Cybersecurity Engineering Review (CSER)

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.

DM21-0074

BLUF

SEI is conducting a Cybersecurity Engineering Review (CSER) of the Spectrum Management Coordination System (SMCS).

- SEI is evaluating SMCS cybersecurity engineering (CSE) practices for conformance to accepted CSE practices
  - Establish the current state of CSE practices for SMCS
  - Identify gaps in relation to accepted CSE practices
  - Provide recommendations for improving a SMCS CSE practices

This presentation is the initial activity for the SMCS CSER.

- Provide an overview of the CSER Method
- Set the scope of the SMCS CSER

SEI's research goals are to

- Collect lessons learned from the SMCS pilot
- Improve the CSER Method

Topics

Introduction

Cybersecurity Engineering Review (CSER) Overview

Preparing for the CSER

Summary

Cybersecurity Engineering Review (CSER)

Introduction

SEI Cybersecurity Engineering (CSE)

An approach for integrating software security engineering with Secure Systems Engineering (SSE) across the acquisition lifecycle.

Key areas of focus:

- Mission assurance/mission engineering
- Procurement strategies
- Secure system design
- Security management / information protection (IP)
- Software assurance (SwA)
- Supply chain risk management (SCRM)
- Anti-tamper (AT)
- Model-based system engineering (MBSE)
- Reference architectures with associated documentation to support assessments

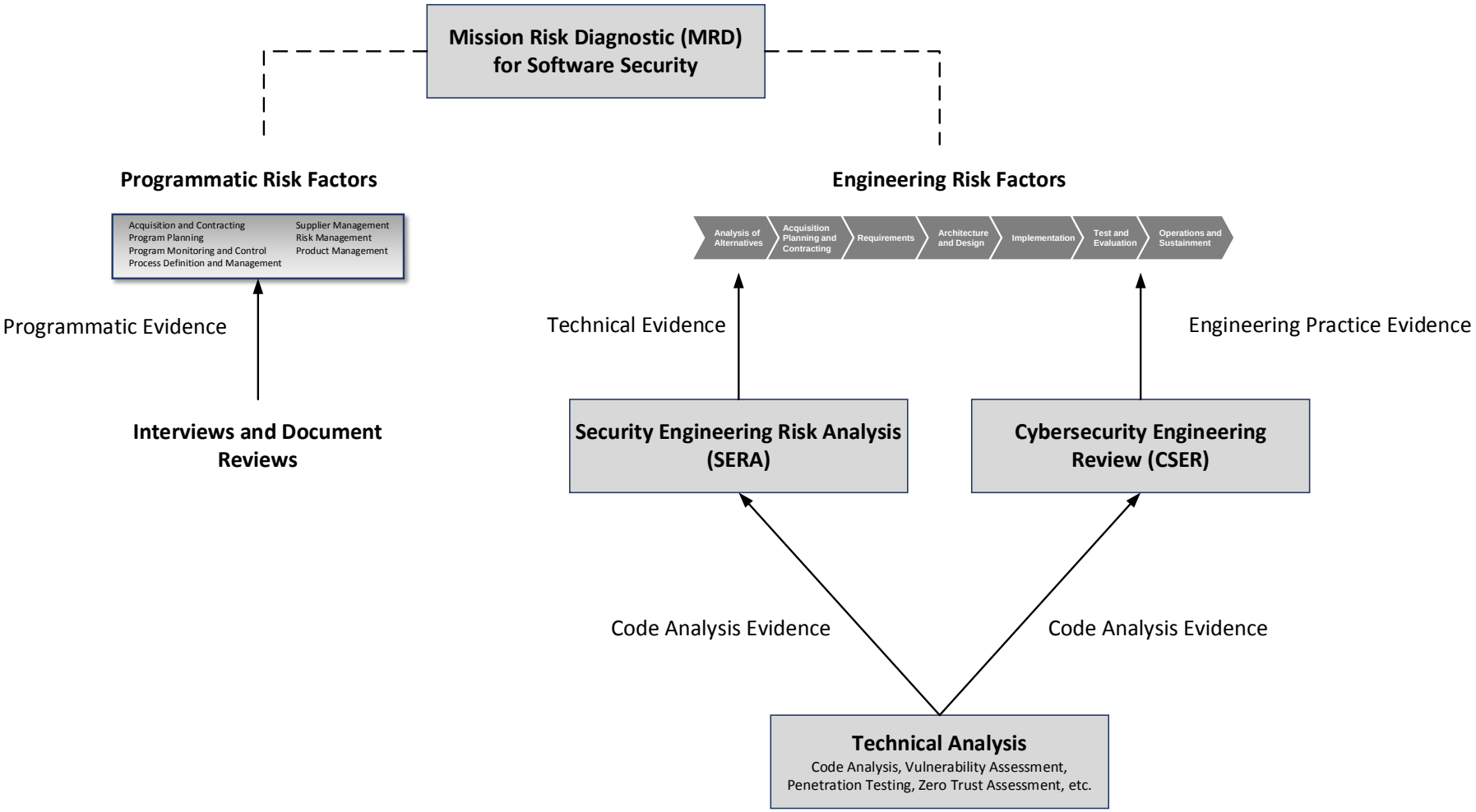
Situational Awareness (SA) CSE Assessments

Assessments are a key component of SEI's CSE strategy.

The CERT SA Team performs the following CSE assessments:

- Mission Risk Diagnostic (MRD)
- Security Engineering Risk Analysis (SERA)
- Cybersecurity Engineering Review (CSER)

SA CSE Assessments: *An Integrated View*



Mission Risk Diagnostic (MRD)

What

- An approach for assessing mission risk in interactively complex, socio-technical systems (e.g., acquisition programs, development projects, enterprise initiatives, organizational capabilities)

Why

- Assess a mission's current potential for success in relation to a set of known risk factors
- Develop a plan for managing risk and increasing the potential for mission success

Benefits

- Provides a time-efficient means of assessing acquisition programs, development projects, initiatives, and capabilities
- Establishes confidence in the ability to achieve mission objectives
- Can be self-applied or expert led

Security Engineering Risk Analysis (SERA)

What

- A systematic approach for analyzing complex security risks in software-reliant systems and systems of systems across the lifecycle and supply chain

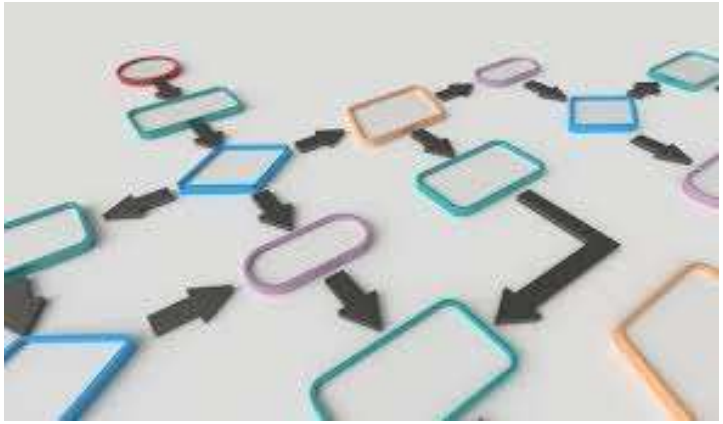
Why

- Build security into software-reliant systems by addressing design weaknesses as early as possible (e.g., requirements, architecture, design)
- Assemble a shared organizational view (business and technical) of cybersecurity risk

Benefits

- Correct design weaknesses before a system is deployed
- Reduce residual cybersecurity risk in deployed systems
- Ensure consistency with NIST Risk Management Framework (RMF)

Cybersecurity Engineering Review (CSER)



What

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

Why

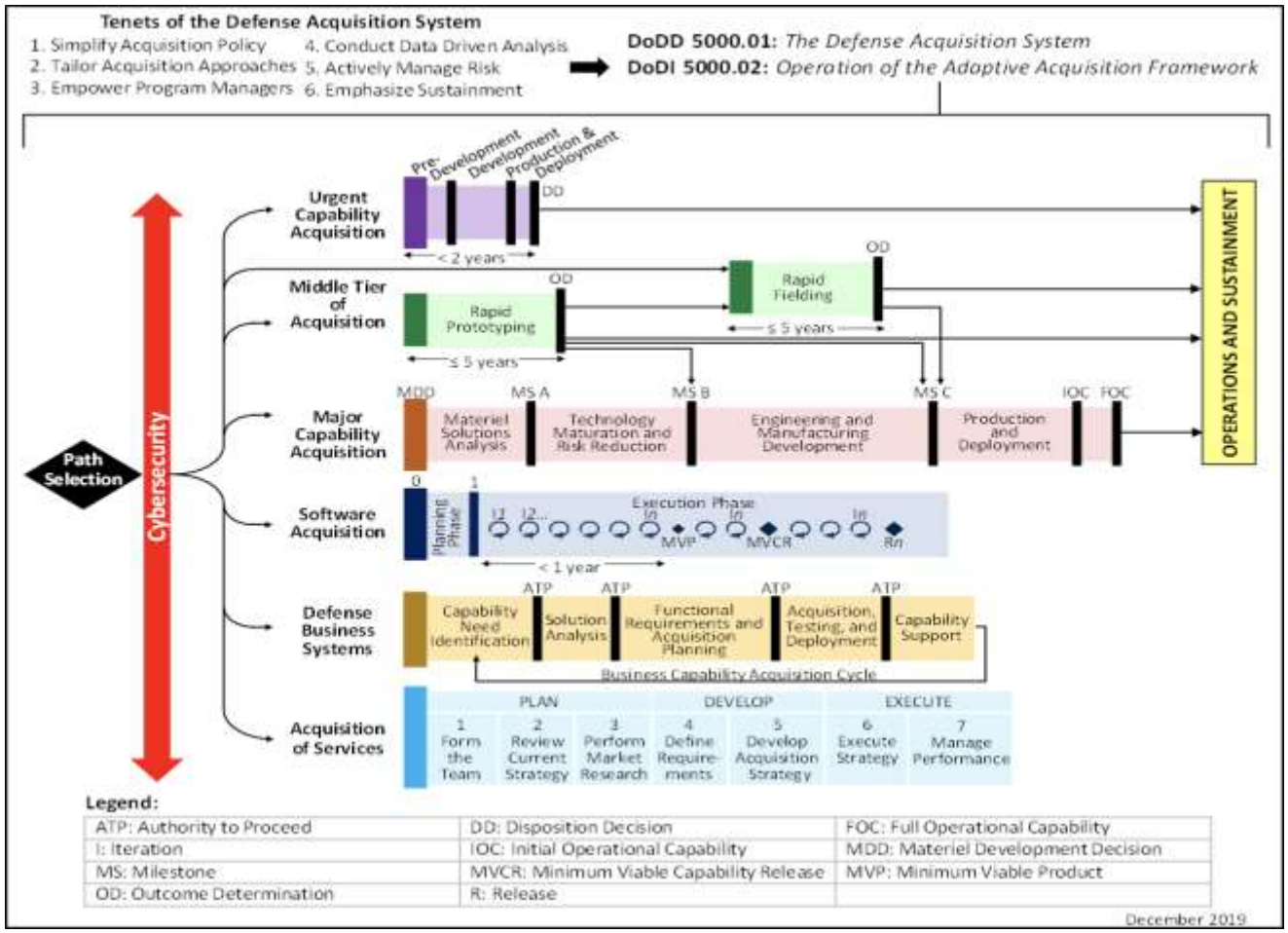
- Understand the effectiveness of an acquisition program's cybersecurity practices
- Develop a plan for improving a program's cybersecurity practices

Benefits

- Establish confidence in a program's ability to acquire software-reliant systems across the lifecycle and supply chain
- Reduce cybersecurity risk of deployed software-reliant systems

Adaptive Acquisition Framework: *Multiple Acquisition Pathways*

SA cybersecurity assessments can be tailored to multiple types of acquisitions.



Cybersecurity Engineering Review (CSER)

Prototype CSE Lifecycle Roadmap

A collection of cybersecurity engineering practices and competencies that can be applied across the lifecycle:

1. Security Risk Assessment
2. Requirements
3. Architecture and Design
4. Implementation
5. Developmental Test and Evaluation (DT&E)
6. Operational Test and Evaluation (OT&E)
7. Operations and Sustainment (O&S)

Each area of the roadmap includes the following:

- Practices
- Evidence (key outputs produced)
- Competencies

CSER: *Assessment Approach*

Collect data on program's security practices.

- Document review
  - Plans and processes
  - Work products (e.g., requirements, architecture analysis)
- Interviews (optional)
- Studies (optional)

Evaluate program's security practices in relation to CSE Lifecycle Roadmap practices.

Document observations about program's security practices.

- Strengths
- Weaknesses

Example: *General Observations*

Compliance Focus

Security is focused on system compliance. [Systems Engineering Management Plan, System Security Plan]

- Lack of a broader context (e.g. system of systems, mission resilience) could lead to unmitigated security risks.

Process Integration

Security is viewed as a specialty engineering activity. [Systems Engineering Management Plan, Critical Design Review]

- This could indicate a lack of process integration.

It is unclear how well cybersecurity engineering practices are integrated with system engineering activities. [Systems Engineering Management Plan, Critical Design Review]

- This could lead to unmitigated security risks.

Example: *Roadmap Observations*

1. Security Risk Assessment

Evaluation: Partially addressed

Rationale:

- Unclear how security assessments are performed
- Unclear if security assessments are comprehensive enough to satisfy the intent of Security Risk Assessment.

Evidence:

- A security assessment is performed on any change created as part of a Systems Engineering (SE) activity. [Systems Engineering Management Plan]
- Security assessments are completed at each relevant SE Lifecyle stage. [Systems Engineering Management Plan]
- For unaccredited systems, a security risk assessment incorporates relevant content from engineering artifacts. [System Security Plan]

CSER: *Summary*

Customer Types:

- Foreign Military Sales (FMS) (1 pilot)

Time to conduct:

- 1-3 months (depending on scope)

Cybersecurity Engineering Review (CSER)

Preparing for the CSER

SMCS Documents

Program Management Plan

System Security Plan

Disaster Mitigation Plan

Template for the Incident Log

Software Development Plan

Configuration Management Plan

Master Test Plan

Operations and Maintenance Plan

Master Training Plan

Incident Log Template

SMCS Product Backlog

Other Documents of Interest -1

Program Plans

- Integrated Master Schedule (IMS)
- Systems Engineering Management Plan (SEMP)
- Information Support Plan (ISP)
- Program Protection Plan (PPP)
- Certification and Accreditation Plan/Procedures

Risk and Metrics

- Risk Management Plan
- Risk Reports
- Metrics Reports

Other Documents of Interest -2

Requirements

- System Requirements Specification (SRS)
- Software Requirements Specification
- Operational Requirements Document (ORD)

Architecture and Design

- Mission Threads
- Reference Architecture
- Architecture Documents/Views
- Technical Data Package (TDP)

Other Documents of Interest -3

Coding/Implementation

- Secure Coding Standards
- Code Analysis Procedures and Tools

Test and Evaluation

- Vulnerability Assessment Procedures
- Adversarial Assessment Procedures
- Vulnerability Assessment Test Reports
- Adversarial Assessment Test Reports

Certification and Accreditation

- Certification and Accreditation Plan/Procedures

Other Documents of Interest -4

Presentations and Meeting Minutes from Program Reviews

- System Requirements Review (SRR)
- Preliminary Design Review (PDR)
- Critical Design Review (CDR)
- Test Readiness Review (TRR)
- Operational Readiness Review (ORR)
- Test and Evaluation Data

Interview Sessions (Optional)

Site Coordinator

- Site point of contact
- Works with SEI team to schedule interview sessions

Interview Participants

- Small group (3-5 people) of organizational peers
  - Management
  - Technical staff
- Discuss an organization's cybersecurity engineering practices (~1 hour session)
  - Strengths
  - Weaknesses
  - Risks

CSER Scope

What information do you need from an assessment?

What is the timeframe for completing the assessment?

Which documents will we receive?

- When will we receive the documents?

Will we be conducting interviews or only performing a document review?

- If we are conducting interviews, who will be the site coordinator?

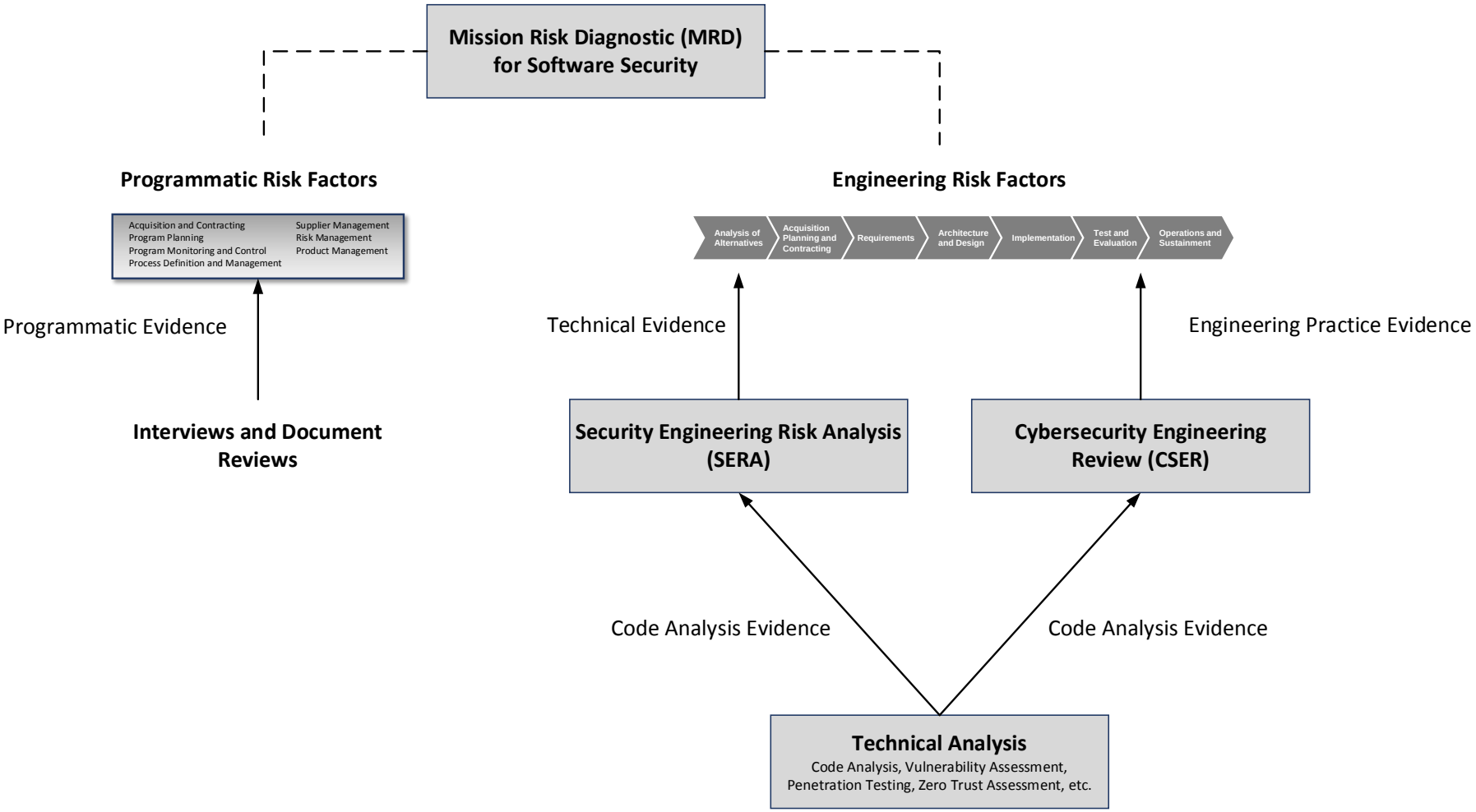
How do you want to receive the results?

- Presentation?
- Report?

Cybersecurity Engineering Review (CSER)

Summary

Summary: *SA CSE Assessments*



Key Points

SEI CSE research is defining an approach for integrating software security engineering with SSE across the acquisition lifecycle.

Assessments are a key component of the SEI CSE strategy.

- Mission Risk Diagnostic (MRD)
- Security Engineering Risk Analysis (SERA)
- Cybersecurity Engineering Review (CSER)

The CERT Situational Analysis Team is looking to expand its portfolio for its assessments.

CSER: *Assessment Approach*

Collect data on program's security practices.

- Document review
  - Plans and processes
  - Work products (e.g., requirements, architecture analysis)
- Interviews (optional)
- Studies (optional)

Evaluate program's security practices in relation to CSE Lifecycle Roadmap practices.

Document observations about program's security practices.

- Strengths
- Weaknesses