MSS Lunch & Learn Series

YALE-MSS-8: Application Development Security

Colby Laracuente
James Tucciarone III

September 2024

What are the MSS?

- The Minimum Security Standards (MSS) are baseline requirements for securing Yale IT Systems based on risk.
- The MSS apply to any Yale IT System that uses Yale data and/or operates in support of Yale's Mission

Yale *Information Security*

Understanding the MSS

Yale *Information Security*

The MSS are broken down into:

- Standard Groups (YALE-MSS-X): These group standards together based on cybersecurity requirements.
- Standards (YALE-MSS-X.Y): Standards tell us we must do to meet that cybersecurity requirement at Yale.
- Controls (YALE-MSS-X.Y.Z): Controls provide details on how you can meet the cybersecurity requirement.

YALE-MSS-1:
System Classification

YALE-MSS-1.1:
Classify the IT System and meet the Minimum Security Standards

YALE-MSS-1.1.2:
Determine your system type

What MSS will we cover today?

Yale *Information Security*

YALE-MSS-8: Application Development Security

Overview

YALE-MSS-8.1: Follow an appropriate secure development methodology when writing software

YALE-MSS-8.2: Test for security vulnerabilities when any changes are made to the system

YALE-MSS-8.1: Follow an appropriate secure development methodology when writing software

- Plenty of suitable methodologies!

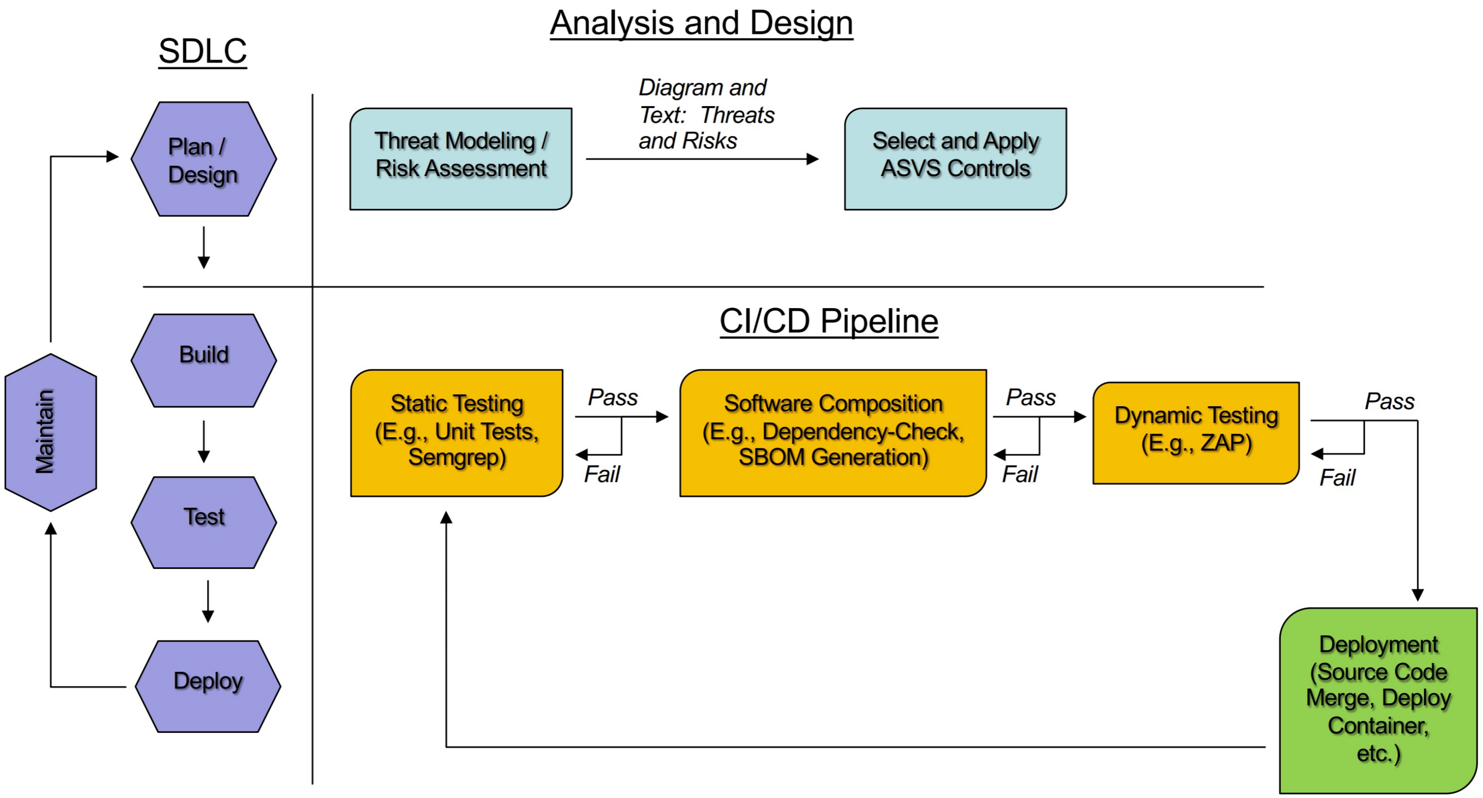
- Generally, your process should consist of
  - Plan/Design
  - Build
  - Test
  - Deploy
  - Maintain

- Consult the OWASP Top 10 and OWASP ASVS during the Plan/Design phase

- Training Platform

YALE-MSS-8: Application Development Security

Yale Information Security



Analysis and Design
SDLC
Plan / Design
Threat Modeling / Risk Assessment
Diagram and Text: Threats and Risks
Select and Apply ASVS Controls
CI/CD Pipeline
Maintain
Build
Test
Deploy
Static Testing (E.g., Unit Tests, Semgrep)
Pass
Fail
Software Composition (E.g., Dependency-Check, SBOM Generation)
Pass
Fail
Dynamic Testing (E.g., ZAP)
Pass
Fail
Deployment (Source Code Merge, Deploy Container, etc.)

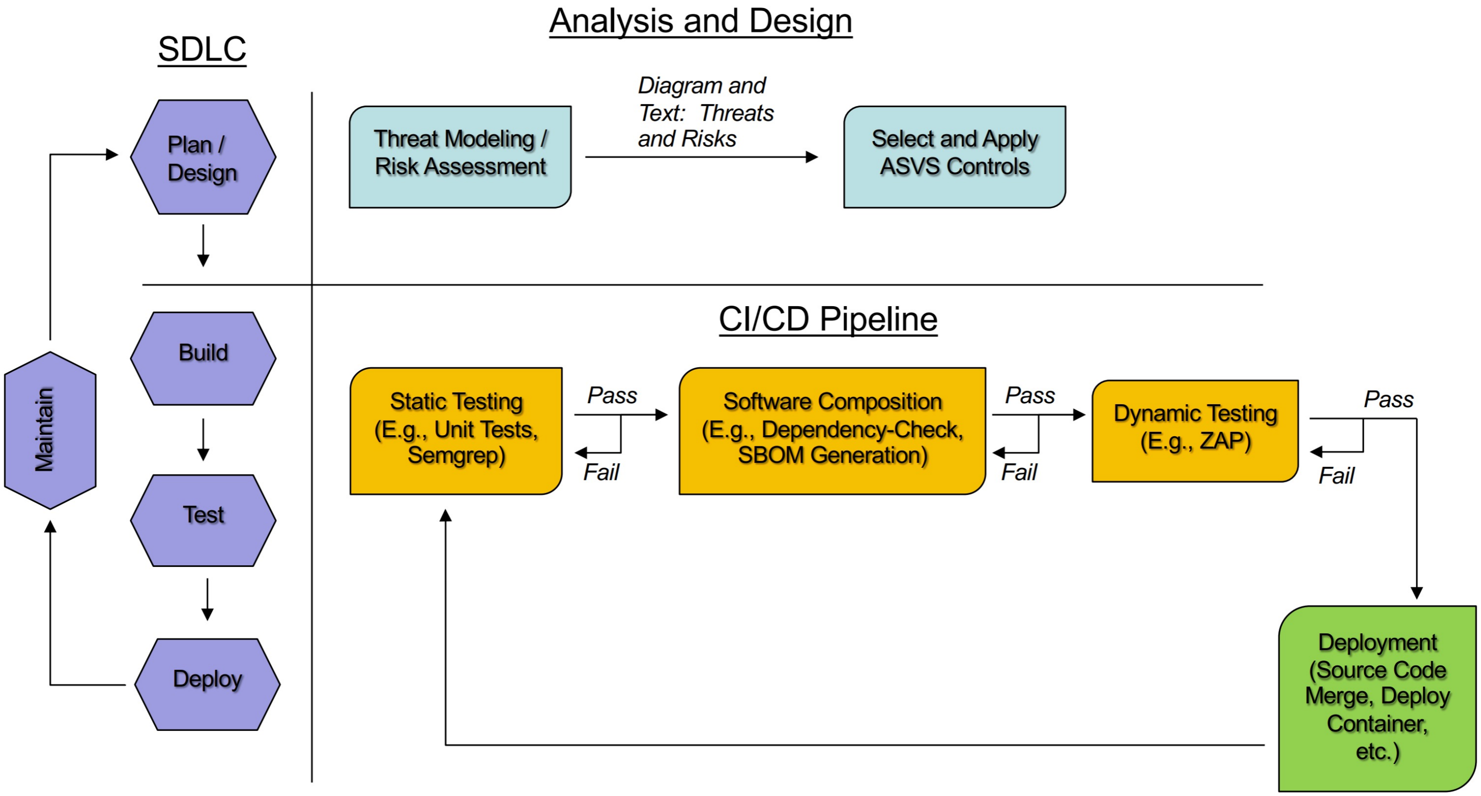
YALE-MSS-8.2: Test for security vulnerabilities when any changes are made to the system

- Deploy changes to test environment first

- Static Application Security Testing (SAST)
  - Semgrep
  - SonarQube
  - CodeQL
- Software Composition Analysis (SCA)
  - FOSSA
  - OWASP Dependency-Check
  - Github Dependabot
- Dynamic Application Security Testing (DAST)
  - ZAP
  - Burp Suite
  - Acunetix

YALE-MSS-8: Application Development Security

Yale *Information Security*



SDLC
Analysis and Design
Plan / Design
Threat Modeling / Risk Assessment
Diagram and Text: Threats and Risks
Select and Apply ASVS Controls
Maintain
Build
Test
Deploy
CI/CD Pipeline
Static Testing (E.g., Unit Tests, Semgrep)
Pass
Fail
Software Composition (E.g., Dependency-Check, SBOM Generation)
Pass
Fail
Dynamic Testing (E.g., ZAP)
Pass
Fail
Deployment (Source Code Merge, Deploy Container, etc.)

Application Security Program

- 3-year effort to promote secure coding at Yale.
- https://yaleedu.sharepoint.com/sites/YaleApplicationSecurityProgram
- Bi-Monthly Forum Meeting

What is a SPA?

Yale's simplified process to highlight and manage this risk through compliance with the MSS. Required for all IT systems (excluding endpoints and mobile devices).

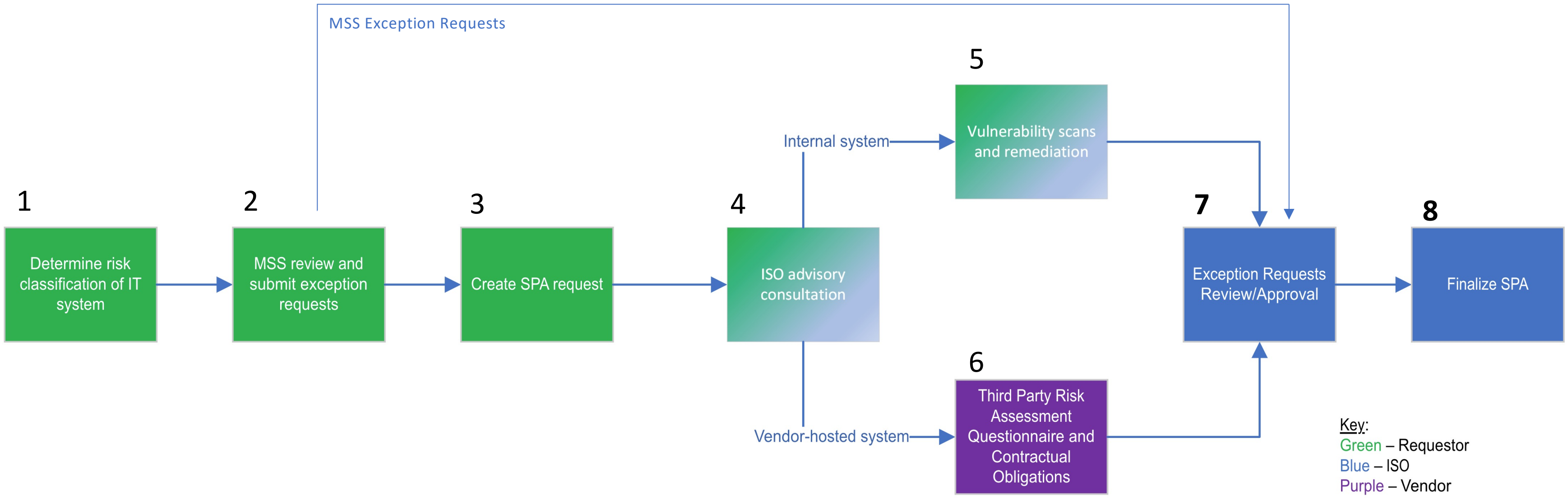
- Think through how to meet and maintain the MSS for a system
- Contribute to a registry of IT systems for security testing
- Identify and understand risk

A SPA is not:

- A detailed review of the security of an IT system
- A statement of approval from ISO about an IT system

Steps to the SPA Process

Yale *Information Security*



1 Determine risk classification of IT system

2 MSS review and submit exception requests

MSS Exception Requests

3 Create SPA request

4 ISO advisory consultation

Internal system

5 Vulnerability scans and remediation

Vendor-hosted system

6 Third Party Risk Assessment Questionnaire and Contractual Obligations

7 Exception Requests Review/Approval

8 Finalize SPA

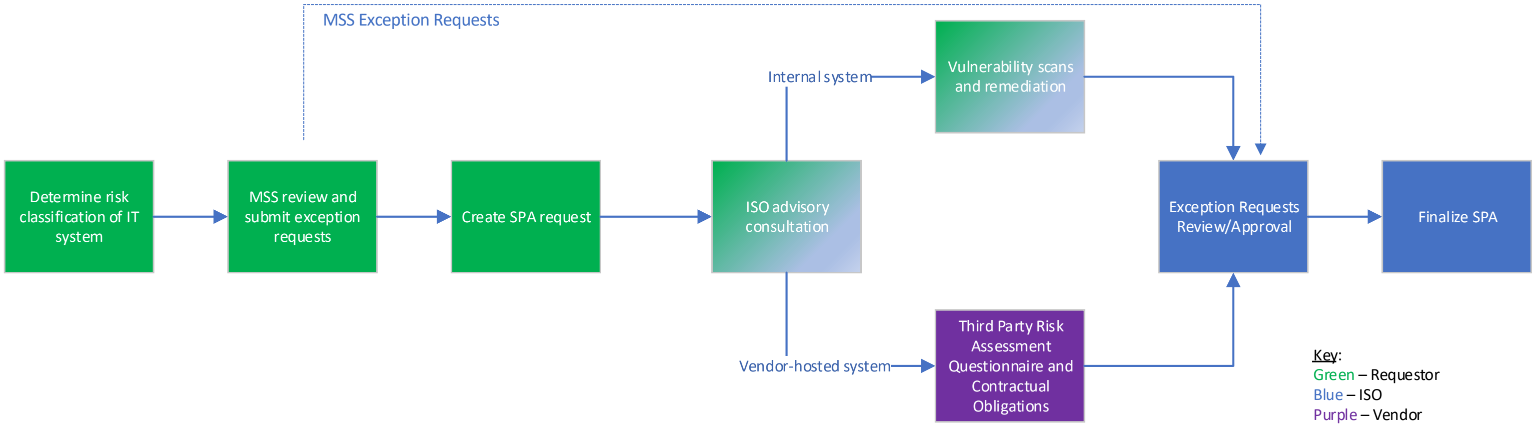
Key:
Green – Requestor
Blue – ISO
Purple – Vendor

Questions and Answers

Yale *Information Security*

Appendix: SPA at a Glance

Yale Information Security



MSS Exception Requests

Determine risk classification of IT system

MSS review and submit exception requests

Create SPA request

ISO advisory consultation

Internal system

Vulnerability scans and remediation

Vendor-hosted system

Third Party Risk Assessment Questionnaire and Contractual Obligations

Exception Requests Review/Approval

Finalize SPA

Key:
Green – Requestor
Blue – ISO
Purple – Vendor

The SPA is used to:

- Think through questions about how to meet and maintain the MSS for your IT system.
- Contribute to a registry of IT systems used for security testing.
- Identify and understand risk related to your IT system.

The SPA is not:

- A detailed review of the security of an IT system.
- A statement of approval from the ISO about an IT system.

Important Links:

Risk Classification
https://cybersecurity.yale.edu/risk-classification

MSS Calculator
https://cybersecurity.yale.edu/mss/calculator

Submitting a SPA
https://cybersecurity.yale.edu/spa

Submitting an Exception Request
https://cybersecurity.yale.edu/exception-request