MSS Lunch & Learn Series

YALE-MSS-4 (Physical Security)
YALE-MSS-7 (Data Protection)

Tom Castiello

June 13, 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 review today?

- YALE-MSS-4: Physical Security
- YALE-MSS-7: Data Protection

Yale *Information Security*

Yale-MSS-4: Physical Security

Yale *Information Security*

YALE-MSS-4.1: Physically secure Critical IT Spaces

YALE-MSS-4.2: Physically secure the IT System

YALE-MSS-4.3: Ensure print jobs are physically secure

Yale-MSS-7: Data Protection (Encryption)

Yale *Information Security*

- MSS 7 covers several areas:
  - Encryption
  - Device controls
  - Data controls
  - Mobile devices

Yale-MSS-7: Data Protection (Encryption)

Yale *Information Security*

- Encrypt all electronic storage devices (MSS 7.2)
- Encrypt data in transit and at rest (MSS 7.3)
- All network traffic must use a strong, industry-standard encryption method (MSS 7.6)

Yale-MSS-7: Data Protection (Device)

Yale *Information Security*

- Recycle IT Systems using Yale's Environmental Health and Safety (EHS) Process (MSS 7.4)
- Sanitize systems before re-use (MSS 7.5)
- Use inactivity locks (MSS 7.9)

Yale-MSS-7: Data Protection (Data)

Yale *Information Security*

- Back up user-level and system-level data (MSS 7.1)
- Purge data once it is no longer required (MSS 7.7)
- Utilize host Data Loss Prevention (MSS 7.8)
- Store Yale Data within the United States (MSS 7.10)

Yale-MSS-7: Data Protection (Mobile)

Yale *Information Security*

- Use secure Bluetooth (MSS 7.11)
- Enroll in a remote wipe capability (MSS 7.12)
- No circumvention of device security (“Jailbreaking”) (MSS 7.13)

What is a SPA?

Yale Information Security

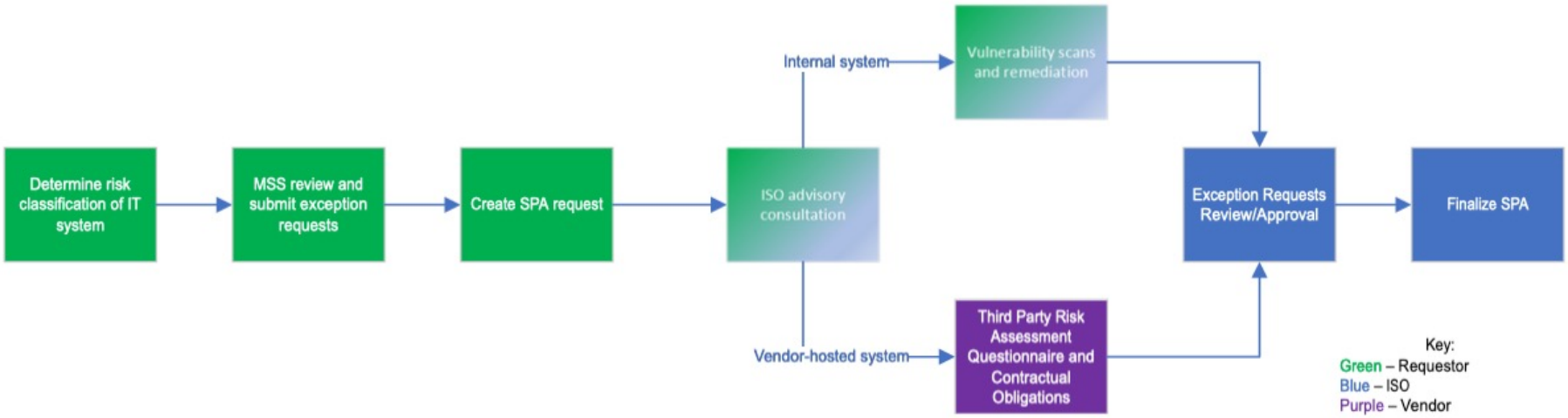
Yale's simplified process to highlight and manage this risk through compliance with the MSS. Required for all IT systems (excluding endpoints and mobile devices).

- 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*



Questions and Answers

Yale *Information Security*

Appendix: Yale-MSS-4 (Physical Security)

Yale *Information Security*

	Low	Moderate	High
YALE-MSS-4.1: Physically secure Critical IT Spaces			X (server)
YALE-MSS-4.2: Physically secure the IT System			X
YALE-MSS-4.3: Ensure print jobs are physically secure			X (printer)

Appendix: Yale-MSS-7 (Data Protection)

Yale *Information Security*

	Low	Moderate	High
YALE-MSS-7.1: Back up user-level and system-level data		X	X
YALE-MSS-7.2: Encrypt all electronic storage devices		X	X
YALE-MSS-7.3: Encrypt data in transit and at rest		X	X
YALE-MSS-7.4: Recycle IT Systems using Yale's Environmental Health and Safety (EHS) Process	X	X	X
YALE-MSS-7.5: Sanitize systems before re-use			X
YALE-MSS-7.6: All network traffic must use a strong, industry-standard encryption method		X	X
YALE-MSS-7.7: Purge data once it is no longer required		X	X
YALE-MSS-7.8: Utilize host Data Loss Prevention (DLP)			X (HIPAA)
YALE-MSS-7.9: Use inactivity locks		X	X
YALE-MSS-7.10: Store Yale Data within the United States		X (server)	X (server)
YALE-MSS-7.11: Use secure Bluetooth			X
YALE-MSS-7.12: Enroll in a remote wipe capability		X (mobile)	X (mobile)
YALE-MSS-7.13: No circumvention of device security ("Jailbreaking")		X (mobile)	X (mobile)

Appendix: Steps to Complete a SPA

Yale *Information Security*

ISO is there to guide and answer questions about the MSS and the SPA process. **Contact your team's IT support if you'll need help** completing the following steps.

1. Risk classification
   - Classify based on data sensitivity, availability requirements, and external obligations

2. MSS review
   - Review your IT system's alignment with the applicable MSS requirements

Appendix: Steps to Complete a SPA (cont)

Yale *Information Security*

3. Submit exception request for:
   - Any MSS requirement that cannot be met
   - Any critical, high, or medium severity vulnerabilities that cannot be addressed in 30 days.

4. Submit SPA request form **after** completing risk classification, MSS review, exception request

Appendix: Steps to Complete a SPA (cont)

Yale *Information Security*

5. ISO guides SPA effort
   - Requester answers various questions; meets with ISO
   - If a vendor is involved
     - Requester works with Procurement: contract, Yale Data Addendum
     - ISO surveys vendor
     - If HIPAA is involved, requester obtains BAA

Appendix: Steps to Complete a SPA (cont)

Yale *Information Security*

6. ISO guides SPA effort (continued)
   - If system is local to Yale
     - ISO scans for vulnerabilities
     - Requester addresses findings (or submits exception request)