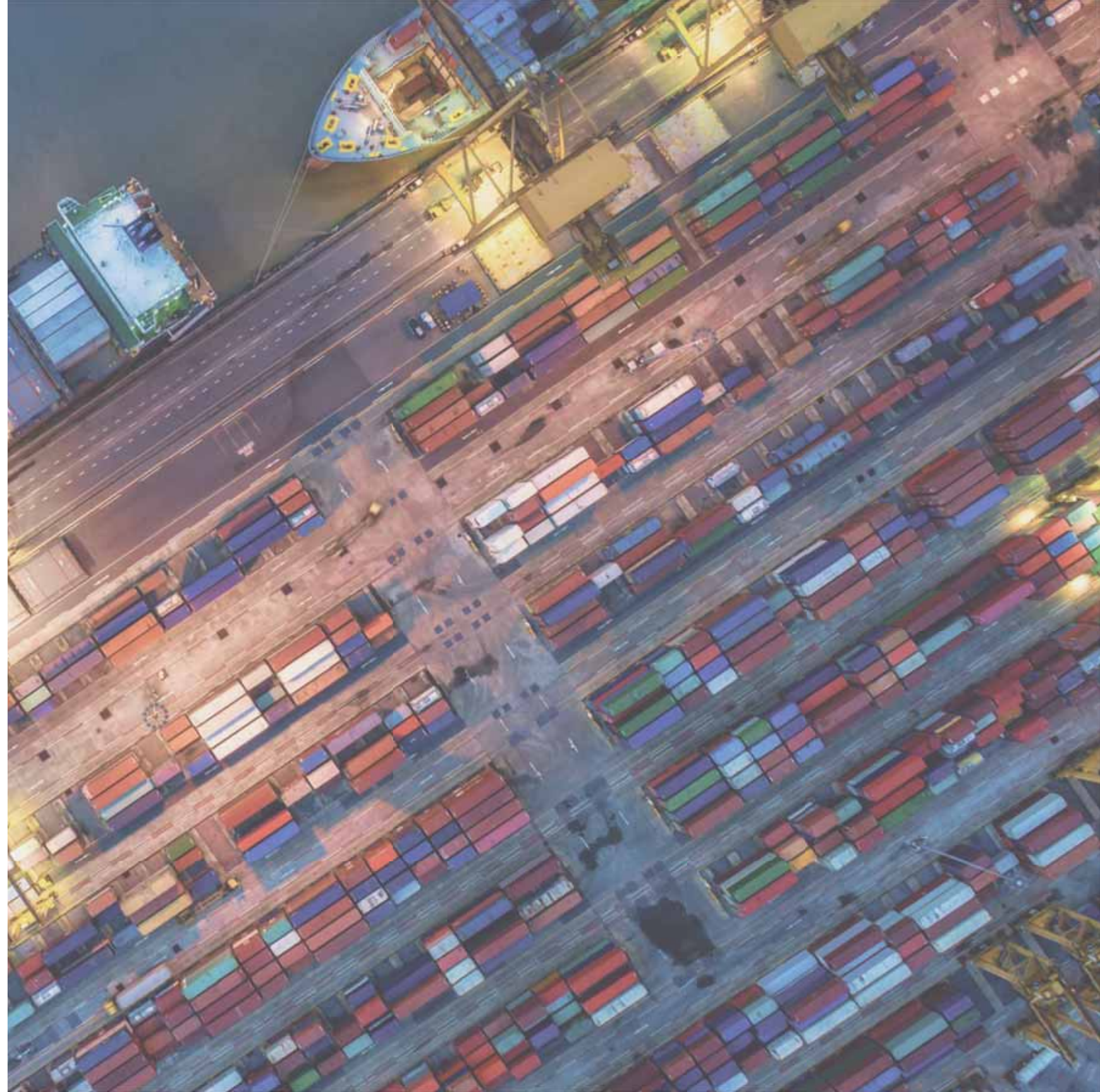


Implementation of PNNL C-SCRM Capabilities

Program Overview



Who We Are?



Faris Pirali

- Cyber Security Analyst
- PNNL Cyber Operations



Arcky Vielma

- Cyber Security Engineer
- Cyber-Aware Design & Testing Team, PNNL Research



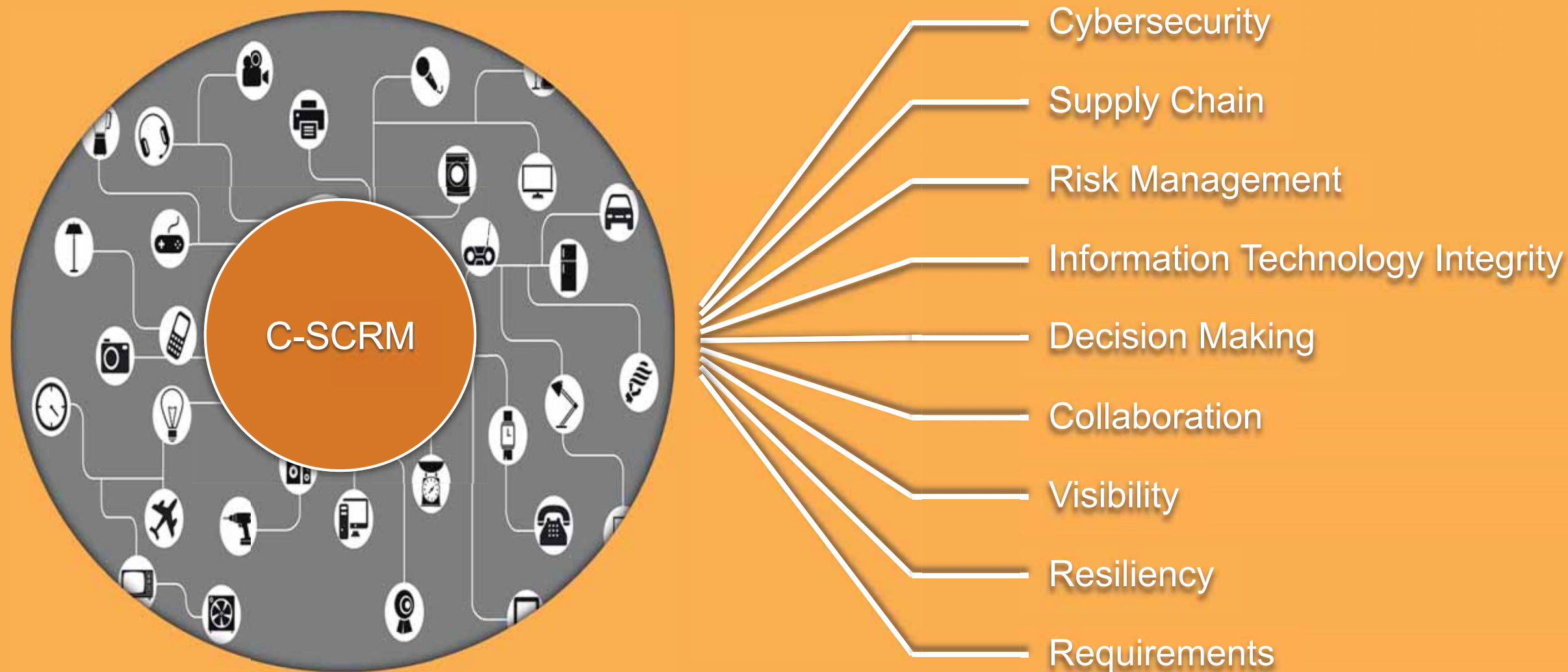
Pacific Northwest National Laboratory

Scientific Discovery

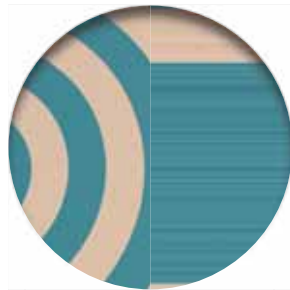
Science at Our Core

A leading center for scientific discovery in chemistry, data analytics, and Earth science, and for technological innovation in sustainable energy and national security.

What Do We Know About C-SCRM?



C-SCRM Operations Program Components



Goals

- Serve as the foundation of the program.
- Represent key, high-level initiatives.



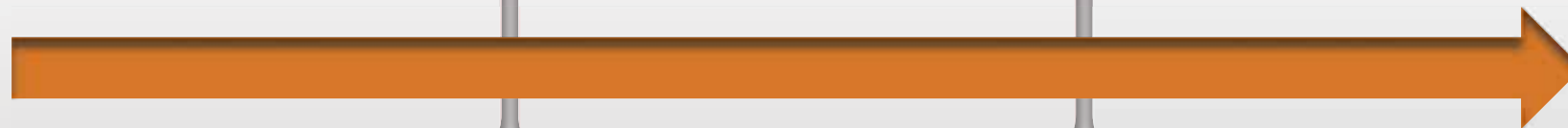
Objectives

- Support the achievement of goals.
- Are defined as annual or long-term targets.



Practices

- Consist of daily actions or tasks.
- Ensure consistent progress toward objectives.



Program Goals



Establish C-SCRM Program

Executive Orders & Federal Laws

- *Executive Order 14028 of May 2021 on Improving the Nation's Cybersecurity, May 2021*
- *Executive Order 13873 of May 2019 on Securing the Information and Communications Technology and Services Supply Chain, May 2019*
- *Federal Information Security Modernization Act, December 2014*
- *Federal Information Technology Acquisition Reform Act (2013-2014)*
- *Federal Acquisition Supply Chain Security Act (FASCSA) of 2018*

Department of Energy Requirements

- *DOE SC Cyber Security Program Plan*

PNNL Enterprise Policies & Requirements

- *Cyber Security Program Plan*

Government Standards & Guidelines

- *NIST SP 800-53 Revision 5, Security and Privacy Controls for Information Systems and Organizations*
- *NIST SP 800-53 B, Control Baselines for Information Systems and Organizations*
- *NIST SP 800-161, Revision 1 Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*
- *NIST SP 800-218, Version 1.1 Secure Software Development Framework*
- *NIST SP 800-37, Revision 2 Risk Management Framework for Information Systems and Organizations*
- *NIST SP 800-30, Revision 1, Guide for Conducting Risk Assessments*
- *NISTIR 8276, Key Practices in Cyber Supply Chain Risk Management*
- *FIPS 199, Standards for Security Categorization of Federal Information and Information Systems*



Establish C-SCRM Program

Document the Program Plan

- NIST SP 800-161 r1

Develop Policies, Process, and Procedures

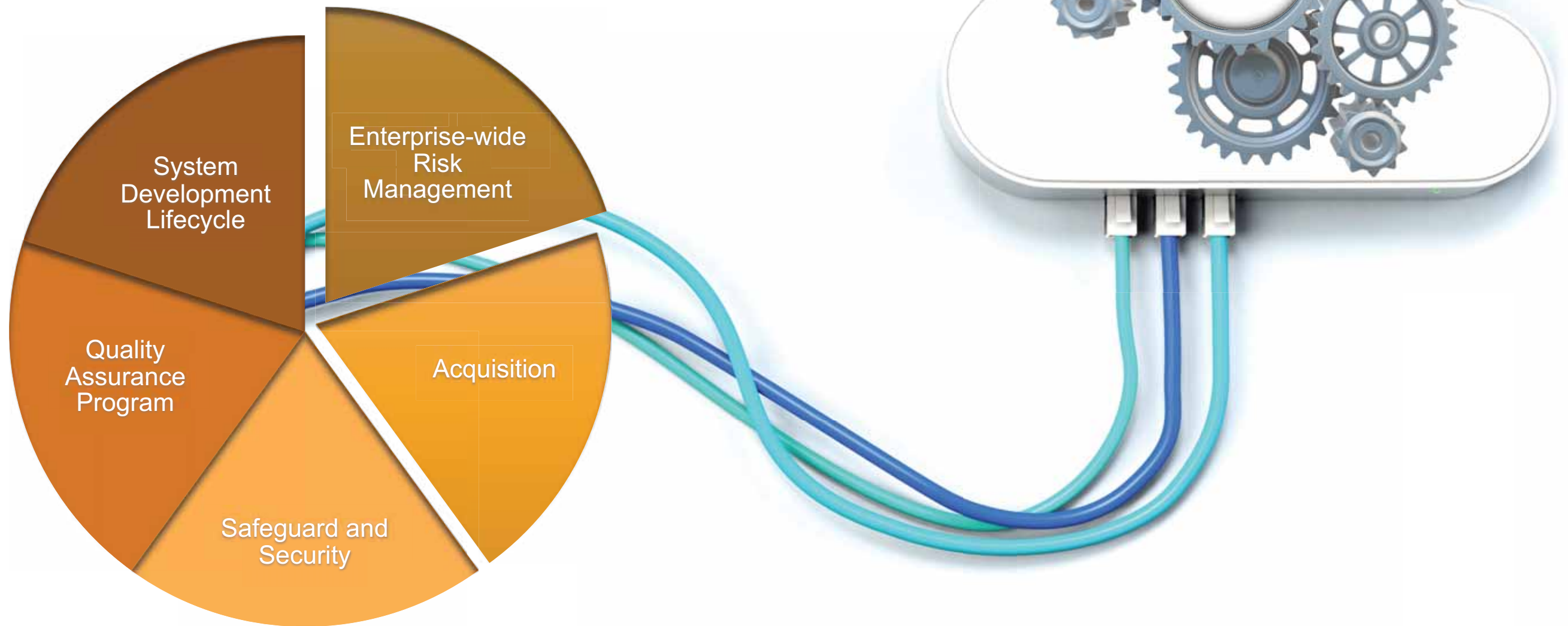
- NIST SP 800-53
- NIST SP 800-39
- NIST SP 800-171

Identify Roles and Their Responsibilities

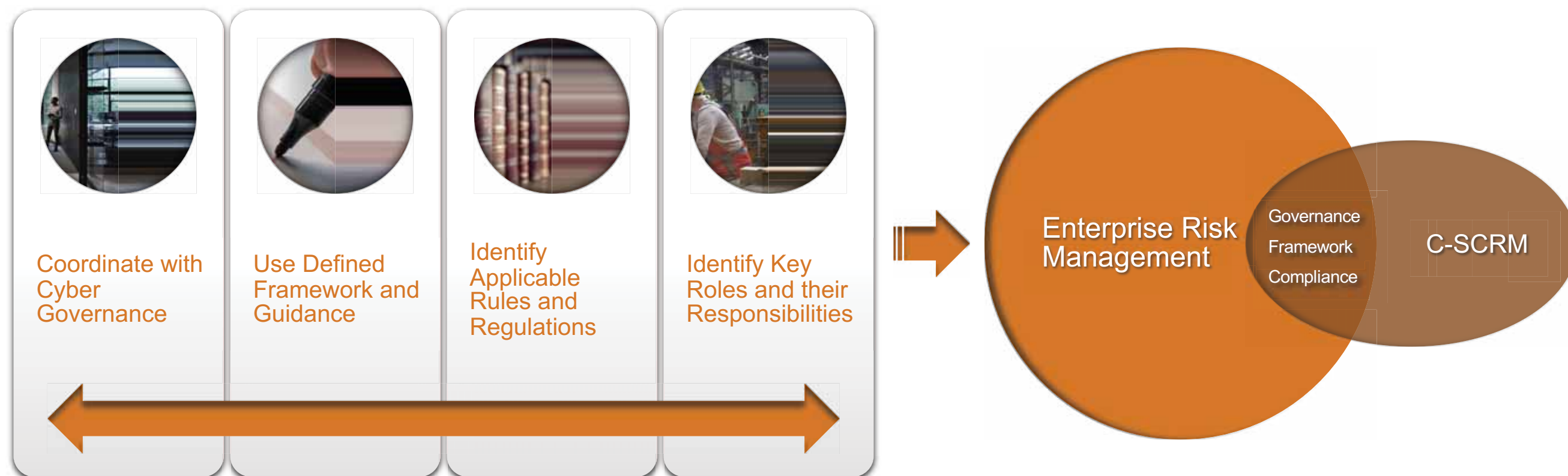
- Internal and external roles



Integration



C-SCRM in Enterprise-wide Risk Management



C-SCRM in Acquisition Activities



Identification

Identifying the product or service and gathering essential information needed to fulfill the evaluation step.



Evaluation

Utilizing available information, methods, and tools to assess the new product for any associated risks.



Validation

This is completed by Cyber Gov to verify everything to ensure that the new supplier can satisfy PNNL's cyber supply chain baseline requirements. Focusing on three factors where PNNL's cyber supply chain requirements are applicable: technical, physical, and human factors.



Monitoring

Continuously monitor suppliers and their associated products and services. Perform periodic reviews and re-evaluations of pre-approved products, this may include both hardware and software



Detection

Use and apply appropriate methods during monitoring phase to detect changes and identify any cybersecurity risks that may affect business operation.



Assessment

Analyze and assess the identified changes to determine the likelihood and potential impact.



Responding

Develop and implement a response strategy. This may include replacement, supplier off-boarding, and product disposal, if necessary.



Inventory

Conduct a thorough inventory of all assets, data, and systems shared with the vendor. Develop a data transfer and deletion plan to securely move necessary data and eliminate sensitive information.



Access Control and Security

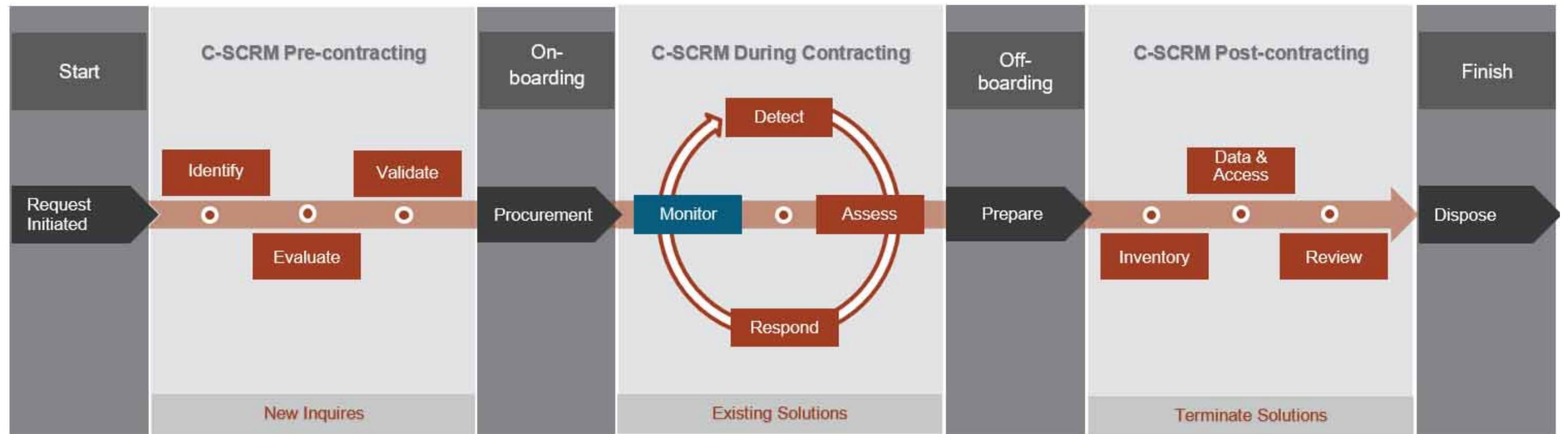
Revoke all user access to the systems, networks, and applications. Disable any API keys, tokens, or other credentials. Conduct a final data security review to verify complete data removal.



Post-offboarding Security and Legal Considerations

Review system configurations and network settings to identify and mitigate vulnerabilities. Update security policies and incident response plans. Consult with legal counsel to address contractual and legal obligations.

C-SCRM Lifecycle in Acquisition



Support the Program



Use Authorized Tools and Methods to Promptly and Responsively Complete Suppliers and Products Due Diligence Checks.



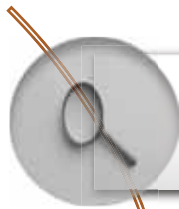
Implement Advanced Threat Intelligence and Analysis Capabilities.



Ensure Notifications of Supply Chain Compromises are Established.



Manage the Program



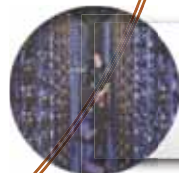
Conduct Thorough and Timely Due Diligence Checks on Products and Suppliers.



Timely Detection and Response to Cyber Supply Chain Related Incidents and Events.



Implement Automation for Processes and Procedures Whenever Feasible.



Ensure Recovery Plans Exist for Critical Systems and Data.



Coordination & Partnership

Internal



Testing and Validation



Threat Intelligence



Continuous Monitoring

External



PNNL's Cyber Research

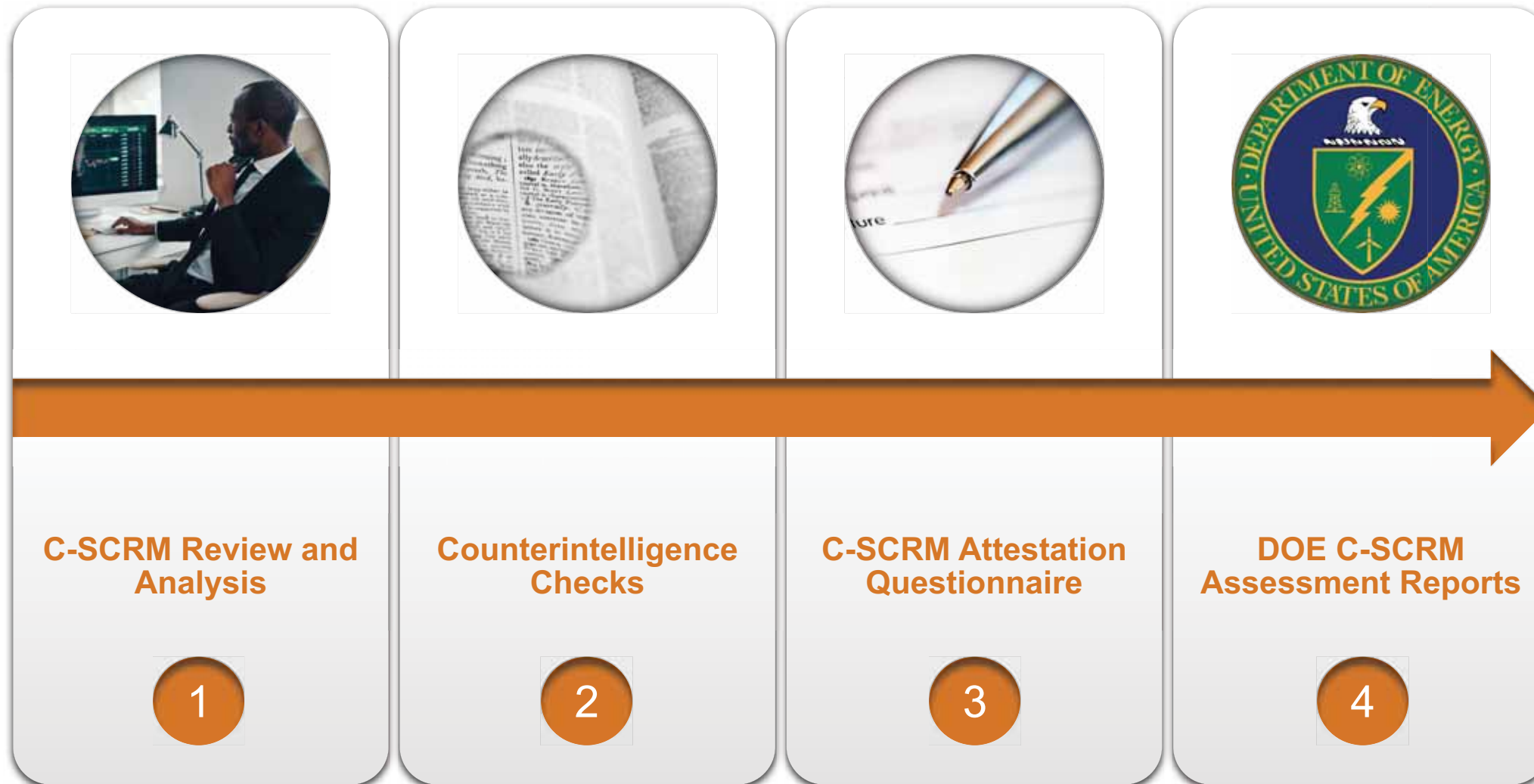


Counterintelligence Office

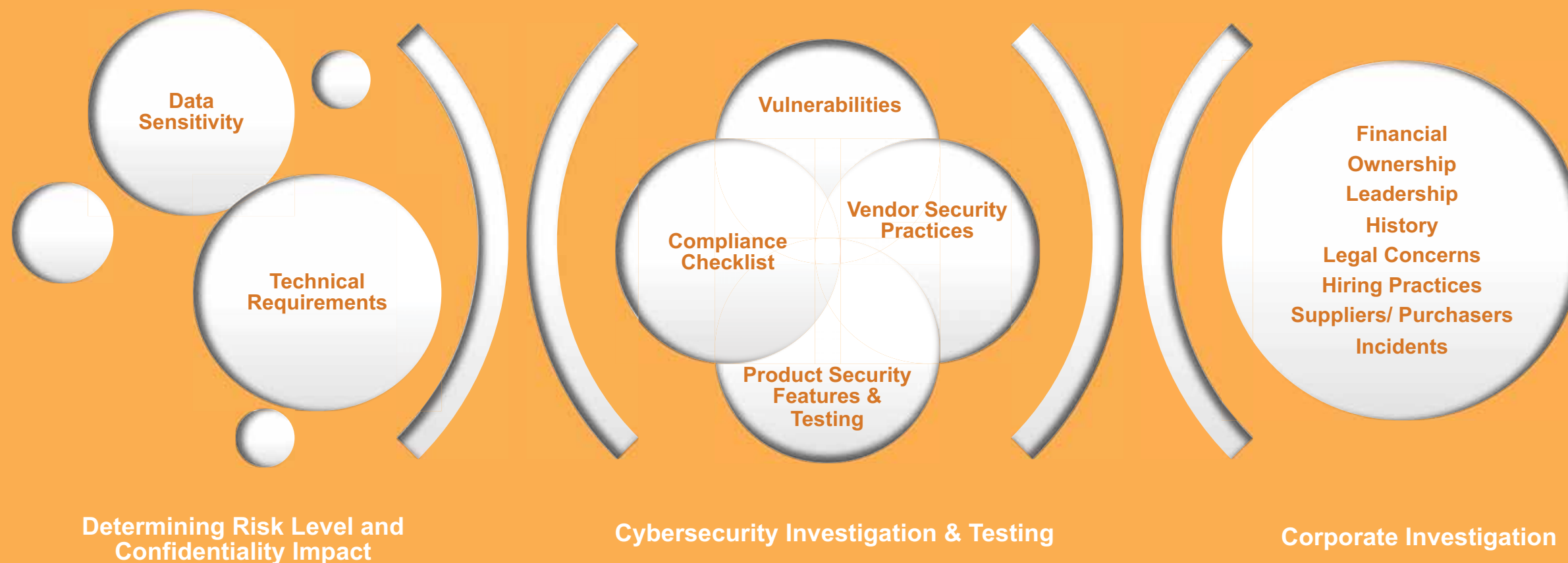


Utilize DOE OCIO C-SCRM Capabilities
(e.g., TPRM tool)

C-SCRM Analysis and Assessment



C-SCRM Initial Review and Analysis



Cyber Supply Chain Team (CSCT)

CSCT was developed to safeguard and enable resilient supply chain acquisitions for USSF and the greater DoD, supporting SSC program offices with analysis and assessments of companies and critical components within their supply chains.

Publicly Available Information (PAI) Research

- Conduct in-depth corporate research
- Analyze known concerns related to hardware and software, along with Subject Matter Expert (SME) insights

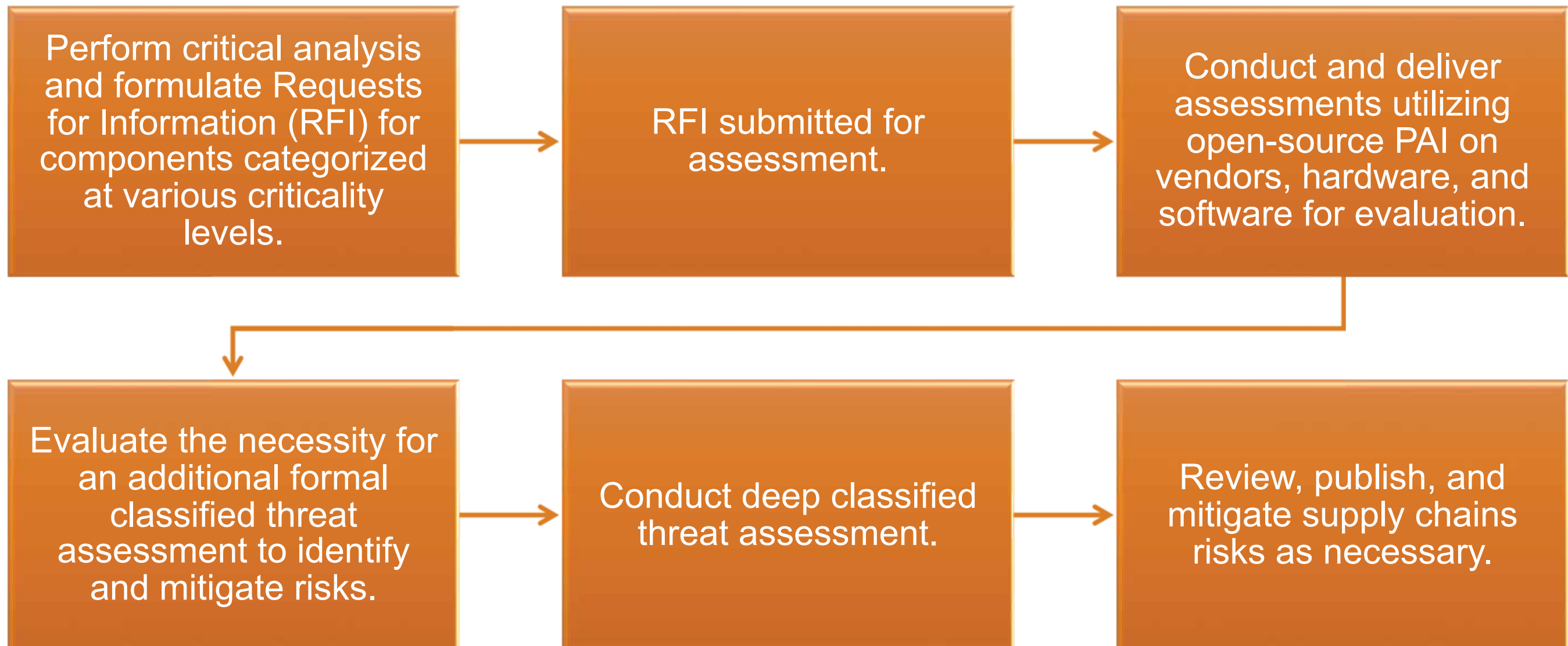
Hardware, Software, and System Deep Dive

- Perform comprehensive assessments for:
 - Counterfeit detection
 - Vulnerability identification and risk assessment
 - Other critical evaluations

Ensuring Trusted Component Acquisition

- Safeguard the integrity of corporate hardware, software, and systems through rigorous assurance processes

General SCRM Process



In Application

Corporate Research Process

- Focused on the potential risks posed by vendors.
- Conducted research across 11 risk categories.
- Reports include the following elements:
 - Analysis of domestic and foreign locations.
 - Examination of ownership and leadership structures.
 - Review of corporate history.
 - Assessment of financial history.
 - Identification of red flag areas highlighted by SMEs and partners.

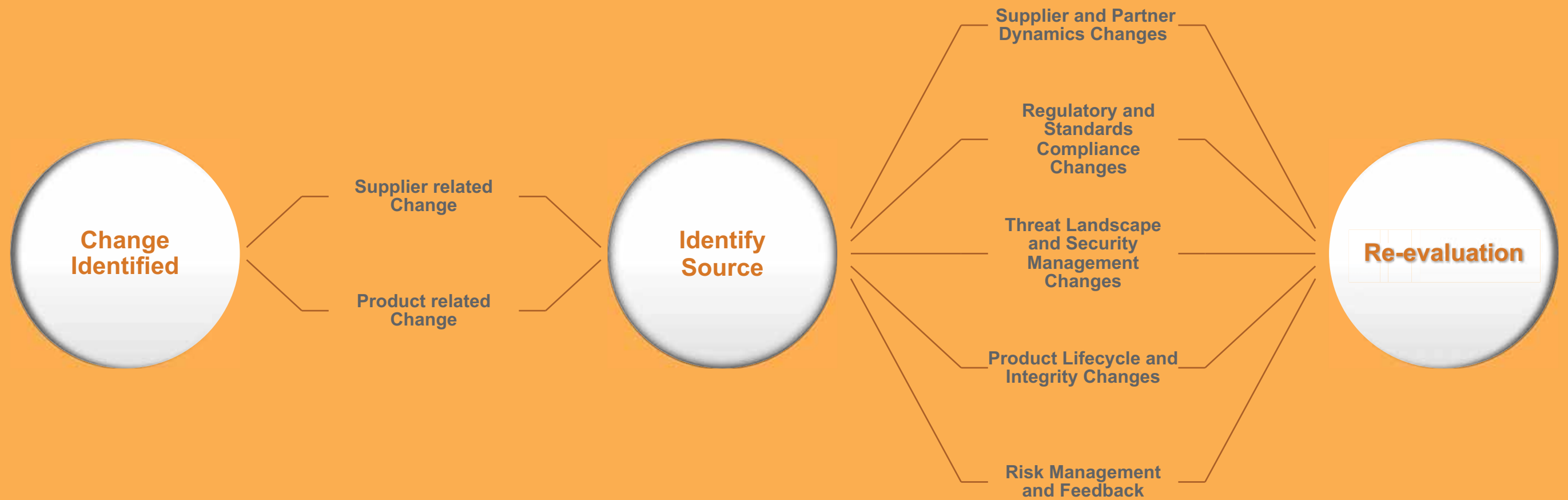
Hardware and Software Research Process

- Product description in layman's terms
- Identify known vulnerabilities
- Key features listed in a table
- Deep dive performed by SME on more complex parts

Risk Matrix Generation

- Key areas of potential risk
- Factors in reliability of sources
- An objective, standardized form to measure risk
- Industry best practices modified for mission specific needs

C-SCRM Re-evaluation & Re-assessment



Summary



Continued Efforts

-  Strengthen C-SCRM Initiatives
-  Incorporate New and Robust Capabilities
-  Leverage Supportive Tools
-  Adopt Advanced Technologies
-  Continue Collaboration Efforts



Points of Contact

PNNL Cyber Operations

- Faris Pirali

faris.pirali@pnnl.gov

PNNL Research, CSCT PAI Lead

- Arcky Vielma

arcadio.vielma@pnnl.gov

PNNL Research/Advisor, Liaison to USSF/SSC

- Ashlee Adamé

ashlee.adame@pnnl.gov

ashlee.adame.3.ctr@spaceforce.mil

Thank you

