

MSS Lunch & Learn Series

YALE-MSS-13: Logging

Timothy Wright
Aaron Wilkey
James Tucciarone III

November 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



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-13: Logging



Yale *Information Security*

What are we talking about here?

- “A *log* is a record of the events occurring within an organization’s systems and networks.” – NIST (National Institute of Standards and Technology) *Guide to Computer Security Log Management* ([SP 800-92](#))
- Why so important?
 - Incident response
 - Troubleshooting
 - Resource use tracking (what gets measured, gets managed)



Yale MSS 13.1: Ensure logging contains information required for incident response

- **Servers only**
- Need a minimum of information for troubleshooting and incident response. E.g.:
 - The time and date an event happens
 - System name
 - Source and destination IPs, if network communications are involved
 - User/service account IDs, if feasible
 - The name and ID of the affected process
 - Any basic messages generated by the process (e.g., error, debug, informational messages)
- Yale MSS 13.1.1: Use multiple time servers (*a person with two clocks is never sure of the time*)
- Yale MSS 13.1.2: Ensure client IP addresses are not obscured by load balancers and reverse proxies
- Yale MSS 13.1.3: Ensure adequate space to log data. Logs should be kept for a minimum of 90 days.

YALE-MSS-13: Logging



Yale MSS 13.2: Log all authentication events

- **Endpoints and Servers** (moderate- and high-risk)
- Becomes a non-issue when you use Yale's central authentication (e.g., single sign-on via CAS)
- Yale MSS 13.2.1: Collect logs that include all authentication and privileged escalation events

YALE-MSS-13: Logging



Yale MSS 13.3: Ensure logs are forwarded to a log server in addition to the in-scope system

- **Not currently required by MSS**—eventually for moderate- and high-risk servers
- Options for access to a log server depend on system deployment; **work with your IT support to deploy the best solution for your system**
 - [AWS CloudWatch](#)
 - [Azure Monitor](#)
 - [Google Cloud Operations](#)
 - Local to Yale
 - Windows—[Winlogbeat/Filebeat](#) (transmits data to ISO's SIEM)
 - Linux—Filebeat (transmits data to [Logstash](#) and [Graylog](#)--possibly to ISO's SIEM, too, depending on server)

Yale MSS 13.4: Collect and review all source system activity logs

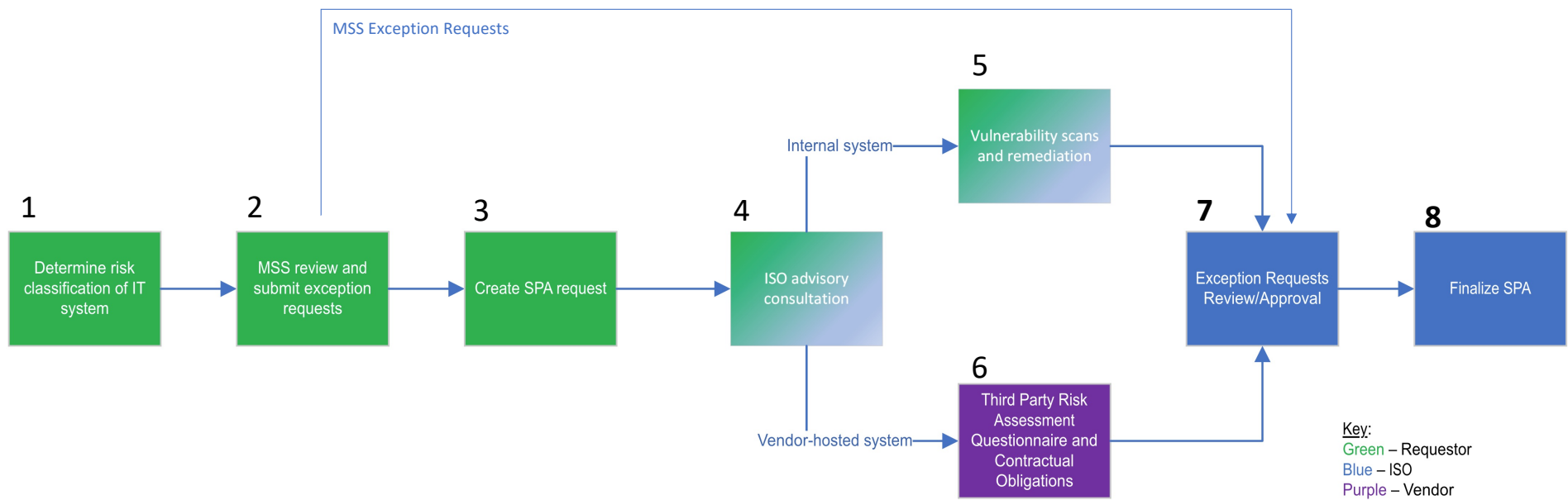
- **HIPAA Systems only**
- *Source system*: in HIPAA, this is an authoritative source of ePHI. [Yale Policy 5142](#) requires auditing of source system activity logs and specifies system activities of interest
- Yale MSS 13.4.1: Identify, track, and periodically audit source systems for compliance with all applicable laws, regulations, and University policies, standards, and procedures
- Yale MSS 13.4.2: Collect log data needed for Information System Activity Review

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



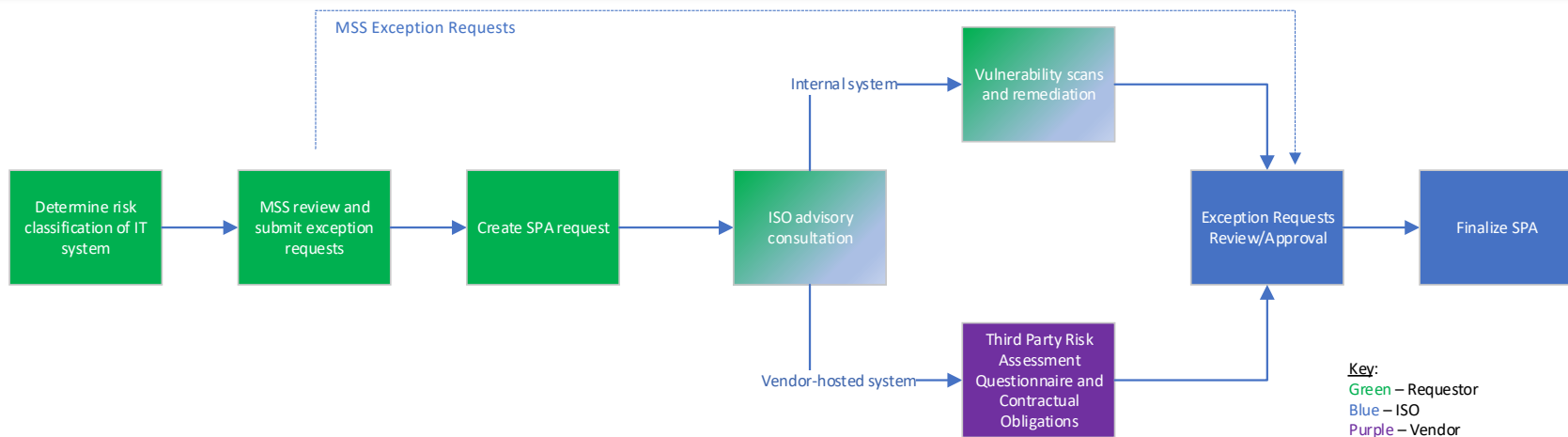
Questions and Answers



Yale *Information Security*



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>