

# MSS Lunch & Learn Series

## YALE-MSS-5 (Software Security)

AJ Labozzo

July 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



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 review today?

- YALE-MSS-5: Software Security



Yale *Information Security*

### YALE-MSS-5.1: Utilize an industry-standard secure configuration method

- <https://www.cisecurity.org/cis-benchmarks/>
- <https://www.nist.gov/programs-projects/national-checklist-program/>

### YALE-MSS-5.1.1: Document your approach to the chosen configuration standard

### YALE-MSS-5.1.2: Utilize file integrity and configuration checking tools

### YALE-MSS-5.2: Utilize endpoint protection

YALE-MSS-5.2.1: Utilize a next generation anti-virus solution

YALE-MSS-5.2.2: Run endpoint detection response tool

### YALE-MSS-5.3: Run supported software and operating systems

**YALE-MSS-5.4: Ensure all software is actively supported by a vendor or open-source project**



YALE-MSS-5.5: Manage all changes to the system through a change control process

YALE-MSS-5.5.1: All changes to the IT system are analyzed to ensure the security posture is not weakened

Yale-MSS-5.5.2: An audit trail for changes to the IT system is maintained to account for when changes were made and by whom

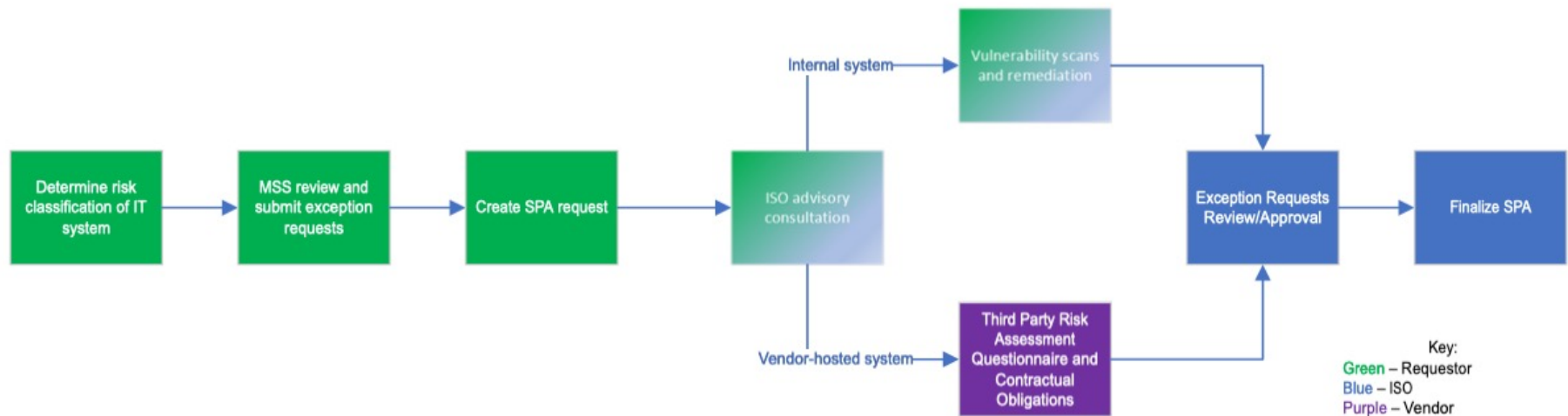
# What is a SPA?



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



# Questions and Answers

