MSS 101: Building the Foundation
Key Slides
Fall 2020
3 Actions to move the needle on the Maturity Model

- KNOW what the MSS are.
- KNOW your role in implementing the MSS.
- KNOW the risk of the work you do.
Why do we classify Yale IT systems?

Risk classification determines the appropriate security requirements

The Goldilocks Dilemma

Too much  Just Right  Too little

The MSS ensures we are here. We get the right requirements for the risk level.
The Risk Classification Guideline walks you through how to determine your risk classification:

cybersecurity.yale.edu/riskclassification
How do the MSS apply to you?

Initiator
(User)
Needs to classify data and systems used to complete his/her work
(Ex: Yale data or system users)

Advisor
(User Support Provider)
Helps users match their needs to available systems and bridge gap between Initiators & System Decision Makers
(Ex: DSP, IT Partner)

Coordinator
Information Security
Builds and maintains the MSS to protect Yale’s risk landscape

System Decision Maker
(System Owner)
Decides system classification and ensures the MSS are maintained
(Ex: PI, Service Owner, Service Offering Manager)

Doer
(System Support Provider)
Configures system to meet MSS throughout lifecycle
(Ex: System administrators, web developers)
Applying Your Role – what do you need to do?

**Users / Initiators**

What data are you working with? Is the system you are using configured to protect that level of data?

What if you’re handed new data? Or asked to use a new system? Does it match the classification of the work you are doing? Ask. It is better to be safe than sorry.

**Advisors / User Support Providers**

Do you know if your users are using tools and IT Systems that support their classification? Do your users know their classification? Get into the habit of asking.

We need you to be our champions. Help ensure users understand their classification and that they are using IT Systems that match their classification.

**System Decision Maker / System Owner**

What is the classification of the system you own? How do you communicate that classification to your users?

Is the system configured to meet the classification? Who makes up your team of system support providers to ensure the MSS are met and maintained?

**Doer / System Support Provider**

Who is the decision maker for the system you support? Have they communicated the system’s risk classification to you?

Is the system able to meet and maintain the MSS for that classification? If not, do you have an exception request for the standards it cannot meet?