MSS Lunch & Learn Series

YALE-MSS-1: System Classification
YALE-MSS-11: Security Training

Jessica Flower
James Tucciarone III
Aaron Wilkey

April 17, 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

YALE-MSS-1: *System Classification*

Yale *Information Security*

YALE-MSS-1: System Classification

STANDARDS

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

YALE-MSS-1.2: Apply any additional security requirements required by external obligations

YALE-MSS-1.3: Ensure appropriate contracts for all third-party relationships are in place

YALE-MSS-1.4: Designate and protect Critical IT Infrastructure

YALE-MSS-1.5: Plan for data recovery requirements

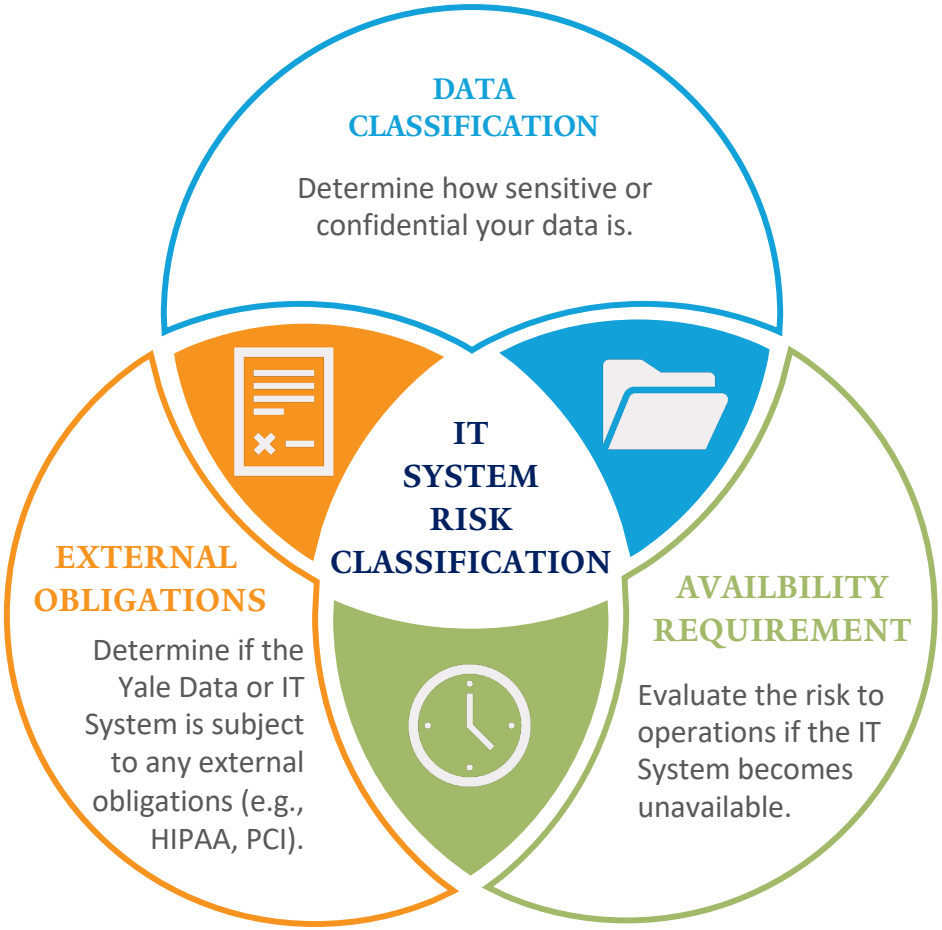
YALE-MSS-1.6: Plan for meeting and maintaining the security requirements for the IT System

YALE-MSS-1.7: Complete a Security Planning Assessment (SPA)

YALE-MSS-1.1
YALE-MSS-1.2

Classify the System and External Obligations

Yale *Information Security*



The highest risk from the three elements = the risk classification of the IT System

YALE-MSS-1.1
YALE-MSS-1.2

Example

Yale *Information Security*

An IT System is being built for the Yale School of Medicine. This system will store personally identifiable patient data (Protected Health Information – "PHI"). The data cannot be unavailable for more than 12 hours.

Data Classification	Availability Requirement	External Obligations	Overall Risk
PHI is classified by Yale as High Risk	0-8 hours = High Risk 8-24 hours = Moderate Risk > 24 hours = Low Risk	All PHI is regulated by HIPAA	High Risk & HIPAA
High Risk	Moderate Risk	HIPAA	

YALE-MSS-1.3

Contracts for Third-Party Relationships

Yale *Information Security*

- A data addendum is required for High Risk and Moderate Risk data stored in a vendor's cloud.

- A Business Associate Agreement (BAA) is required when PHI is disclosed to, created by, or received by a business associate.

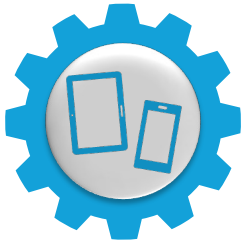
YALE-MSS-1.1

Determine the System Type

Yale *Information Security*

Servers

Endpoints



Mobile Devices

Network Printers

YALE-MSS-1.4: *Critical IT Infrastructure*

Yale *Information Security*

Critical IT Infrastructure is defined as an IT system that:

- Unrelated IT systems have a dependency on
- Is complex or specialized in nature and requires special protections beyond Yale's MSS

This standard enforces extra security controls to protect critical IT infrastructure appropriately.

YALE-MSS-1.5

Plan for Data Recovery Requirements

Yale *Information Security*

- Ensure adequate backups of the data the IT System contains.
- Determine the maximum amount of data that can be lost during a disruption before incurring significant impact to operations.

YALE-MSS-1.6

Plan for Meeting and Maintaining the MSS

Yale *Information Security*

Security planning should include:

1. Classifying the system
   "What do I have?"

2. Knowing your game plan
   "Who is doing what?"

3. Submitting exception requests
   "What is not being met?"

YALE-MSS-1.7: *Complete a Security Planning Assessment*

Yale *Information Security*

What is a SPA?

The Security Planning Assessment (SPA) is a process to ensure the security of Yale IT Systems. The SPA replaces the old Security Design Review (SDR) process. The SPA process is based on Yale's Minimum Security Standards (MSS). It ensures you have a plan to operate a secure IT System through the life span of the system.

MSS Review

Know your system's risk and apply requirements before requesting a SPA.

SPA Intake

Request a SPA and complete a risk assessment of the system.

Risk Mitigation

Address specific risks to the system to complete the SPA.

YALE-MSS-11: *Security Training*

Yale *Information Security*

YALE-MSS-11: Security Training

STANDARDS

YALE-MSS-11.1: Require security training for all users of Yale Data and Yale IT Systems

YALE-MSS-11.2: Ensure all third parties complete required training

Addendum

Yale *Information Security*

- YALE-MSS-1: Risk Classification
- YALE-MSS-11: Security Training
- Yale's Risk Classification Guideline
- Contacting Procurement: Purchasing Intake Portal
- HIPAA Policy 5033: Disclosure of PHI to Business Associates
- Minimum Physical Security Standards for Critical IT Spaces
- Applying the MSS to IT Systems
- Security Planning Assessment (SPA)
- Request an Exception
- Contact the Information Security Office: information.security@yale.edu