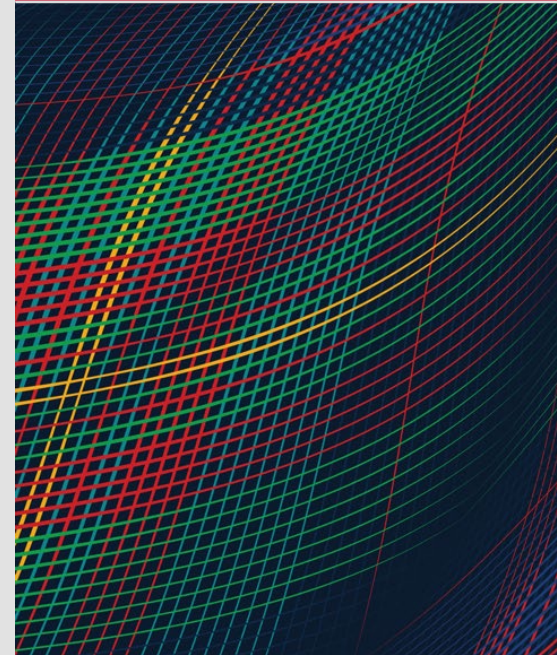


Meeting Challenges of Software Assurance and Supply Chain Risk Management

AUGUST 6, 2024

Carol Woody, PhD



Document Markings

Copyright 2024 Carnegie Mellon University.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

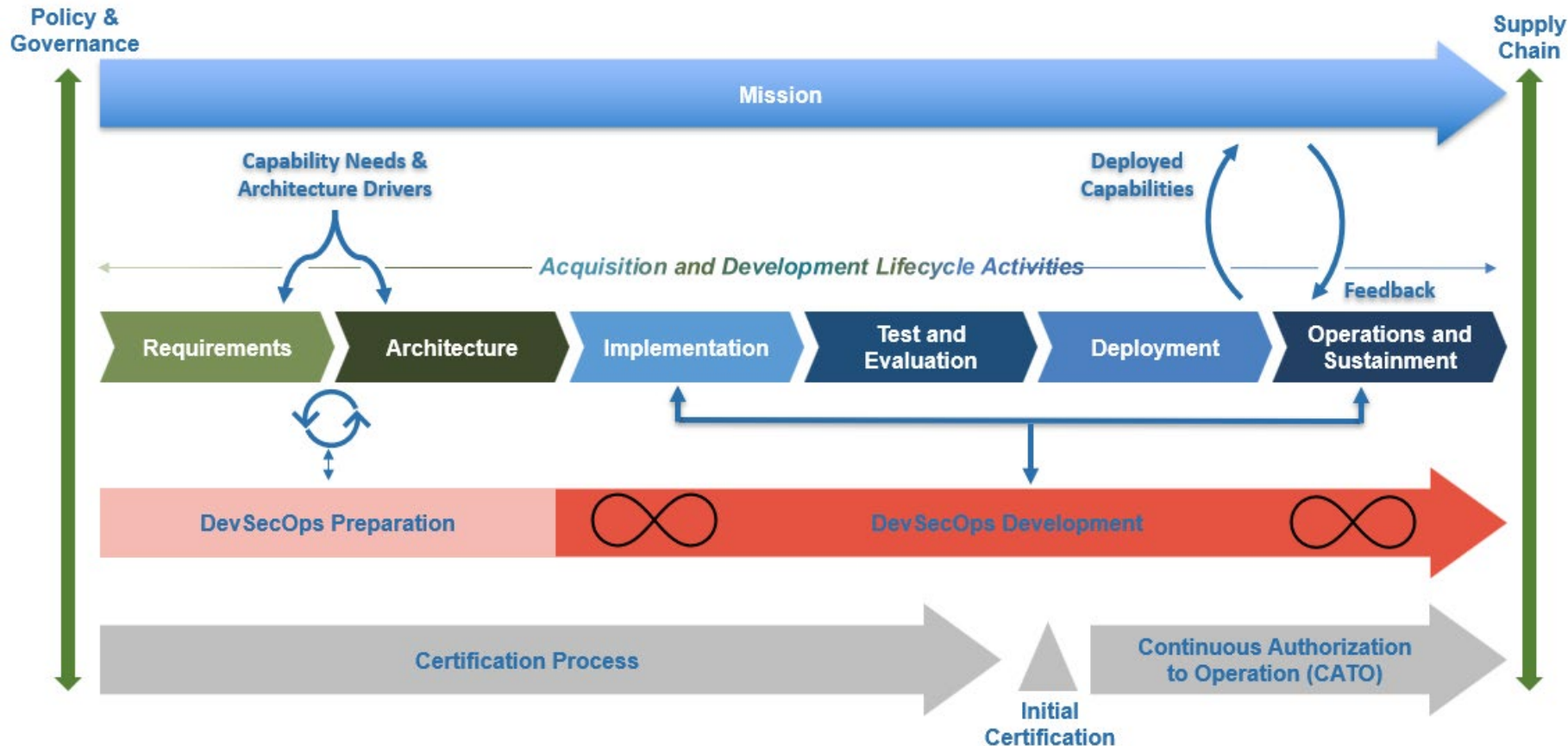
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

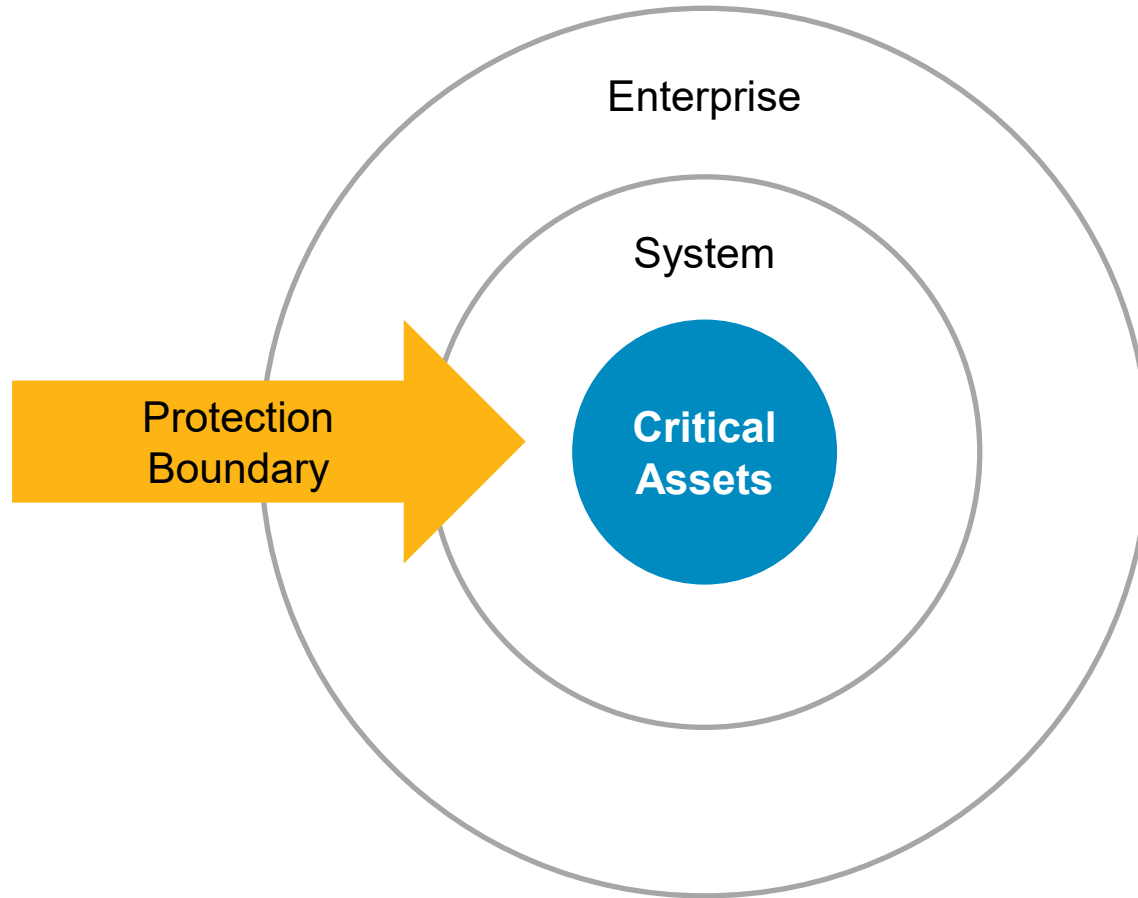
CERT® and Carnegie Mellon® are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM24-1000

Acquisition Landscape



Cybersecurity View



Risk Management Framework (RMF) and other compliance mandates focus attention on the system.

Controls are placed at the system level to protect critical assets.

Software that is not properly constrained can readily bypass these controls.

Software Attack Surface Extends Beyond the System

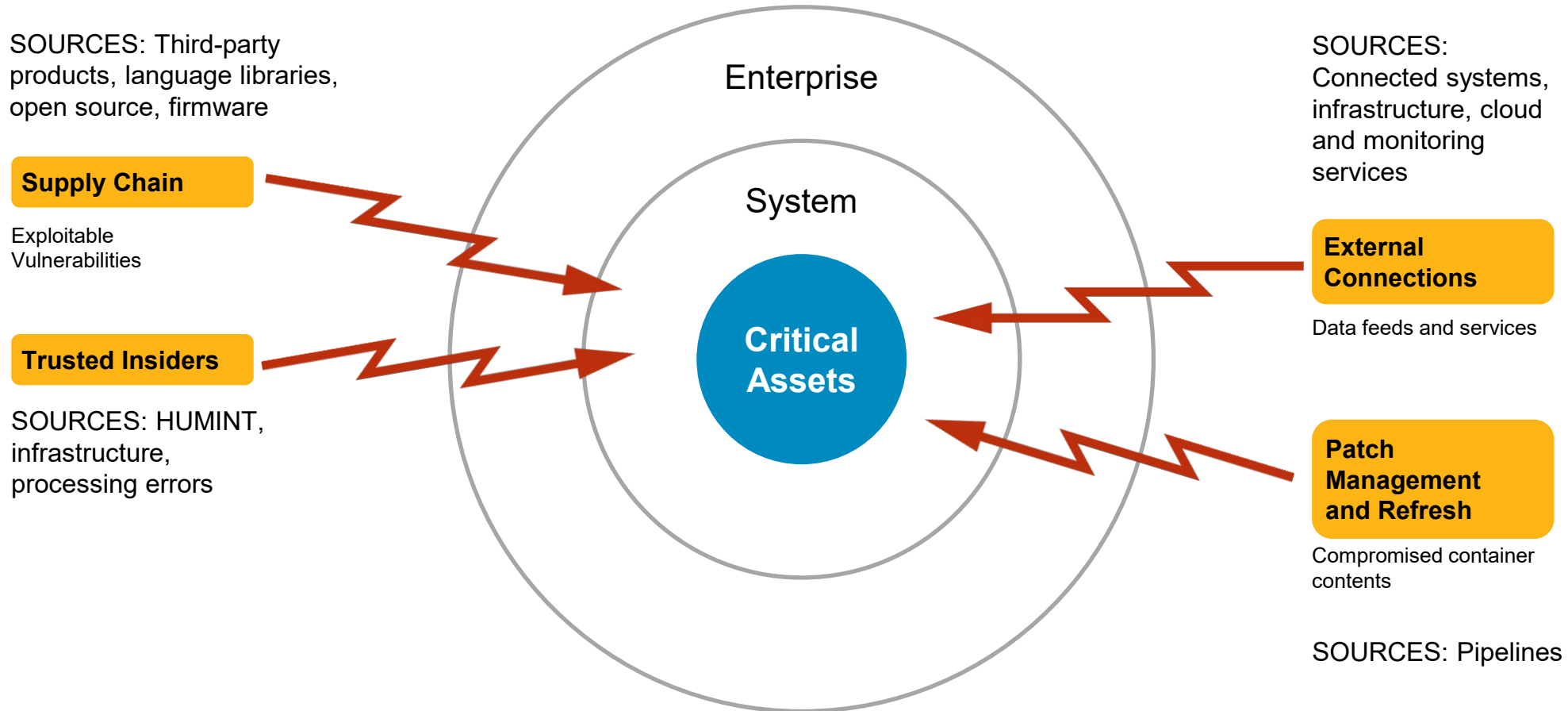
SOURCES: Third-party
products, language libraries,
open source, firmware

Supply Chain

Exploitable
Vulnerabilities

Trusted Insiders

SOURCES: HUMINT,
infrastructure,
processing errors



Supply Chain/Acquisition Risk Is Increasing



- Heartland Payment Systems (2009)
- Silverpop (2010)
- Epsilon (2011)
- New York State Electric and Gas (2012)
- Target (2013)
- Lowes (2014)
- AT&T (2014)
- HAVEX / Dragonfly attacks on energy industry (2014)
- DoD TRANSCOM contractor breaches (2014)
- Equifax (2017)
- Marriott (2018)
- SolarWinds (2020)
- Log4j (2021)
- Medibank (2022)
- MOVEit (2023)
- CrowdStrike (2024)

In more than 230,000 organizations, 98% have a relationship with a third party that has been breached within the last two years.

<https://www.securityweek.com/98-of-firms-have-a-supply-chain-relationship-that-has-been-breached-analysis/>

Key Software Assurance Acquisition Challenges

Third-party components are widespread throughout every system and require an integrated acquisition, engineering, development, and operational focus to ensure sufficient security and resilience.

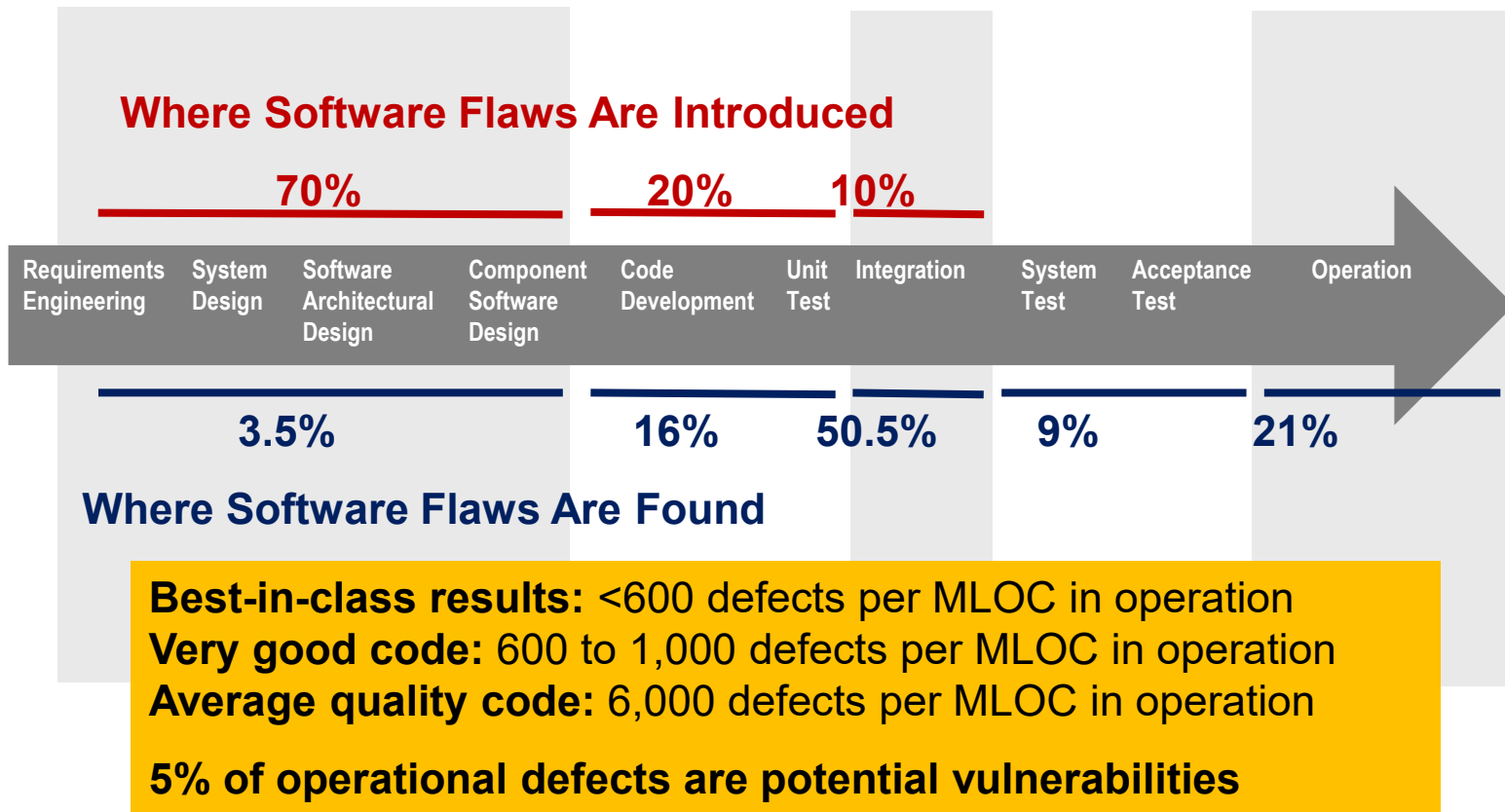
Many Software Development Plans (SDPs) only consider RMF, which does not address a major portion of the software-assurance attack surface.

Managing relationships with third parties is a critical success factor.

- A program can no longer effectively manage cyber risks alone.
- Supply chain risk management requires each supplier to manage its suppliers.
- Interactions with suppliers are increasingly data driven.

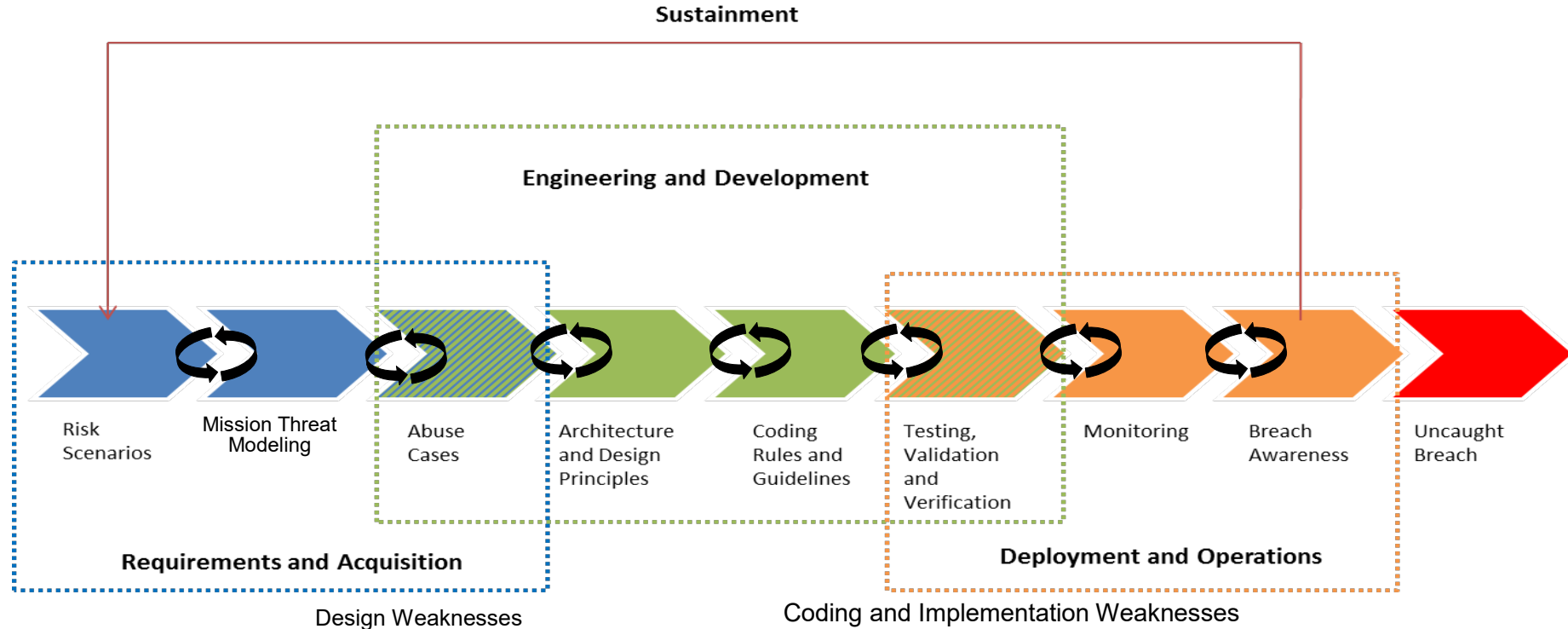
Identifying an attack requires monitoring for it with knowledge of system and software weaknesses and vulnerabilities and understanding of abnormal behavior.

Defect, Weakness, and Vulnerability Landscape



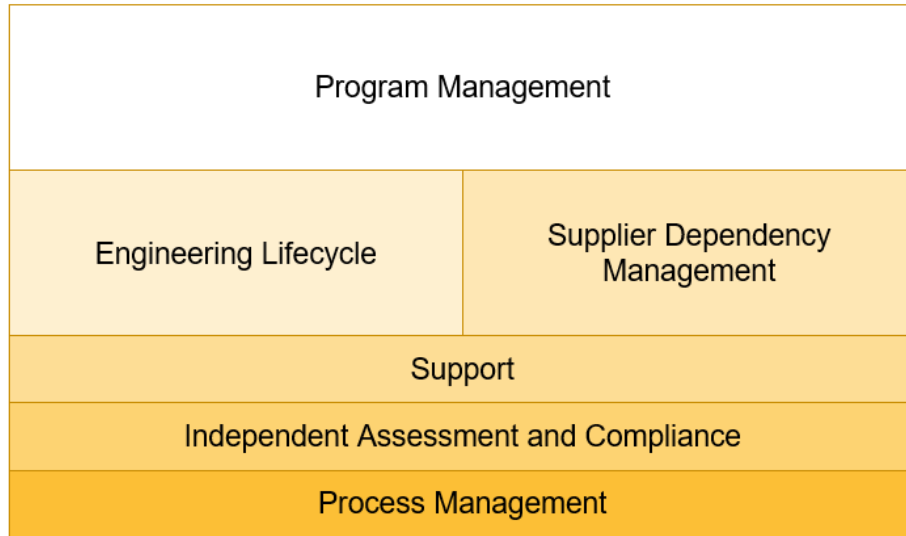
Sources: *Critical Code*; NIST, NASA, INCOSE, and Aircraft Industry Studies

Activities to Reduce Defects and Vulnerabilities



These activities are needed in every acquisition and every organization in the supply chain.

Acquisition Security Framework (ASF): Best Practices

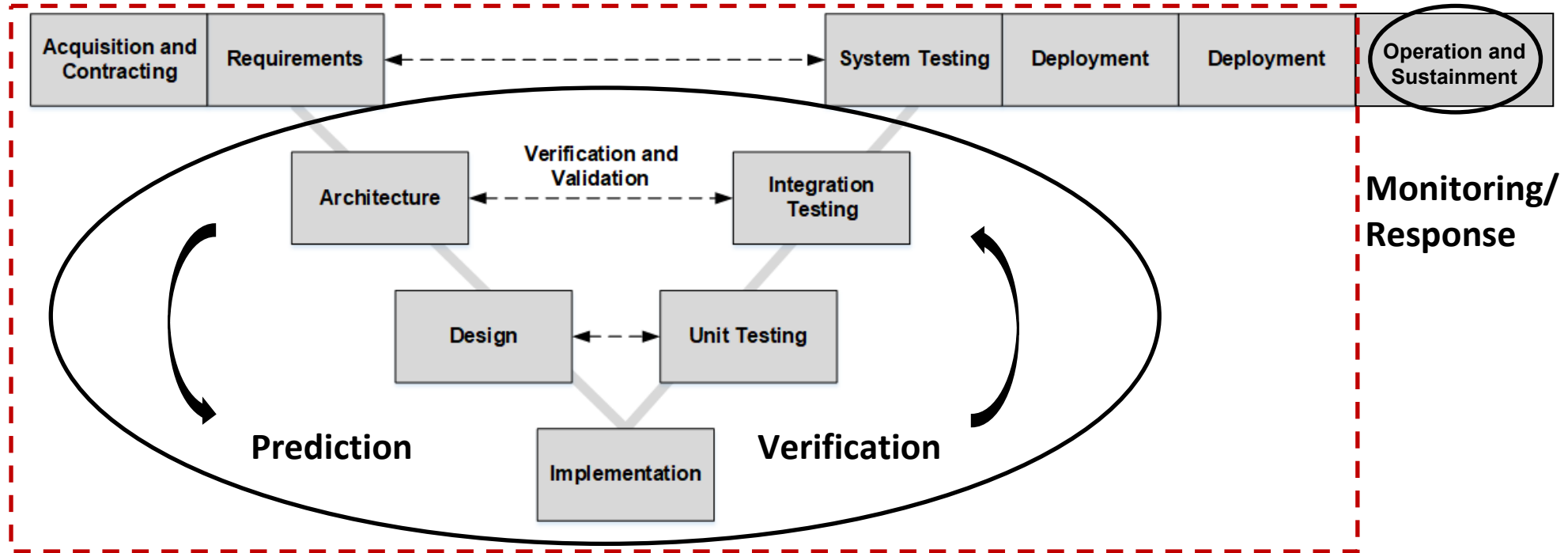


The ASF includes 51 goals and 334 practices spread across the following six practice areas:

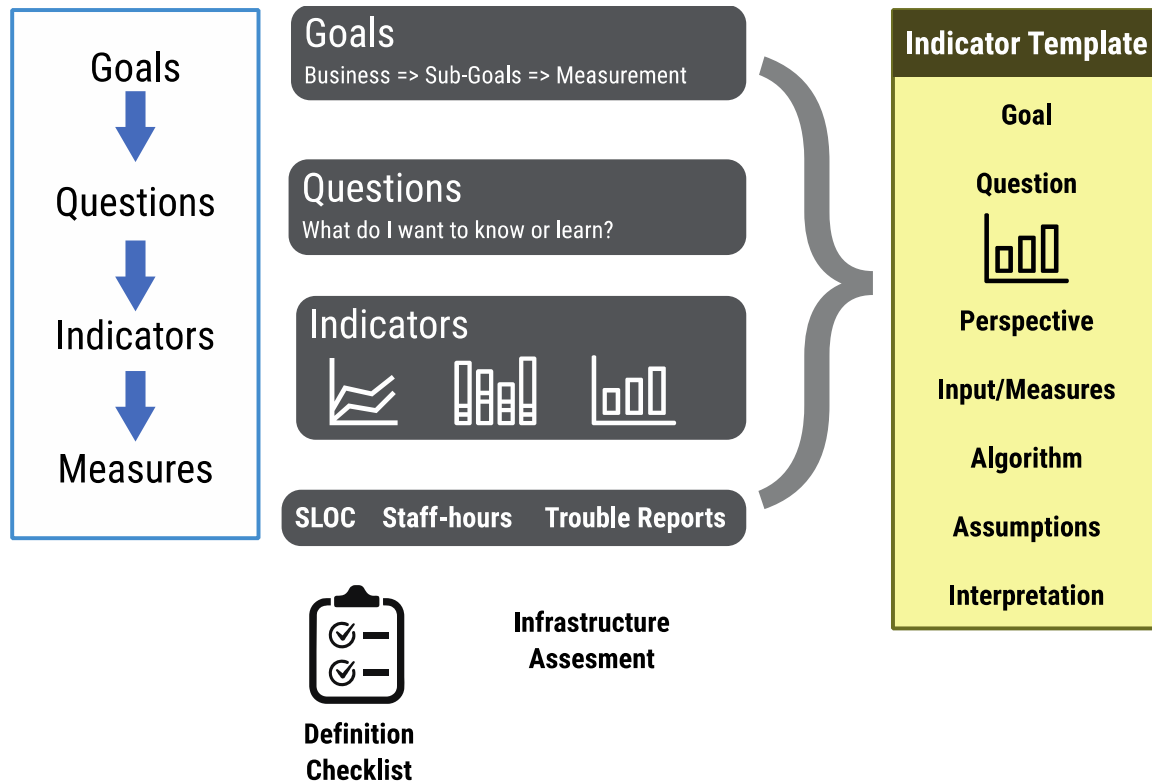
- Program Management
- Engineering Lifecycle
- Supplier Dependency Management
- Support
- Assessment and Compliance
- Process Management

Source: Alberts, C.; Bandor, M.; Wallen, C.; & Woody, C. *Acquisition Security Framework (ASF): Managing Systems Cybersecurity Risk (Expanded Set of Practices)*. CMU/SEI-2023-TN-004. Software Engineering Institute. 2023. <https://doi.org/10.1184/R1/24128475>

Software Assurance Across the Lifecycle

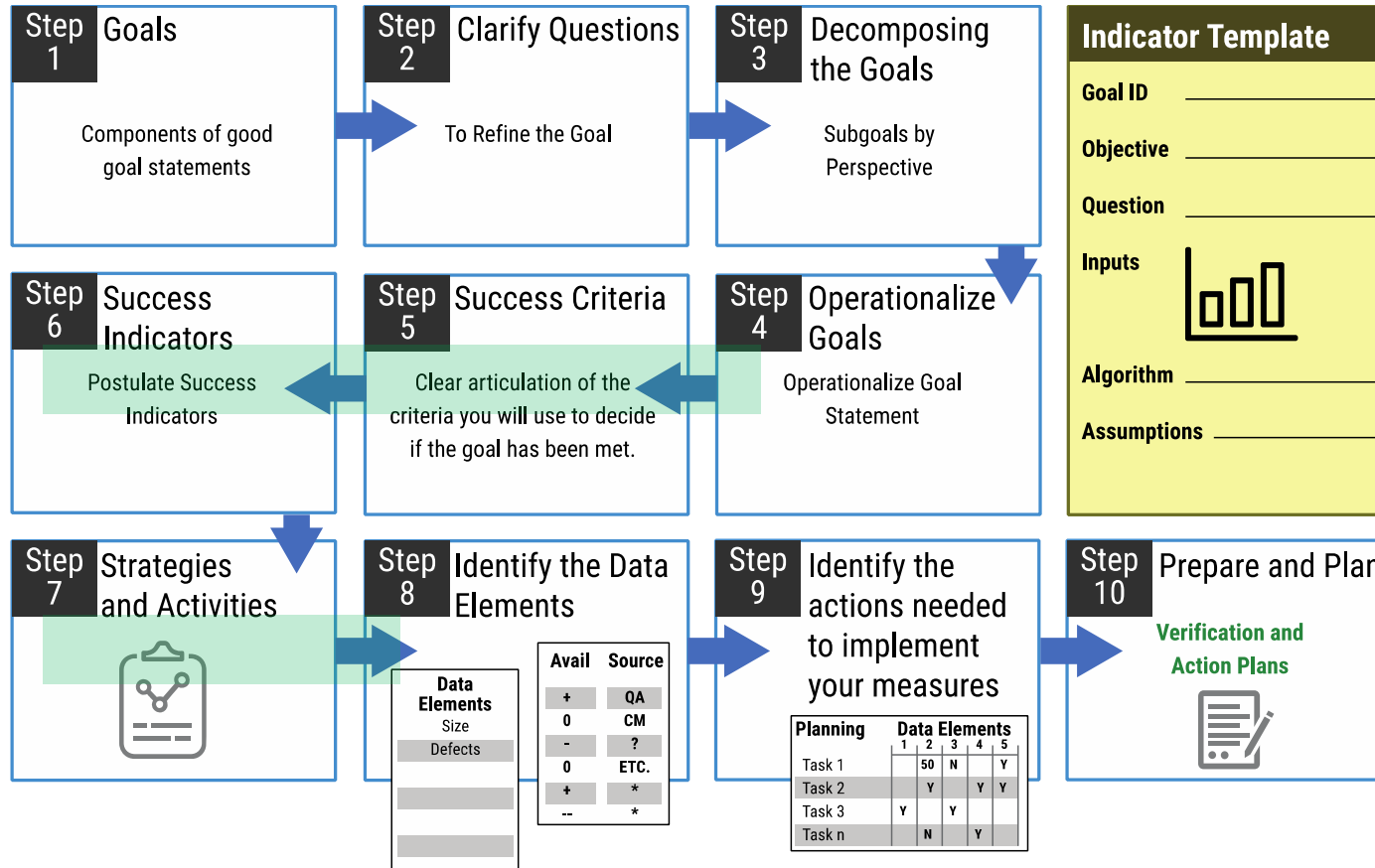


Goal-Driven Measurement Overview



Source: *Implementing Goal-Driven Measurement (IGDM) SEMA Course*. 2019. <https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=635664>

GQIM Workshop



Source: *Implementing Goal-Driven Measurement (IGDM) SEMA Course*. 2019. <https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=635664>

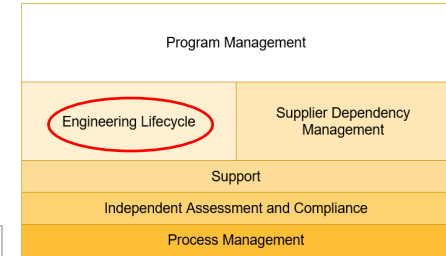
ASF Target Risk Area Example: Systems Engineering

Technical Activity Management

Goal 1—Engineering activities are planned and managed.

The purpose of this goal is to oversee the execution of engineering activities, including those performed by third-party contractors.

1. Is a plan for conducting the engineering activity developed and implemented?
2. Is progress against the plan tracked and reported?
3. Are criteria established for reviewing and accepting acquisition and engineering work products?
4. Are acquisition and engineering work products reviewed and accepted?
5. Are issues and risks that can affect engineering activities identified and resolved?
6. Are issues and risks that can affect engineering activities escalated to program management and other stakeholders as appropriate?



ASF practices are in the form of goals and questions to initiate the GQIM.

Software Security Requirements Metrics

Performance of the SwA activities can provide metrics; in some cases, these must be obtained from the vendor

Activities/Practices	Outputs	Candidate Metrics
Conduct security risk analysis (includes threat modeling and abuse/misuse cases).	<p>Prioritized list of software security risks</p> <p>Prioritized list of design weaknesses</p> <p>Prioritized list of controls/mitigations</p> <p>Mapping of controls/mitigations to design weaknesses</p>	<p>Number and % of software security risks controlled/mitigated (e.g., high and medium risks)</p> <p>Number and % of software security risks accepted/transferred</p> <p>Number and % of software security controls/mitigations selected for requirements development</p>

ASF Target Risk Area Example: System Supplier Oversight

Supplier Performance Management

Goal 2—Supplier performance is governed and managed.

The purpose of this goal is to assess whether performance is considered when evaluating suppliers that support the security/resilience of the program or system.

1. Is the performance of suppliers monitored against the security/resilience requirements of the program or system?
2. Is the responsibility for monitoring and managing the supplier established and maintained?
3. Are supplier performance issues documented and reported to the appropriate stakeholders?
4. Are corrective actions taken to address issues with supplier performance?
5. Are corrective actions evaluated to ensure issues are remedied?



How can the selected practice be applied to all suppliers (including open source)?

Managing Contractors and Suppliers: 4P Framework

Identified Criteria		Project	Product	Protection	Policy
	Long-Term Support	Forked Project			No Security Policy
	Dependencies	74 Abandoned Dependencies	No Update Tools		
	Security		4 Unfixed Critical Vulnerabilities	Workflow with Excessive Permissions	
	Integrity		No Fuzz Testing	30 Unreviewed Change Sets	
	Malicious Actors	Commit ID Known Malicious			
	Suitability				12 Restrictive Licenses

Red Flag

Realm of Observable Facts of OSS Projects and Products

- Review data available
- Identify useful criteria
- Extract key data
- Map to acceptable criteria
- Evaluate red flags
- Identify appropriate mitigations
- Confirm supportability

Measure and baseline what you have, especially open source.

Assess how you are vulnerable and identify an improvement path.

Integrate measurement and monitoring throughout the lifecycle.

References - 1

[Acquisition Security Framework \(ASF\) Collection](#)

Woody, Carol; Ellison, Robert; & Ryan, Charles. *Exploring the Use of Metrics for Software Assurance*. CMU/SEI-2018-TN-004. Software Engineering Institute. 2019.

<https://insights.sei.cmu.edu/library/exploring-the-use-of-metrics-for-software-assurance/>

Mead, Nancy; Woody, Carol; & Hissam, Scott. Open Source Software (OSS) Transparency for DoD Acquisition. In *Proceedings of the 21st Annual Acquisition Research Symposium*. Naval Post-graduate School, Monterey, CA. May 8-9 2024.

<https://arxiv.org/abs/2404.16737>

References - 2

Goethert, W. B. & Siviyy, J. *Applications of the Indicator Template for Measurement and Analysis*. CMU/SEI-2004-TN-024. Software Engineering Institute. 2004.

<https://insights.sei.cmu.edu/library/applications-of-the-indicator-template-for-measurement-and-analysis/>

Public course

Implementing Goal-Driven Measurement (IGDM) SEMA Course. 2019.

<https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=635664>

Contact Information



Carol Woody, PhD
cwoody@cert.org

Web Resources
<https://sei.cmu.edu/>