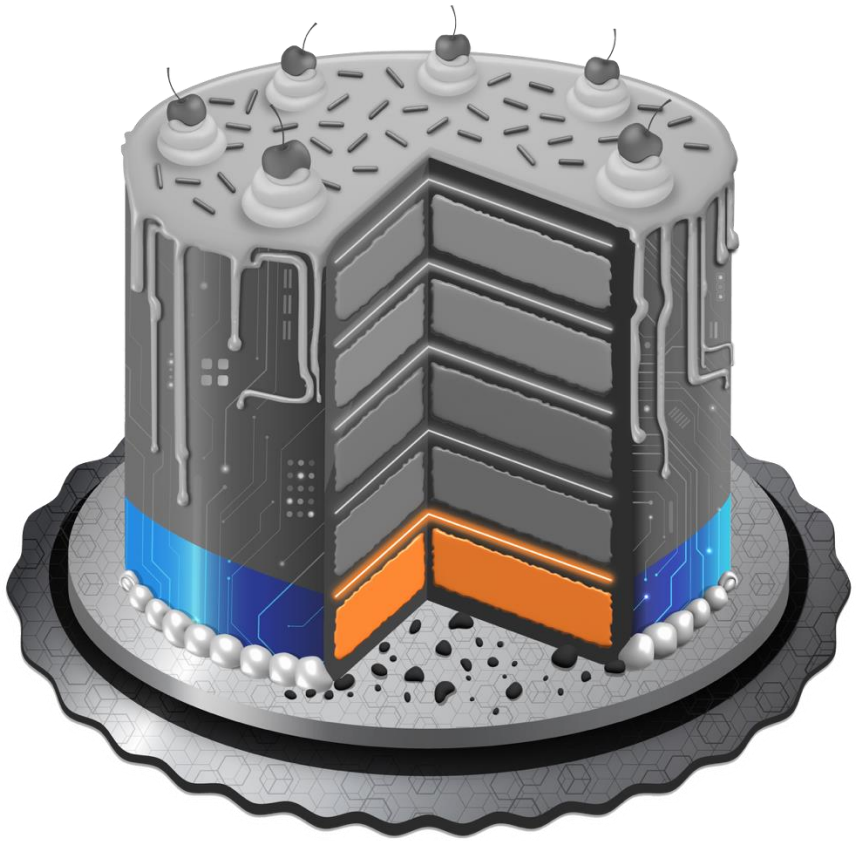
Back to RMF

Core Cookbooks: SCRM

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

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

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



Back to SCRM

Core Cookbooks: C-SCRM

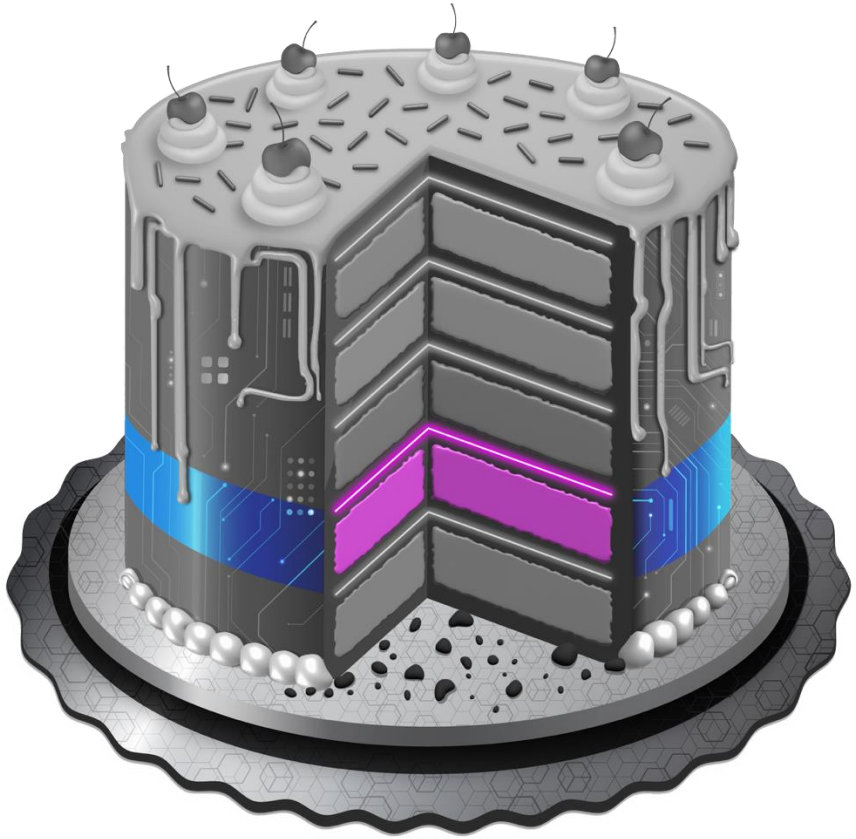
NIST SP 800-161r1-upd1, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations, https://csrc.nist.gov/pubs/ sp/800/161/r1/upd1/final

NIST SP 1326, NIST Cybersecurity Supply Chain Risk Management: Due Diligence Assessment Quick-Start Guide, https://csrc.nist.gov/pubs/sp/1326/ipd

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

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

DoD Information and Communications Technology Supply Chain Risk Management Home Page, https://www.denix.osd.mil/ict-scrm/

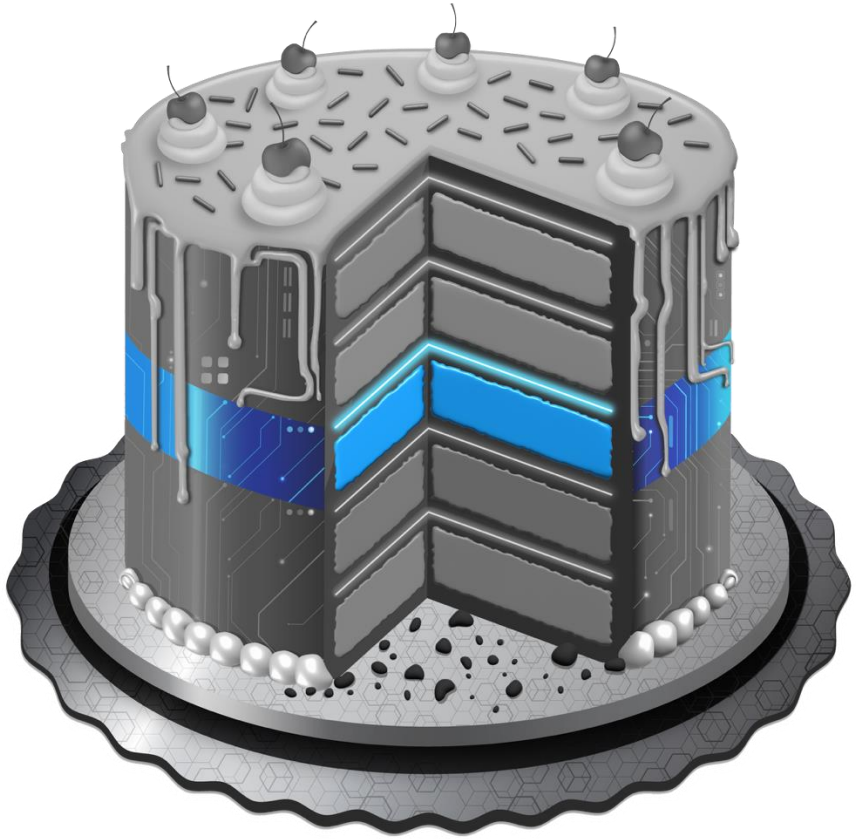


Back to C-SCRM

Core Cookbooks: CREF

NIST Special Publication 800-160 Volume 1 Revision 1, Engineering Trustworthy Secure Systems, https://nvlpubs.nist.gov/nistpubs/ SpecialPublications/NIST.SP.800-160v1r1.pdf

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



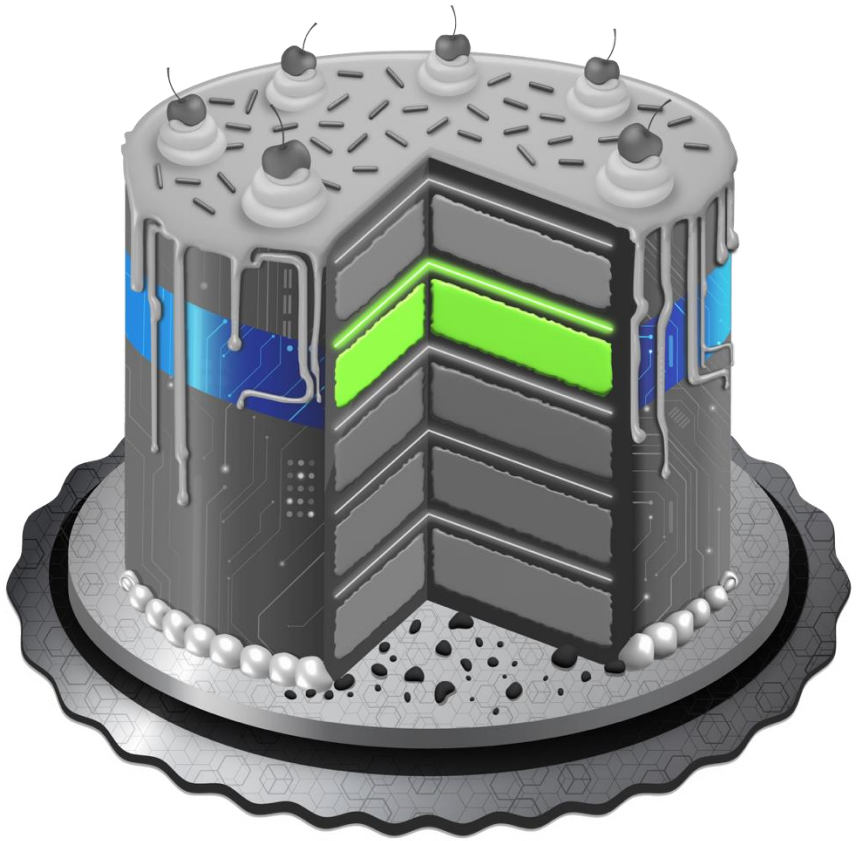
Back to CREF

Core Cookbooks: Zero Trust

NIST Special Publication 800-207,
Zero Trust Architecture,
https://www.nist.gov/publications/zero-trust-architecture

DoD Zero Trust Strategy,
https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-ZTStrategy.pdf

DAF Zero Trust Strategy v1.0,
https://www.safcn.af.mil/Portals/64/Documents/Strategy/DAF%20Zero%20Trust%20Strategy%20v1.0%20(002).pdf



Back to Zero Trust

Core Cookbooks: MITRE ATT&CK Framework

MITRE ATT&CK,
https://attack.mitre.org/

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

Back to MITRE ATT&CK

Core Cookbooks: Privacy, SSDF, CUI, and AI Strategies

NIST Privacy Framework,
https://www.nist.gov/privacy-framework/privacy-framework

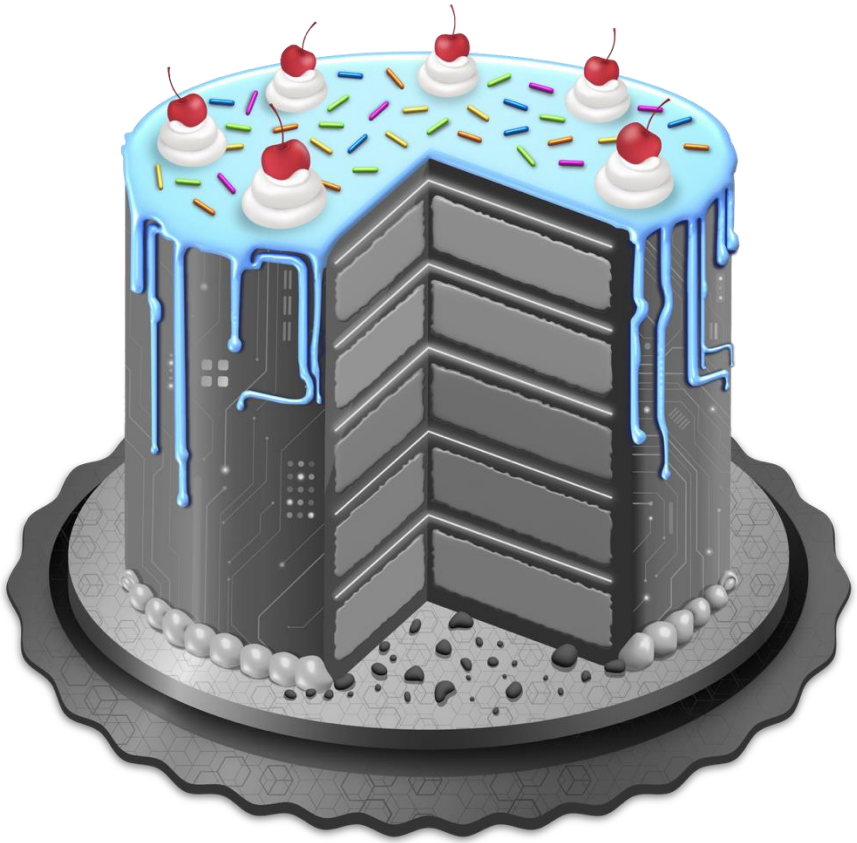
NIST Secure Software Development Framework (SSDF),
https://csrc.nist.gov/projects/ssdf

The DoD CUI Program,
https://www.dodcui.mil/

The NIST AI RMF Home Page,
https://www.nist.gov/itl/ai-risk-management-framework

NIST AI 100-1, The Artificial Intelligence (AI) Risk Management Framework,
https://nvlpubs.nist.gov/nistpubs/ ai/NIST.AI.100-1.pdf

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



Back to Toppings

Core Cookbooks: Cybersecurity Framework 2.0

NIST Cybersecurity Framework (CSF) 2.0,
https://www.nist.gov/cyberframework

DoDI 8500.01, Cybersecurity,
https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodi/850001_2014.pdf

DAFI 17-130, Cybersecurity Program Management,
https://static.e-publishing.af.mil/ production/1/saf_cn/publication /afi17-130/afi17-130.pdf

Back to CSF 2.0