Acquisition Security Framework (ASF): Overview

Dr. Carol Woody
Christopher Alberts
Charles Wallen
Mike Bandor

May 5, 2021

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Document Markings

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM21-0435

Software Engineering Institute (SEI) Project Team

Dr. Carol Woody
Principal Researcher
Project Lead

Cybersecurity engineering, system modeling, project management

Christopher Alberts
Principal Cybersecurity Analyst

Cybersecurity engineering, security risk management, threat modeling

Mike Bandor
Senior Software Engineer

Agile software development, process improvement, DoD acquisition

Charles Wallen
Information and Infrastructure Security Analyst

Resilience management, critical infrastructure protection, supply chain risk management

Acquisition Security Framework (ASF) Task: Goals

Integrate software security engineering practices into the acquisition lifecycle

- Expand Acquisition Security Framework (ASF) Version 1.0 based on lessons learned from successful supply chain attacks (e.g., the SolarWinds attack)
- Incorporate DevSecOps concepts and principles into ASF V2.0
- Adapt system and software engineering measurement activities to include security where appropriate

Acquisition Security Framework (ASF) Task: Related SEI Research and Development

Supply chain responsibility analysis for Air Force decision approving authority to define government responsibility for security risk management

DHS critical infrastructure security process assessments (including questionnaires and analysis tools)

Cybersecurity engineering assessments for evaluating security engineering technologies and practices across the lifecycle and supply chain

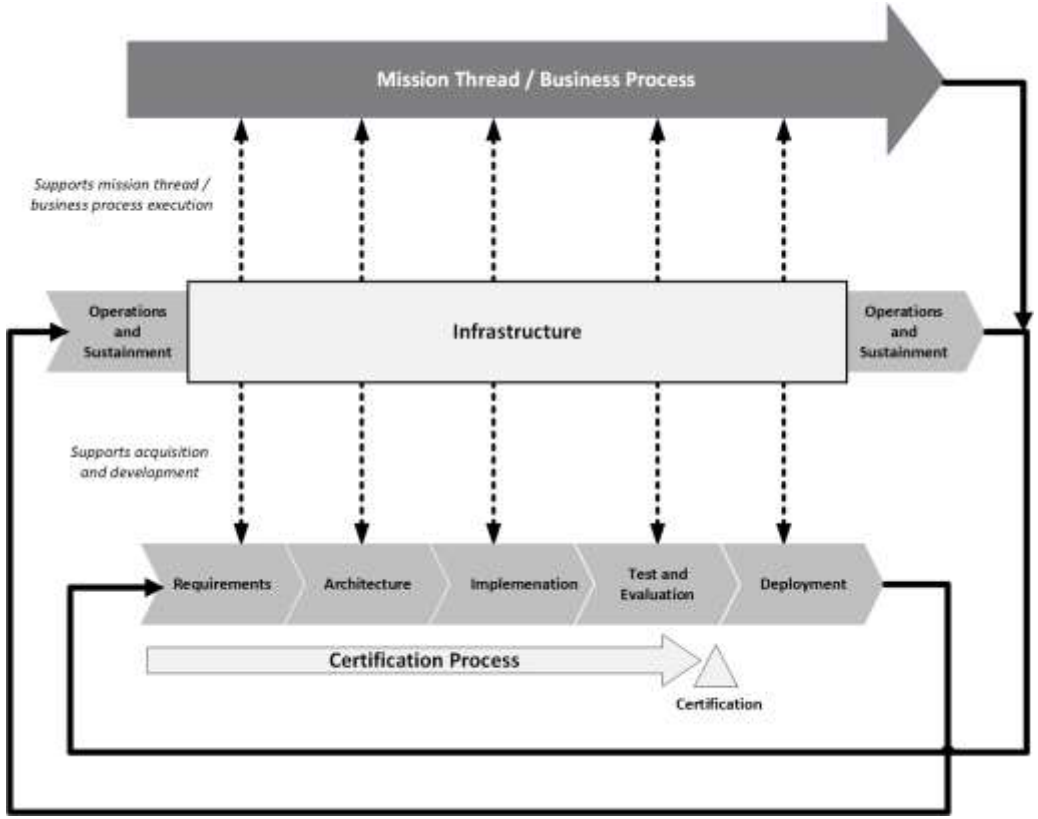
Supply Chain: Example Incidents

- Heartland Payment Systems (2009)
- Silverpop (2010)
- Epsilon (2011)
- New York State Electric and Gas (2012)
- California Department of Child Support Services (2012)
- Thrift Savings Plan (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)

Case Study: SolarWinds

[Supply Chain Compromise | CISA]

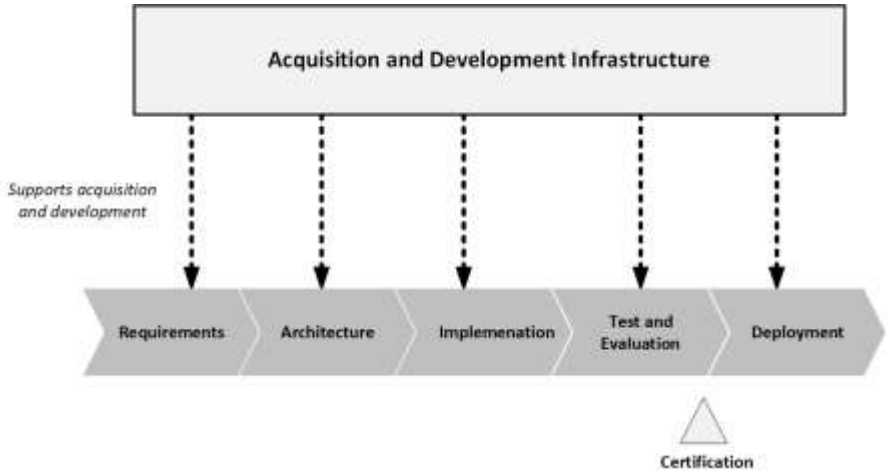
Problem Space: Lifecycle Model



Acquisition and Development Perspective

Acquisition and development personnel focus on building security controls into the cyber-physical system.

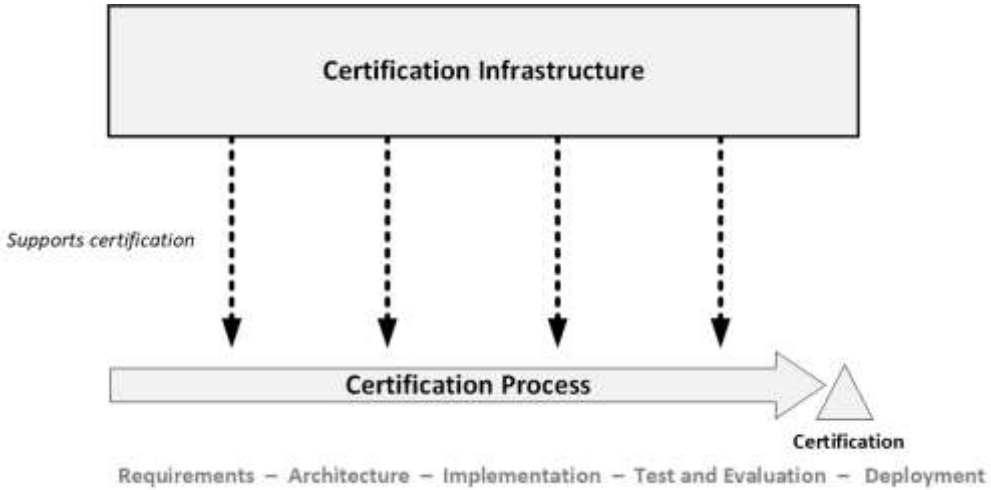
They use the acquisition and development infrastructure to support their activities.



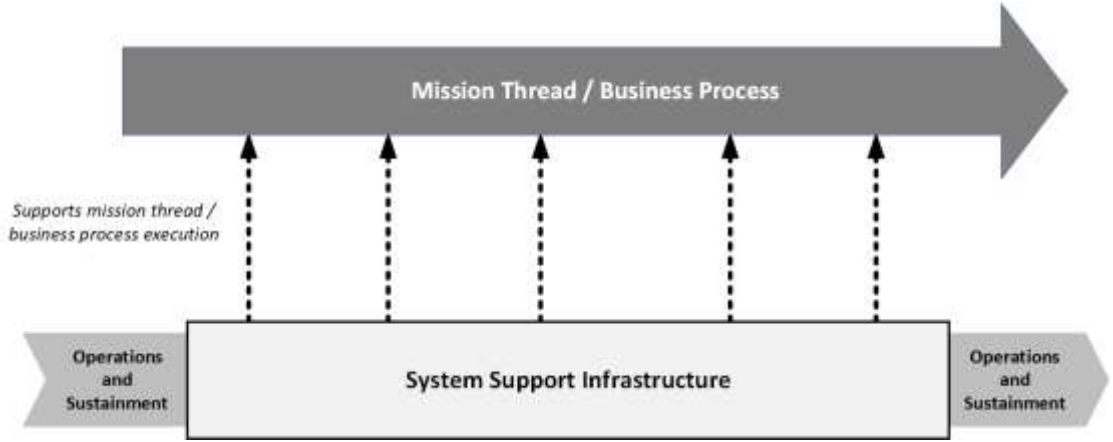
Certification Perspective

Certification groups (e.g., nuclear surety, cybersecurity) are focused on system certification and accreditation activities.

They use the certification infrastructure to support their activities.



Operations and Sustainment Perspective



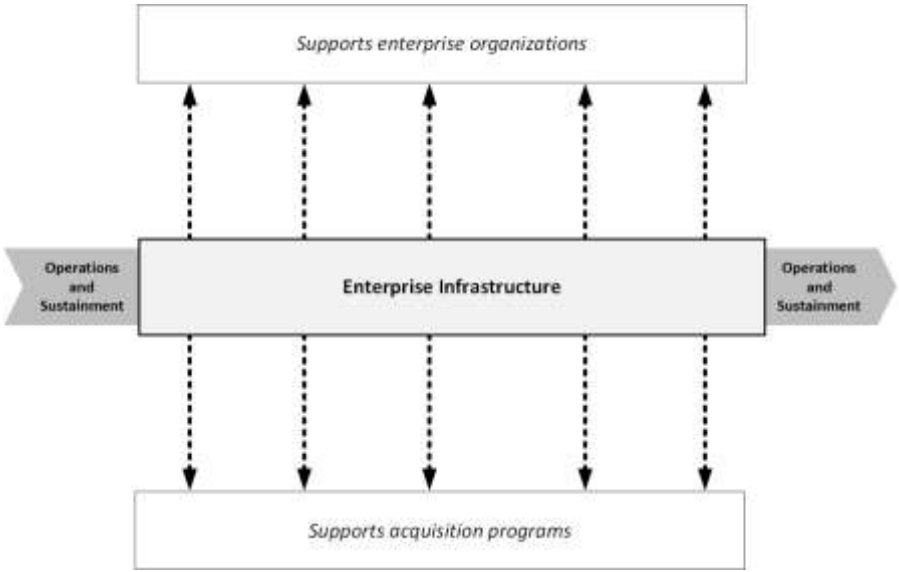
The Operations and Sustainment group is focused on maintaining the operational security of the deployed cyber-physical system.

They use the system support infrastructure to support their activities.

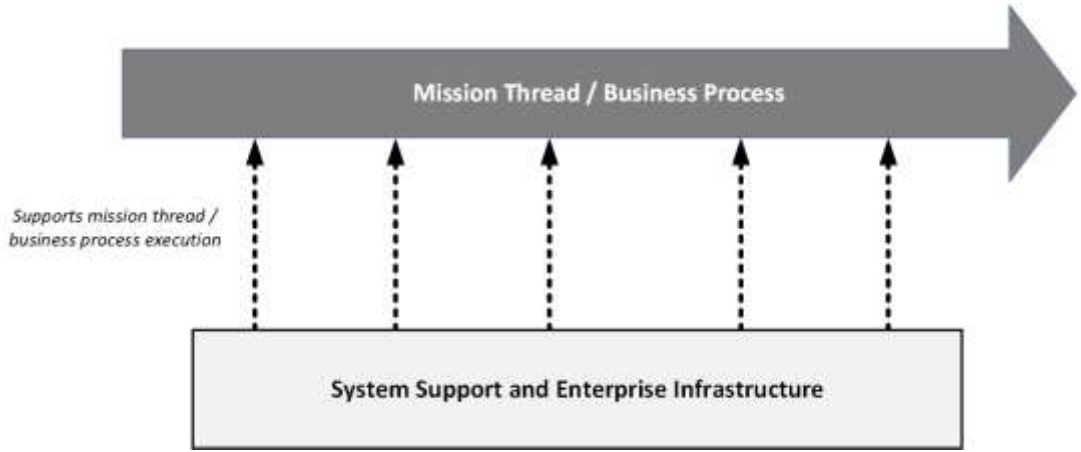
Enterprise Infrastructure Perspective

The enterprise infrastructure group is focused on maintaining the operational security of systems and networks, including

- Acquisition and development systems
- Certification systems
- Business systems
- Logistics systems
- Planning systems
- Financial systems
- Other systems



Mission Perspective



The mission team is focused on executing the mission thread / business process successfully.

The team uses system support and enterprise infrastructure to support their activities.

Complexity: Aligning and Managing Security Objectives Across the Supply Chain

Mission View

- Focus: Assuring mission success

Infrastructure View

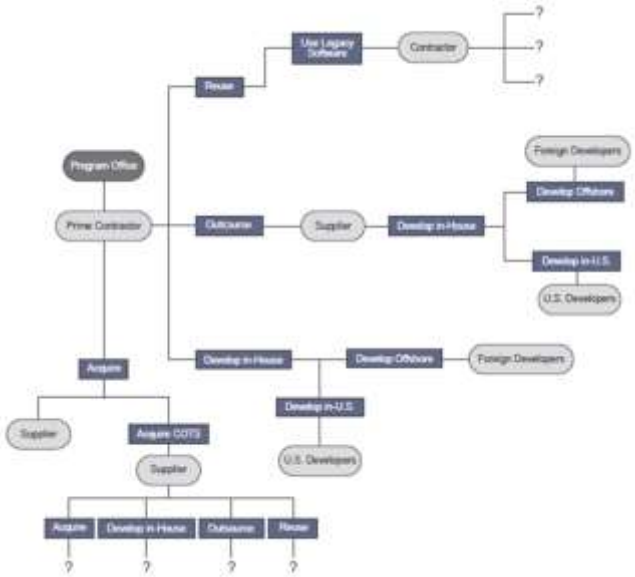
- Focus: Protection and sustainment of the infrastructure

Acquisition and Development View

- Focus: Build security into systems

Certification View

- Focus: Certify systems for deployment



Each organization/program unit addresses security from a different perspective (e.g., mission, infrastructure, acquisition and development).

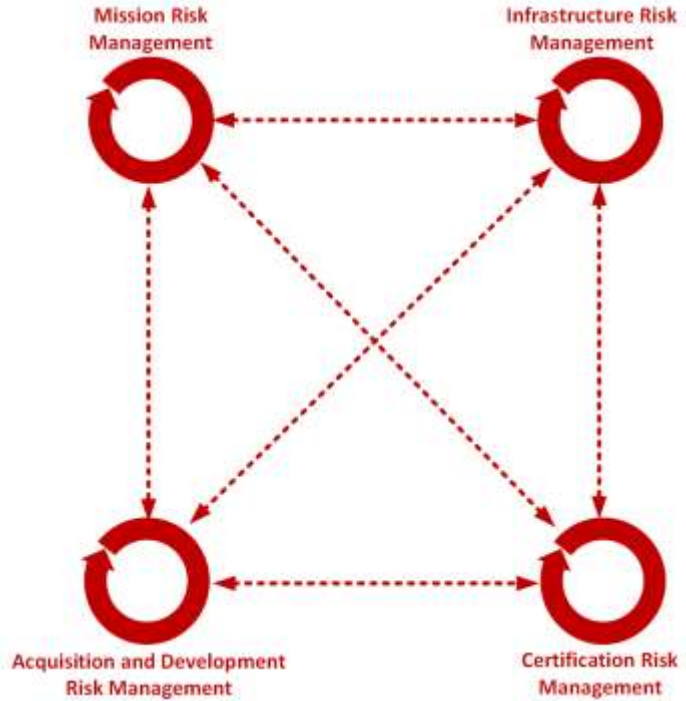
Security objectives across organizations/program units need to be aligned and managed.

Complexity: Managing Security Risk Across Organizations -1

Security risk is managed by multiple organizations/program units.

Security risk management activities must be aligned to keep overall security risk within an acceptable tolerance.

- Acquisition and development risk
- Certification risk
- Mission risk
- Infrastructure risk



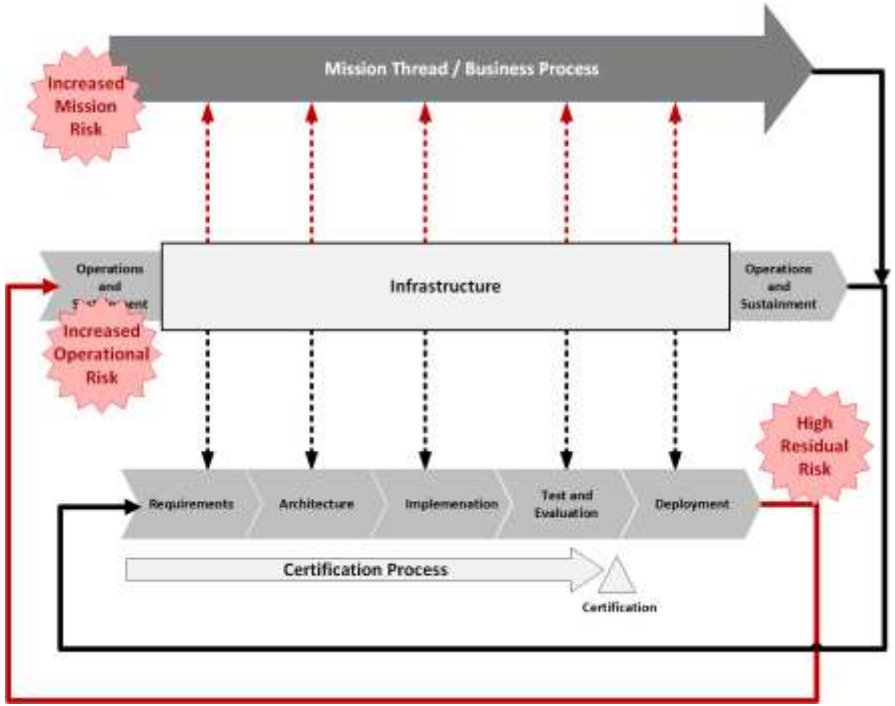
Complexity: Managing Security Risk Across Organizations -2

Ineffective/uncoordinated security engineering processes lead to deployed systems with high residual risk.

High residual risk increases

- Operational risk
- Increased mission risk

Some security risks are difficult to mitigate after deployment (e.g., architectural security risks).



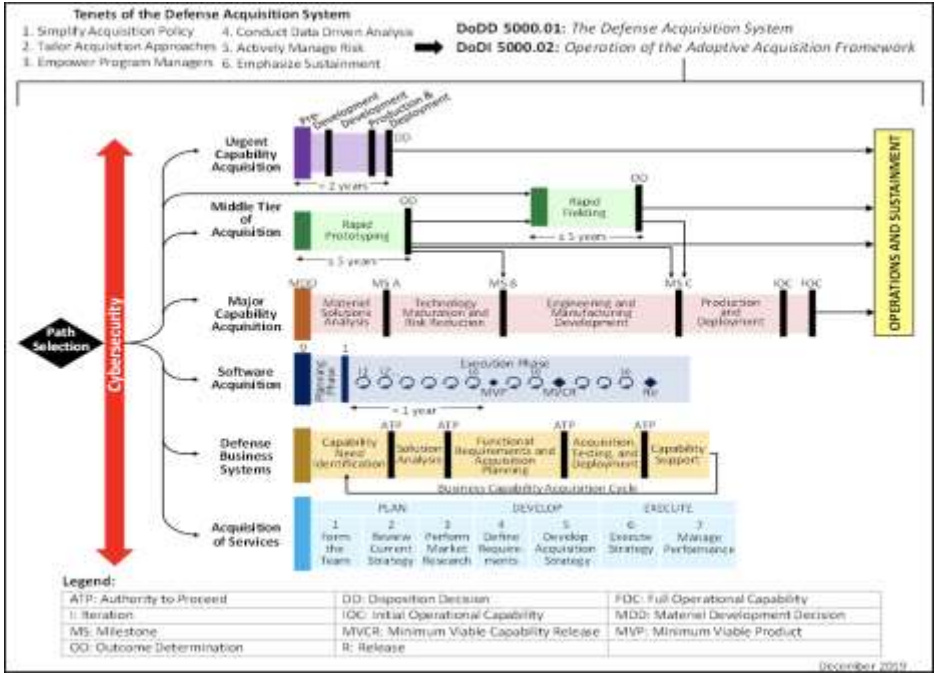
Complexity: Integrating Security into Acquisition and Engineering

Security practices (management and technical) need to be integrated into a program's existing acquisition and engineering practices.

Security practices and processes (management and technical) need to scale to multiple types of acquisitions, including

- Major capability acquisition
- Software acquisition
- Defense business systems
- Acquisition of services

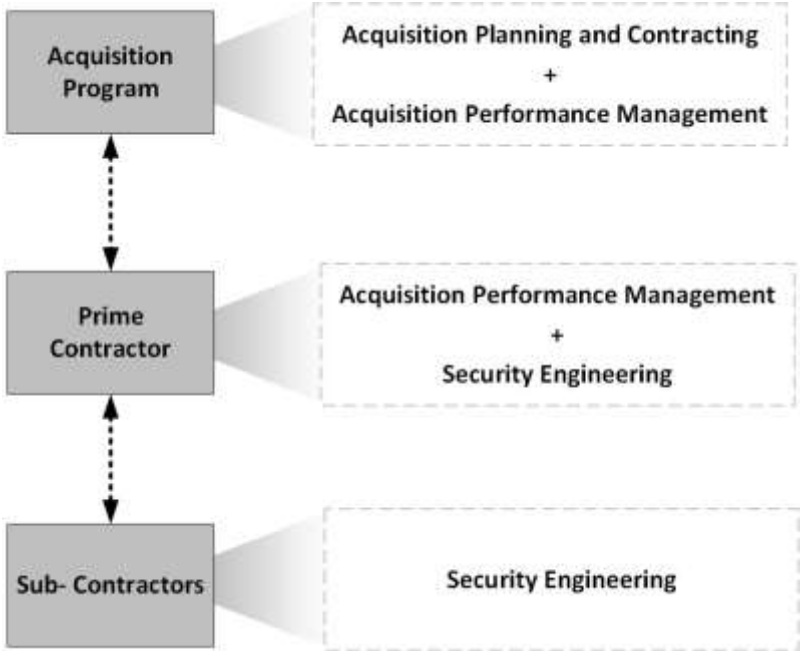
Security practices and processes must scale to specific development approaches, such as DevSecOps.



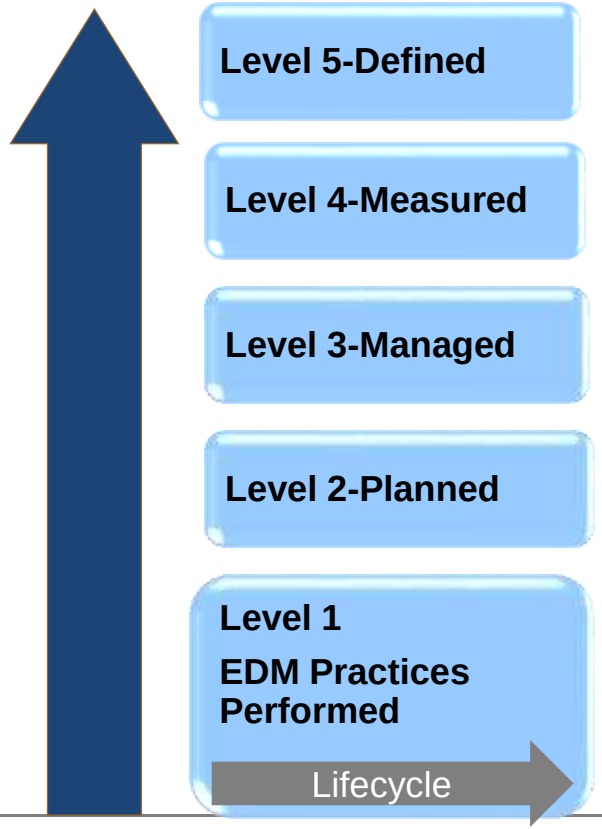
Complexity: Aligning Security Practices Across Organizations

Each participating organization/program unit is responsible for some aspect of security management.

Security practices across these groups must be aligned to ensure that security is managed effectively.



Complexity: Managing Process Maturity



Higher degrees of process management translate to more stable environments that

- Produce consistent results over time
- Are able to achieve their missions during times of stress

Each organization/program unit must manage the maturity of its security practices.

Security practices do not need to be at a uniform level of maturity to be sufficient.

Barriers to Effective Management

Complexity

Siloed departments operating under different requirements

- Procurement/acquisitions
- Operations
- Incident management

Vagueness or limitations in formal agreements

Changing requirements across system lifecycles

Incomplete or narrow risk management processes

Acquisition Security Framework (ASF)

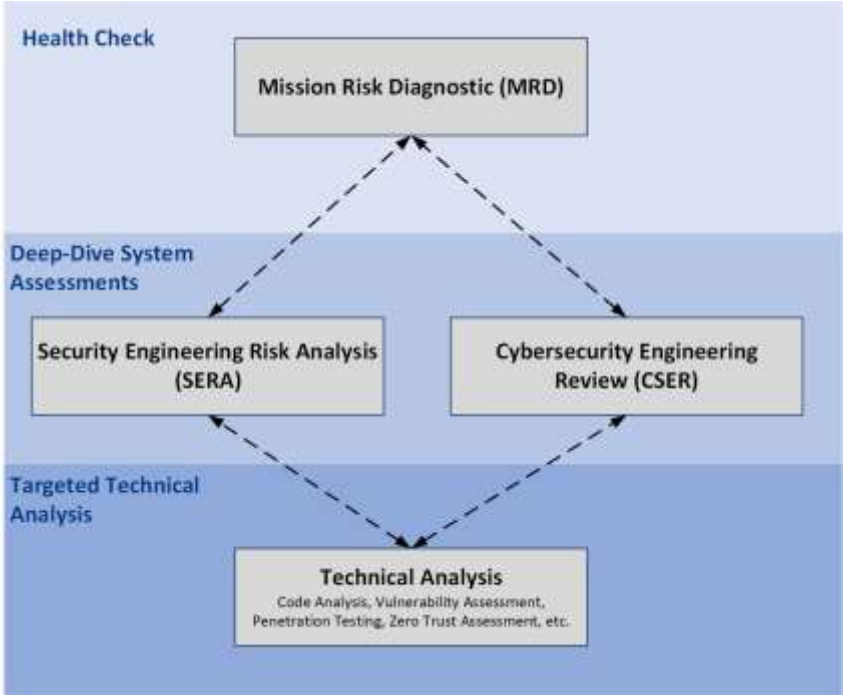
The ASF comprises practices in the following areas for managing software supply chain risk across acquisition programs:

- Mission Assurance
- System Acquisition and Development
- Certification and Accreditation
- Infrastructure Protection and Sustainment
- Process Maturity

Cybersecurity Engineering Assessments -1

ASF provides an integrated approach for assessing and managing security across the system lifecycle and supply chain.

- Health check
- Deep-dive system assessments
- Targeted technical analysis



Cybersecurity Engineering Assessments -2

Mission Risk Diagnostic (MRD)

Assesses a mission's current potential for success in relation to a set of known risk factors

Pilots

- DoD weapon system acquisition
- Civil agency system acquisition and operation
- Software security
- Software supply chain
- Cloud technology adoption
- Custom risk assessments

Security Engineering Risk Analysis (SERA)

Analyzes security risks in software-reliant systems and systems of systems across the lifecycle and supply chain

Pilots

- DoD weapon system acquisition
- Foreign Military Sales (FMS)
- Civil agency system acquisition and operation

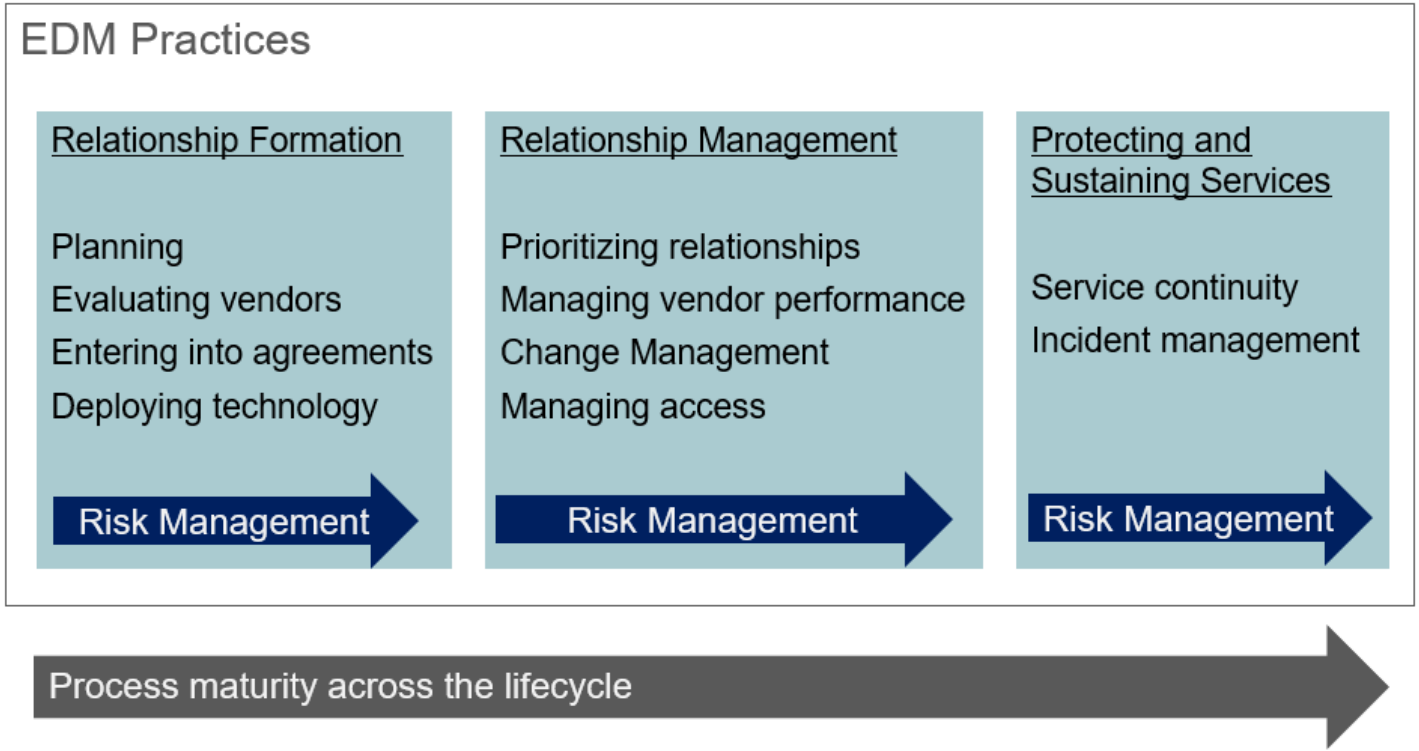
Cybersecurity Engineering Review (CSER)

Evaluates an acquisition program's security practices for conformance to accepted security engineering practices

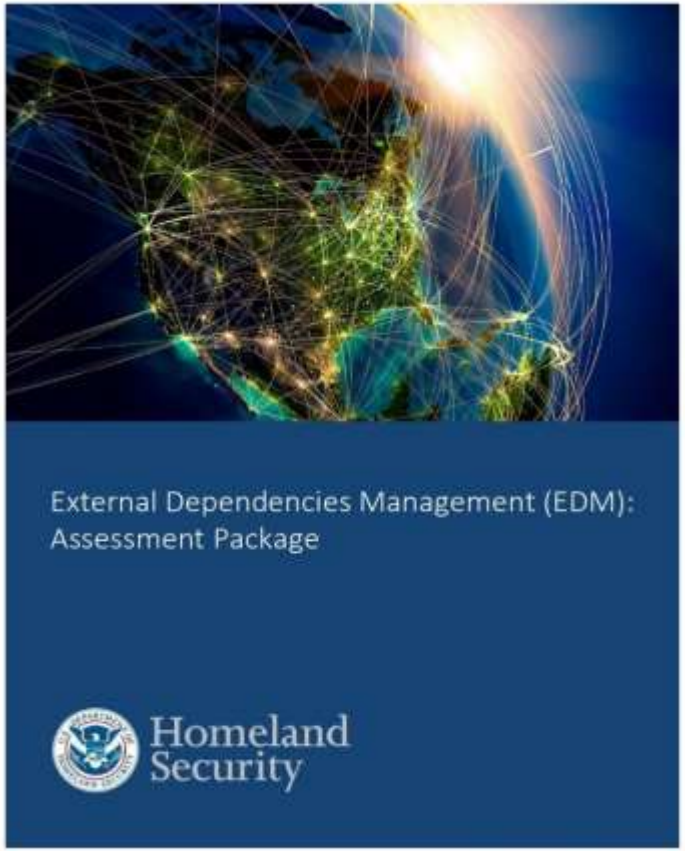
Pilots

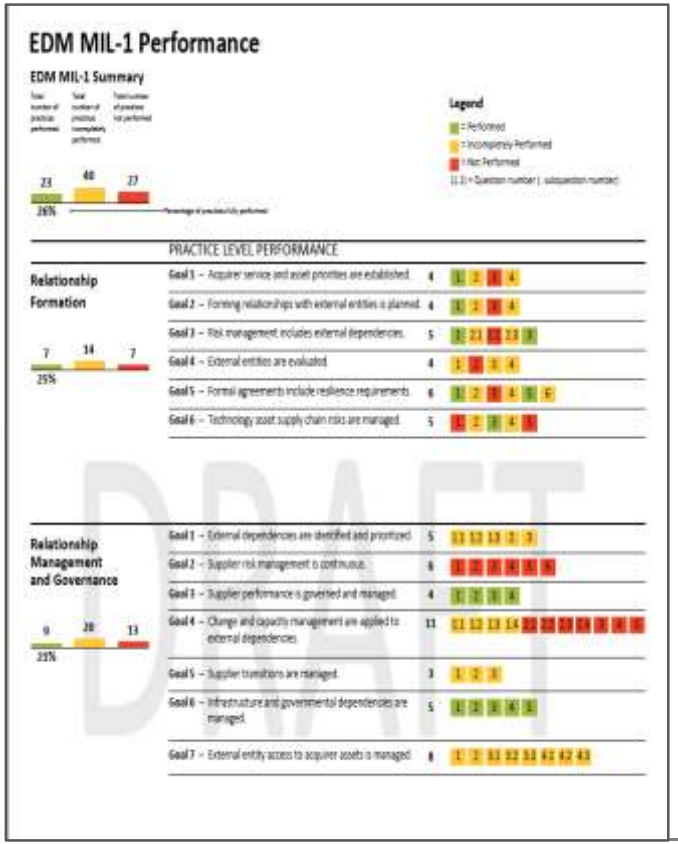
- Foreign Military Sales (FMS)
- Civil agency system acquisition

External Dependencies Management (EDM): A Unified, Resilience-based Approach



EDM: Utilized by DHS to Support Efforts to Protect Critical Infrastructure





Who Participates?

Chemical
Commercial Facilities
Communications
Critical Manufacturing
Dams
Defense Industrial Base
Emergency Services
Energy
Financial Services
Food and Agriculture
Government Facilities
Health Care and Public Health
Information Technology
Nuclear Reactors, Materials, & Waste
Transportation Systems
Water and Wastewater Systems

Critical Infrastructure and Key Resources (CIKR) sectors and State, Local, Tribal, and Territorial (SLTT) Governments within the United States (and its territories) participate.

Participation is voluntary.

Proposed Milestone Schedule

Task Name	Start	Finish
Prepare introduction briefing and overview	3/01/2021	4/28/2021
Kickoff meeting with Stakeholders	**5/7/2021**	**5/7/2021**
Develop draft Acquisition Security Framework (ASF)	4/6/2021	7/15/2021
Initial development	**4/6/2021**	**5/14/2021**
SEI internal subject matter expert (SME) review	5/17/2021	5/28/2021
Finalize initial draft with SME feedback	5/28/2021	7/15/2021
Deliver initial draft for stakeholder review (workshops)	7/15/2021	7/15/2021
Develop revised draft with stakeholder feedback	7/01/2021	8/30/2021
Complete Draft Final ASF and draft a plan for program use	8/30/2021	8/30/2021
Editing and SEI Reviews	8/31/2021	9/30/2021
Deliver Integration Plan and draft plan for program use	9/30/2021	9/30/2021

Deliverables

1. Draft Acquisition Security Framework (ASF)
2. ASF workshops
3. Plan for program implementation of ASF

In Closing . . .

Supply chain risk management is a lifecycle challenge (acquisition, engineering, and operation).

Decisions made during system acquisition and engineering will either mitigate or amplify operational and mission risks.

New approaches are needed to manage cybersecurity risks collaboratively with third-party suppliers.

Managing relationships with third parties is a critical success factor—a program cannot effectively manage cybersecurity risks by itself.

Effective process management translates to more stable environments that

- Produce consistent results over time
- Are able to achieve their missions during times of stress