Risk Management Framework Overview

Learn @ Lunch CDSE

Presenter: Noah Lebaron

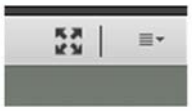
- Mr. LeBaron has been the Cybersecurity Curriculum Manager for CDSE since October 2012
- He is a former DSS Information System Security Professional from the Northern Region Field Office
- Prior to DSS, Mr. LeBaron served as an Information Systems Security Manager in private industry and spent over four years on active duty with the U.S. Air Force
- In addition, Mr. LeBaron holds CISSP, Security+, and Network+ certifications

CDSE – Cybersecurity CM

2

Learn @ Lunch CDSE

Navigation in the Meeting Room



Notes box for audio information and other announcements

To enlarge the slide, click on the Full Screen button. To get out of Full Screen view, select Full Screen again. You will need to be out of Full Screen view to enter question responses.

Learn @ Lunch

CDSE

Navigation in the Meeting Room

Q&A box for entering questions to the presenters

File share box to download resources relevant to today's presentation

Learn @ Lunch

CDSE

Three Steps to Download Files

Print slides now for note-taking during the presentation

- ✓Click on file in the **File share** box
- ✓Click "Save To My Computer"
- ✓Click to Download

Click to Download may appear in a new tab behind the meeting room

Learn @ Lunch

CDSE

Example of a Chat Question

Risk Management Framework Overview

Learn @ Lunch CDSE

Overview

- Define Cybersecurity
- Describe the DoD Transformation to Risk Management Framework
- Discuss Enterprise Wide Risk Management
- Identify the Steps of the Risk Management Framework

Learn @ Lunch CDSE

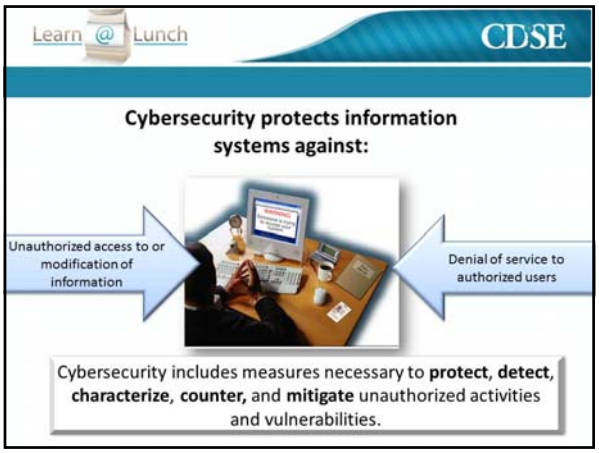
Where we've been and where we're going

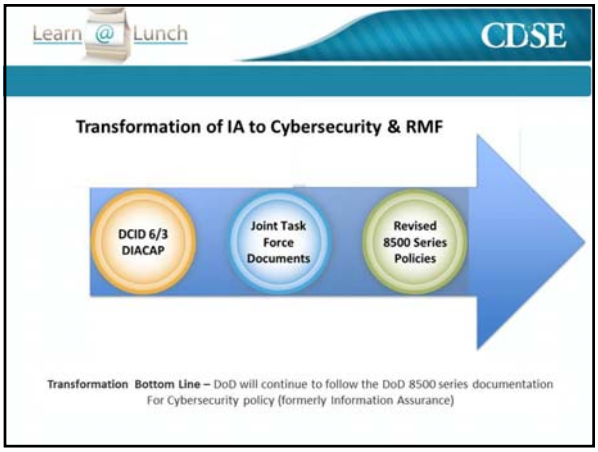
~~Information Assurance~~

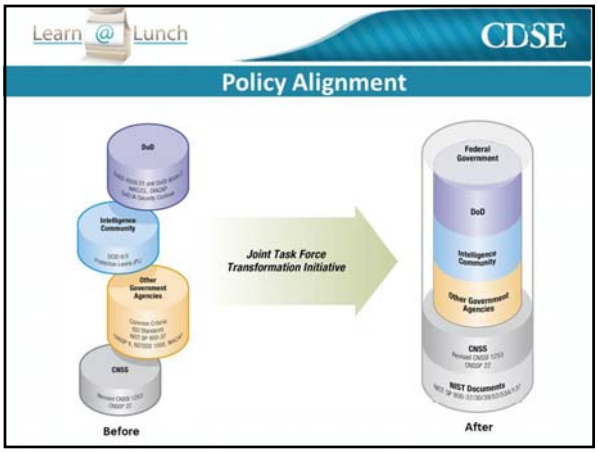
DoD Instruction 8500.01, Para 1(d), adopts the term "cybersecurity" as it is defined in National Security Presidential Directive-54/Homeland Security Presidential Directive-23 to be used throughout the DoD instead of the term "information assurance (IA)."

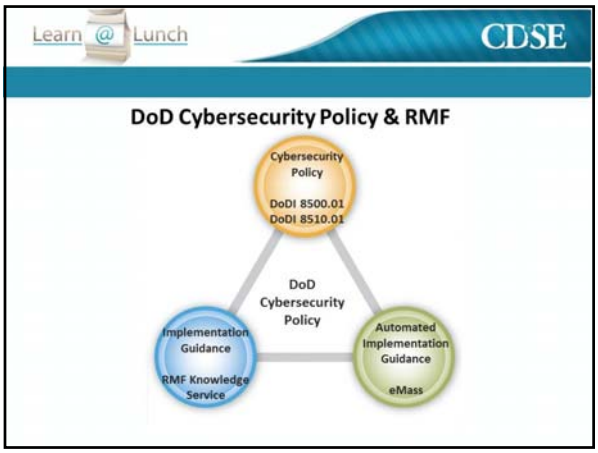
Cybersecurity Defined

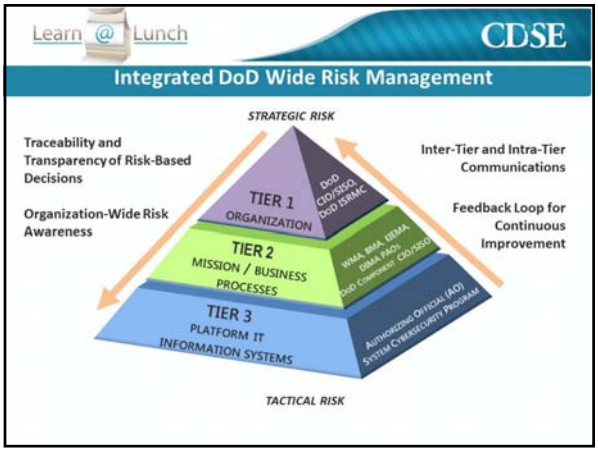
Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.

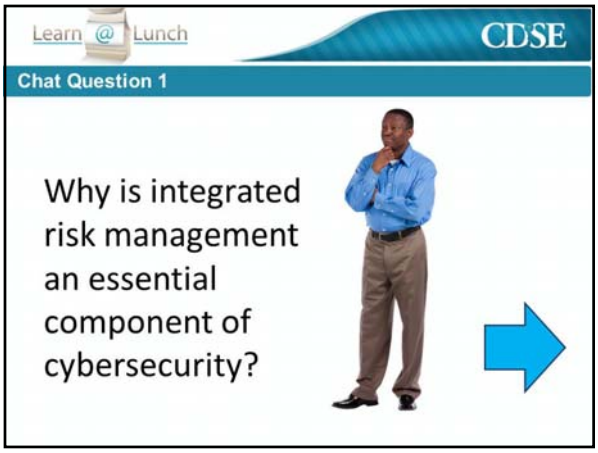

Learn @ Lunch
CDSE
Cybersecurity protects information systems against:
Unauthorized access to or modification of information
Denial of service to authorized users
Cybersecurity includes measures necessary to **protect**, **detect**, **characterize**, **counter**, and **mitigate** unauthorized activities and vulnerabilities.

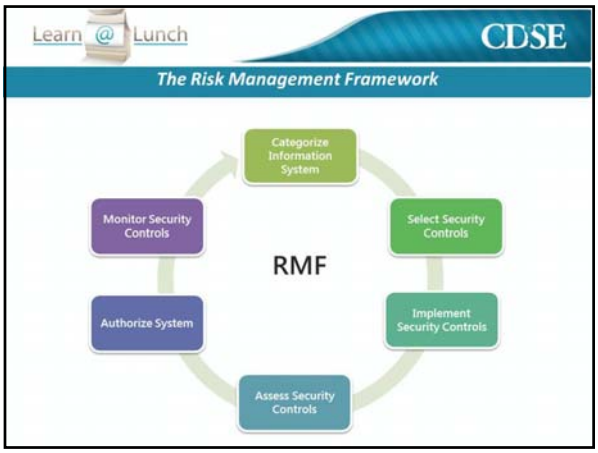

Learn @ Lunch
CDSE
Transformation of IA to Cybersecurity & RMF
DCID 6/3 DIACAP
Joint Task Force Documents
Revised 8500 Series Policies
Transformation Bottom Line – DoD will continue to follow the DoD 8500 series documentation For Cybersecurity policy (formerly Information Assurance)


Learn @ Lunch
CDSE
Policy Alignment
DoD
Intelligence Community
Other Government Agencies
CNSS
Joint Task Force Transformation Initiative
Federal Government
DoD
Intelligence Community
Other Government Agencies
CNSS
NIST Documents
Before
After

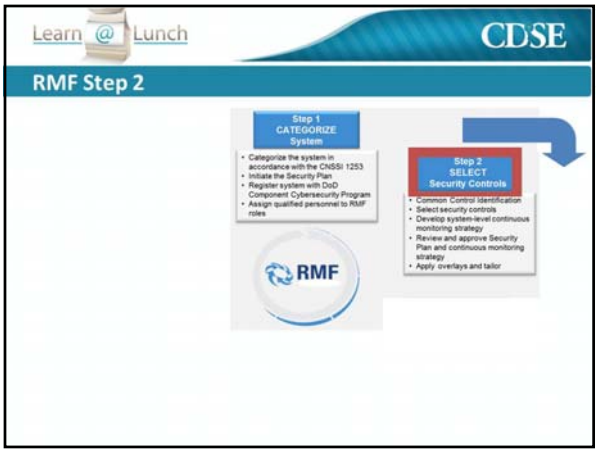

Learn @ Lunch
CDSE
DoD Cybersecurity Policy & RMF
Cybersecurity Policy
DoDI 8500.01
DoDI 8510.01
DoD Cybersecurity Policy
Implementation Guidance
RMF Knowledge Service
Automated Implementation Guidance
eMass

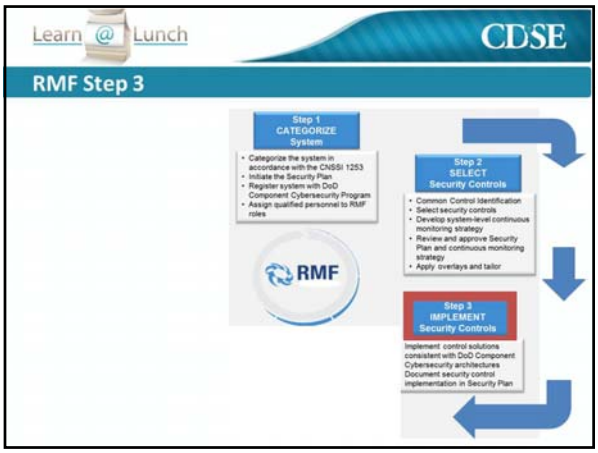

Learn @ Lunch
CDSE
Integrated DoD Wide Risk Management
STRATEGIC RISK
Traceability and Transparency of Risk-Based Decisions
Organization-Wide Risk Awareness
Inter-Tier and Intra-Tier Communications
Feedback Loop for Continuous Improvement
TIER 1
ORGANIZATION
DoD CIO/JSO, DoD ERMC
TIER 2
MISSION / BUSINESS PROCESSES
WMA, BMA, IEMA, DMA PMO
DoD Component CIO/JSCO
TIER 3
PLATFORM IT INFORMATION SYSTEMS
Authorizing Official (AO)
System Cybersecurity Program
TACTICAL RISK

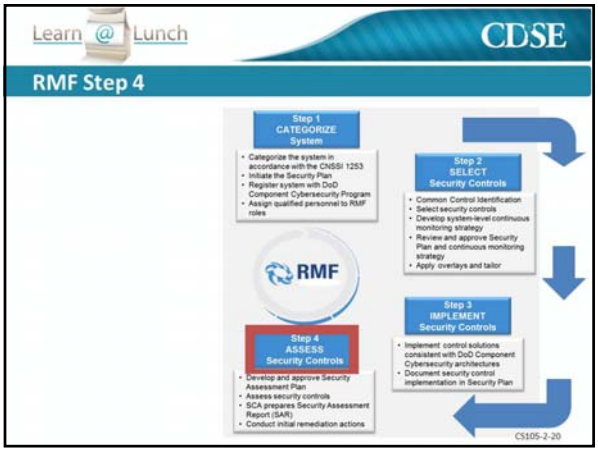

Learn @ Lunch
CDSE
Chat Question 1
Why is integrated risk management an essential component of cybersecurity?

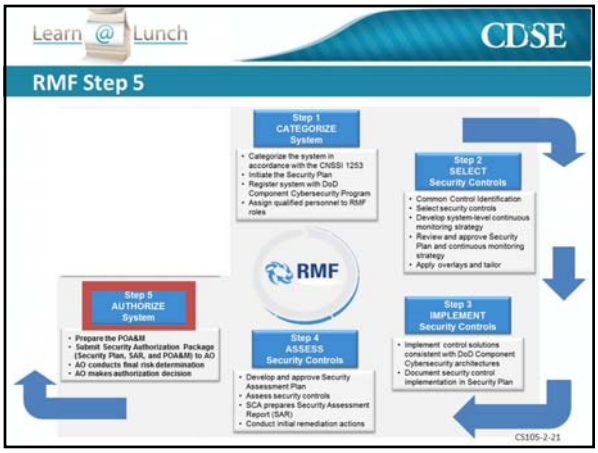

Learn @ Lunch
CDSE
The Risk Management Framework
Categorize Information System
Select Security Controls
Implement Security Controls
Assess Security Controls
Authorize System
Monitor Security Controls
RMF

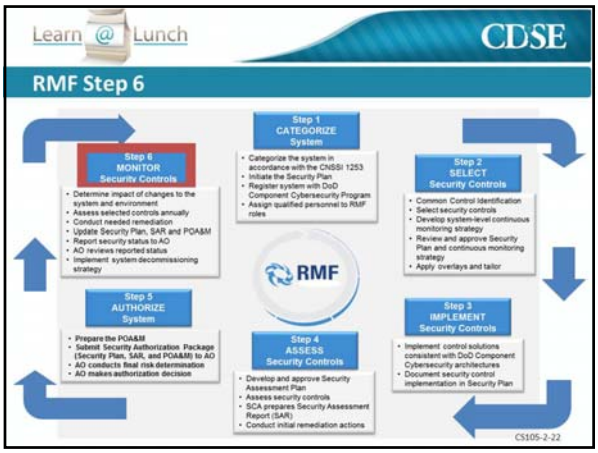
Learn @ Lunch
CDSE
RMF Step 1
Step 1
CATEGORIZE
System
• Categorize the system in accordance with the CNSSI 1253
• Initiate the Security Plan
• Register system with DoD Component Cybersecurity Program
• Assign qualified personnel to RMF roles
RMF

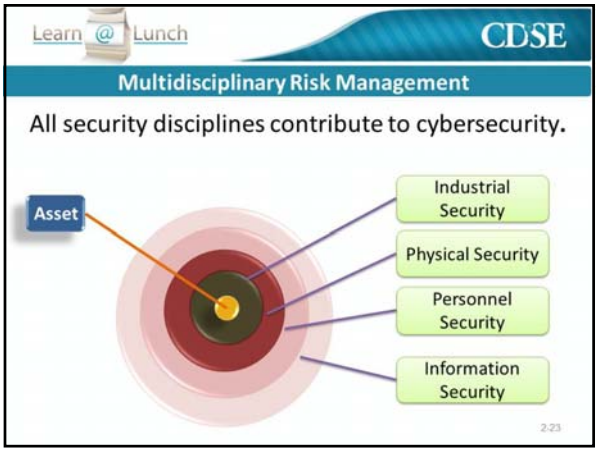

Learn @ Lunch
CDSE
RMF Step 2
Step 1
CATEGORIZE
System
• Categorize the system in accordance with the CNSSI 1253
• Initiate the Security Plan
• Register system with DoD Component Cybersecurity Program
• Assign qualified personnel to RMF roles
RMF
Step 2
SELECT
Security Controls
• Common Control Identification
• Select security controls
• Develop system-level continuous monitoring strategy
• Review and approve Security Plan and continuous monitoring strategy
• Apply overlays and tailor

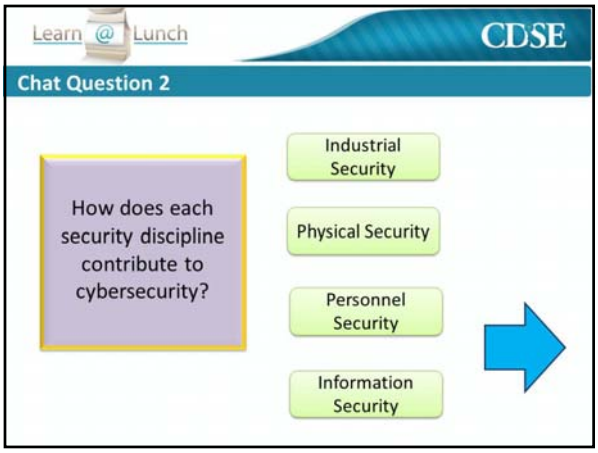

Learn @ Lunch
CDSE
RMF Step 3
Step 1
CATEGORIZE
System
• Categorize the system in accordance with the CNSSI 1253
• Initiate the Security Plan
• Register system with DoD Component Cybersecurity Program
• Assign qualified personnel to RMF roles
Step 2
SELECT
Security Controls
• Common Control Identification
• Select security controls
• Develop system-level continuous monitoring strategy
• Review and approve Security Plan and continuous monitoring strategy
• Apply overlays and tailor
RMF
Step 3
IMPLEMENT
Security Controls
Implement control solutions consistent with DoD Component Cybersecurity architectures
Document security control implementation in Security Plan


Learn @ Lunch
CDSE
RMF Step 4
Step 1
CATEGORIZE
System
• Categorize the system in accordance with the CNSSI 1253
• Initiate the Security Plan
• Register system with DoD Component Cybersecurity Program
• Assign qualified personnel to RMF roles
Step 2
SELECT
Security Controls
• Common Control Identification
• Select security controls
• Develop system-level continuous monitoring strategy
• Review and approve Security Plan and continuous monitoring strategy
• Apply overlays and tailor
RMF
Step 3
IMPLEMENT
Security Controls
• Implement control solutions consistent with DoD Component Cybersecurity architectures
• Document security control implementation in Security Plan
Step 4
ASSESS
Security Controls
• Develop and approve Security Assessment Plan
• Assess security controls
• SCA prepares Security Assessment Report (SAR)
• Conduct initial remediation actions
CS105-2-20


Learn @ Lunch
CDSE
RMF Step 5
Step 1
CATEGORIZE
System
• Categorize the system in accordance with the CNSSI 1253
• Initiate the Security Plan
• Register system with DoD Component Cybersecurity Program
• Assign qualified personnel to RMF roles
Step 2
SELECT
Security Controls
• Common Control Identification
• Select security controls
• Develop system-level continuous monitoring strategy
• Review and approve Security Plan and continuous monitoring strategy
• Apply overlays and tailor
RMF
Step 5
AUTHORIZE
System
• Prepare the POA&M
• Submit Security Authorization Package (Security Plan, SAR, and POA&M) to AO
• AO conducts final risk determination
• AO makes authorization decision
Step 3
IMPLEMENT
Security Controls
• Implement control solutions consistent with DoD Component Cybersecurity architectures
• Document security control implementation in Security Plan
Step 4
ASSESS
Security Controls
• Develop and approve Security Assessment Plan
• Assess security controls
• SCA prepares Security Assessment Report (SAR)
• Conduct initial remediation actions
CS105-2-21


Learn @ Lunch
CDSE
RMF Step 6
Step 1
CATEGORIZE
System
• Categorize the system in accordance with the CNSSI 1253
• Initiate the Security Plan
• Register system with DoD Component Cybersecurity Program
• Assign qualified personnel to RMF roles
Step 2
SELECT
Security Controls
• Common Control Identification
• Select security controls
• Develop system-level continuous monitoring strategy
• Review and approve Security Plan and continuous monitoring strategy
• Apply overlays and tailor
Step 3
IMPLEMENT
Security Controls
• Implement control solutions consistent with DoD Component Cybersecurity architectures
• Document security control implementation in Security Plan
Step 4
ASSESS
Security Controls
• Develop and approve Security Assessment Plan
• Assess security controls
• SCA prepares Security Assessment Report (SAR)
• Conduct initial remediation actions
Step 5
AUTHORIZE
System
• Prepare the POA&M
• Submit Security Authorization Package (Security Plan, SAR, and POA&M) to AO
• AO conducts final risk determination
• AO makes authorization decision
Step 6
MONITOR
Security Controls
• Determine impact of changes to the system and environment
• Assess selected controls annually
• Conduct needed remediation
• Update Security Plan, SAR and POA&M
• Report security status to AO
• AO reviews reported status
• Implement system decommissioning strategy
RMF
CS105-2-22


Learn @ Lunch
CDSE
Multidisciplinary Risk Management
All security disciplines contribute to cybersecurity.
Asset
Industrial Security
Physical Security
Personnel Security
Information Security
2-23


Learn @ Lunch
CDSE
Chat Question 2
How does each security discipline contribute to cybersecurity?
Industrial Security
Physical Security
Personnel Security
Information Security

Learn @ Lunch CDSE

Knowledge Service

To become part of the DoD RMF community of interest, visit the online Knowledge Service:

https://rmfks.osd.mil/rmf

*Access requires a DoD PKI certificate or an ECA PKI certificate

Learn @ Lunch CDSE

Conclusion

The Risk Management Framework provides a holistic solution for managing risk to an organization's information and information systems

Learn @ Lunch CDSE

New Course

Learn @ Lunch CDSE

Questions

Learn @ Lunch CDSE

Cybersecurity Training Products and POC

Past Webinars
- Cyber Insider Threat

All Other Training
- CDSE Cybersecurity

Learn @ Lunch CDSE

Feedback

Before we conclude today's presentation, we hope you'll take a moment to participate in our feedback questionnaire. Your feedback is very helpful to us and is greatly appreciated. If you have ideas for future webinar topics, you can share them in the questionnaire.

0:30