

# MSS Lunch & Learn Series

## YALE-MSS-6: Patching

Timothy Wright  
Aaron Wilkey  
James Tucciarone III  
Jessica Flower

August 21, 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-6: Patching



**Yale** *Information Security*

# Microsoft Digital Defense Report 2023

# 99%

Basic security  
hygiene protects  
against 99%  
of attacks

Patch early,  
patch often!



Enable multifactor  
authentication (MFA)



Apply Zero Trust  
principles



Use extended detection and  
response (XDR) and antimalware



Keep up  
to date



Protect  
data

← Outlier attacks on the bell curve make up just 1% →



Yale *Information Security*

## Yale MSS 6.1: Apply security patches regularly

- “Timely patching is critical...” (Patch early, patch often!)
- Apply security patches every 30 days—vendors, too
  - What does this get us? **Helps with TTE**
  - Time-to-Exploit (TTE): average time for a threat actor to exploit a vulnerability
    - [One study \(by Mandiant\)](#) puts TTE at about 32 days in 2022
    - [Another study \(by Rapid7\)](#) puts TTE at 7 days for known vulnerabilities in 2022
- Docker containers: update and re-execute images
- Emergency patches may need to be applied in less than 30 days (more to come...)

Yale MSS 6.1.1: Apply all security patches to operating systems, software, and firmware based on risk

- Critical-severity vulnerabilities ([CVSS](#) score 9+) **must be patched immediately**
- Recipe: it's an emergency if you answer 'yes' to any three of the following...
  - Is system high-risk? ([Risk Classification Guideline](#))
  - Is the vulnerability's severity (CVSS score) 7 or higher? ([National Vulnerability Database](#))
  - Is system Internet Accessible? ([MSS Key](#))
  - Is there an active exploit? (National Vulnerability Database, [KEV](#), et al.)
- Otherwise, patch per normal: within 30 days

## YALE-MSS-6: Patching



Yale MSS 6.1.2: Identify maintenance windows for necessary upgrades/patches

- Window should be every 30 days
- The 'when' is up to your team (e.g., on 15<sup>th</sup> of each month from 5 p.m. to 5 a.m.)



## Yale MSS 6.1.3: Implement an emergency patch process

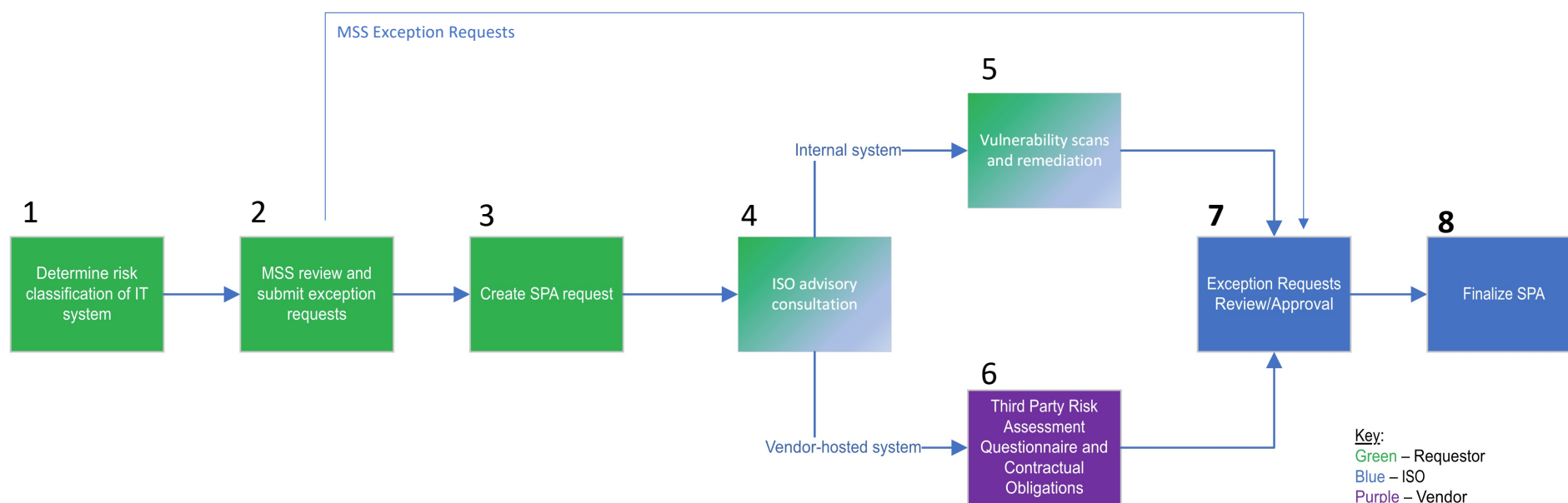
- First, a Configuration Management Plan is needed ([MSS 5.5](#)): describes how changes to a system are managed and tracked (for ITS-managed systems see [ITS Change Guides](#)):
  - Roles and responsibilities
  - Pre-approved and exempt changes
  - Change management records (to document a change)
  - Normal change procedure: test, document change, review change, deploy if approved, re-test
- Next, within the Plan, add a process for emergency changes
  - Deploy before testing and documentation
  - Retroactively go through change procedure—back out change if needed

# What is a Security Planning Assessment (SPA)?



- A 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
- A SPA is **not**:
  - A gate (from ISO's perspective)
  - A detailed review of the security of an IT system
  - A statement of approval from the Information Security Office about an IT system

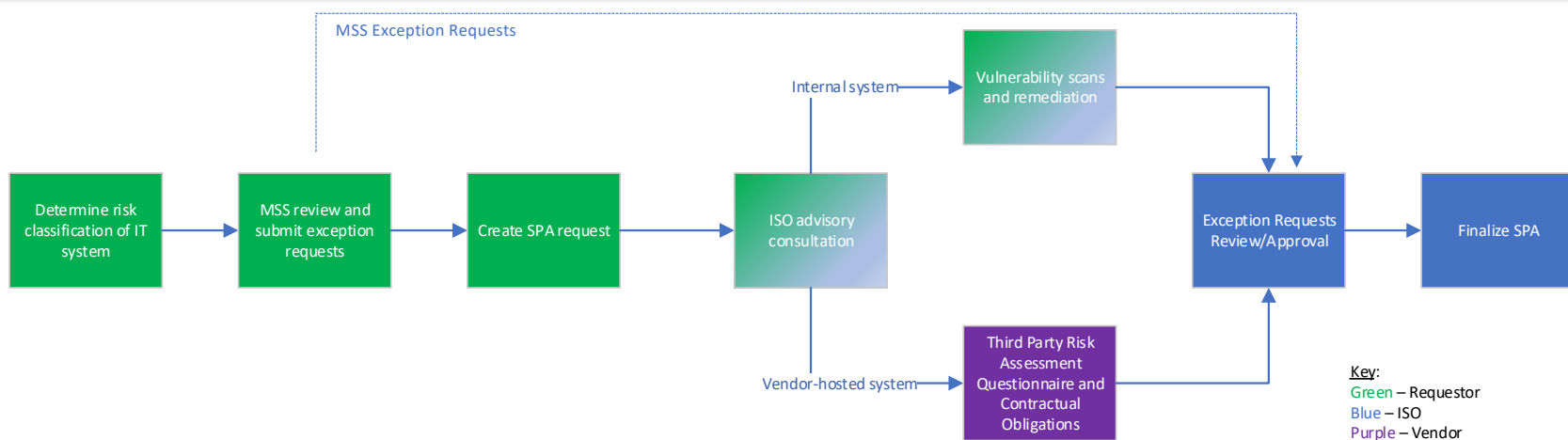
# Steps to the SPA Process



# Questions and Answers



# Appendix: SPA at a Glance



## 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>