Yellow Cards?
Agenda:

Introduction and Background
Key Concepts
Risk Assessment
The Risk Management Framework
Introduction and Background
Cybersecurity Risk Management Policy:

Strategy and policy for IT security
Cybersecurity Risk Management Policy:

IT Governance
Campus Leadership
Shared Governance
IT supports the mission of the University:

Provide effective, reliable, secure, appropriate and affordable IT systems for the University’s mission

“The people who provide IT services at UW-Madison are working every hour of every day to help support the Wisconsin Idea so that the university can help improve people’s lives beyond the classroom.”
IT security supports and protects the University and Campus community:

- Privacy
- Academic Freedom
- Intellectual Property
- Academic Integrity
- Reputation
- Legal and other obligations
- Resources
It’s NOT always “all about the data”
Key Concepts
Strategy: Risk-based

Decision Making: “Risk Executive”

Framework: Structured approach
Strategy: Risk-based

Identify and consider the risk in specific IT systems, make decisions in that context
Alternate Security Strategy?
Risk Executive:

Decision-maker who has the Authority, Responsibility, and Resources to accept the risk

IT staff provides risk assessment for an informed decision
Risk Assessment
Prepare risk assessment of the proposed system

Identify options to reduce the risk if necessary

Decision-maker (*Risk Executive*) makes and documents the decision
Divide complex systems into smaller, manageable building blocks

Use and reuse common building blocks
New application has higher risk data:

Use existing database?
The Risk Management Framework
Continuous Diagnostics and Mitigation (CDM):

Monitor and evaluate security on an appropriate schedule, fix any problems
Questions?