Overview of the NIST SP 800-53 Introductory Courses

Briefing for:
Federal Cybersecurity & Privacy Professionals Forum Meeting
May 21, 2024 (Virtual)

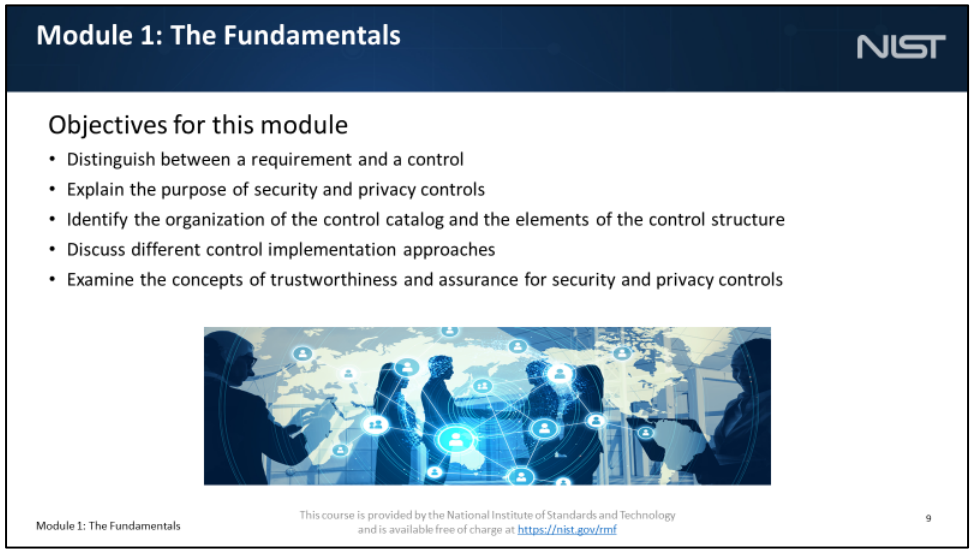
Presented by:
Jeremy Licata (NIST)
NIST Risk Management Framework (RMF) Team
Computer Security Division (CSD)

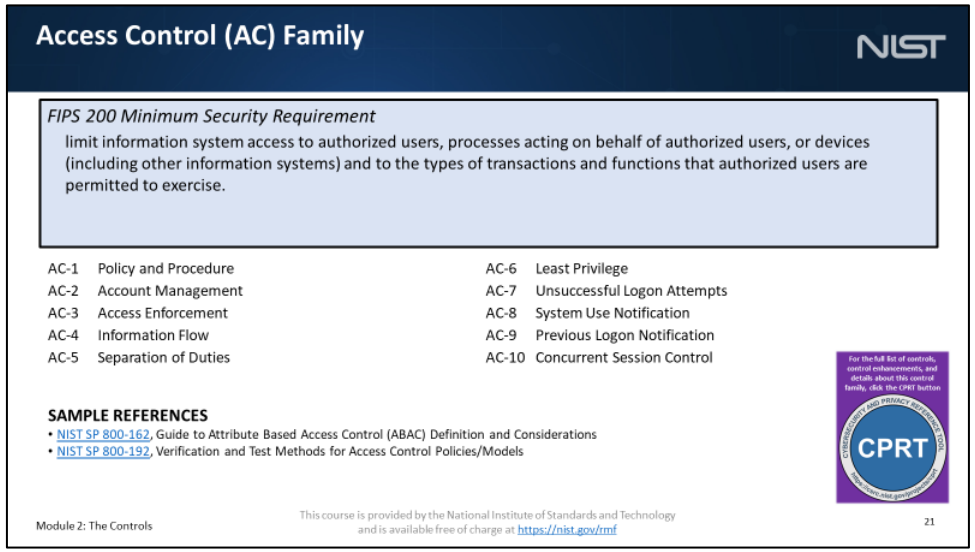
NIST INFORMATION TECHNOLOGY LABORATORY

Security and Privacy Controls

Security and Privacy Controls for Information Systems and Organizations Introductory Course

Based on NIST SP 800-53, *Security and Privacy Controls for Information Systems and Organizations*, explains the concepts of security and privacy controls and introduces the SP 800-53 control catalog

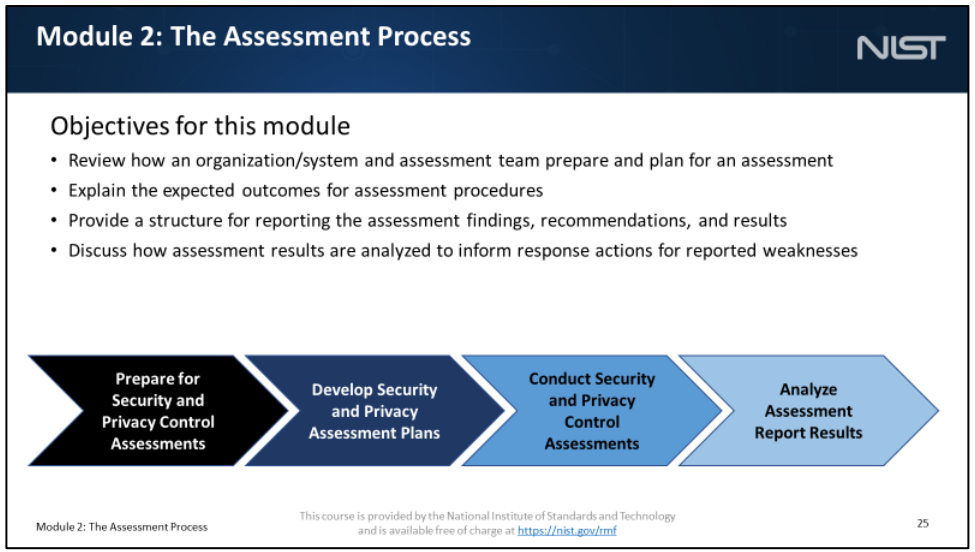


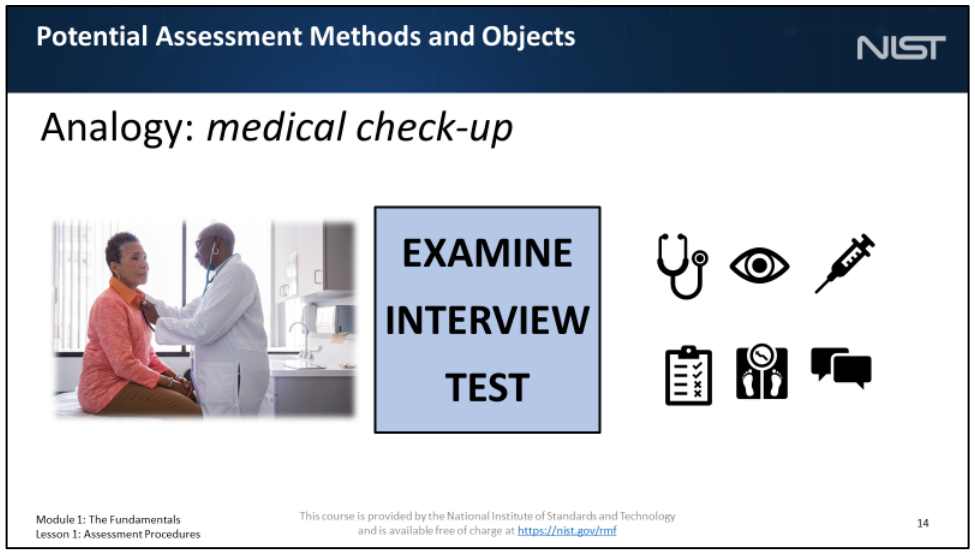


Assessing Security and Privacy Controls

Assessing Security and Privacy Controls in Information Systems and Organizations Introductory Course

Based on NIST SP 800-53A, *Assessing Security and Privacy Controls in Information Systems and Organizations*, explores a methodology and set of procedures for assessing and monitoring the effectiveness of SP 800-53 controls selected and implemented.

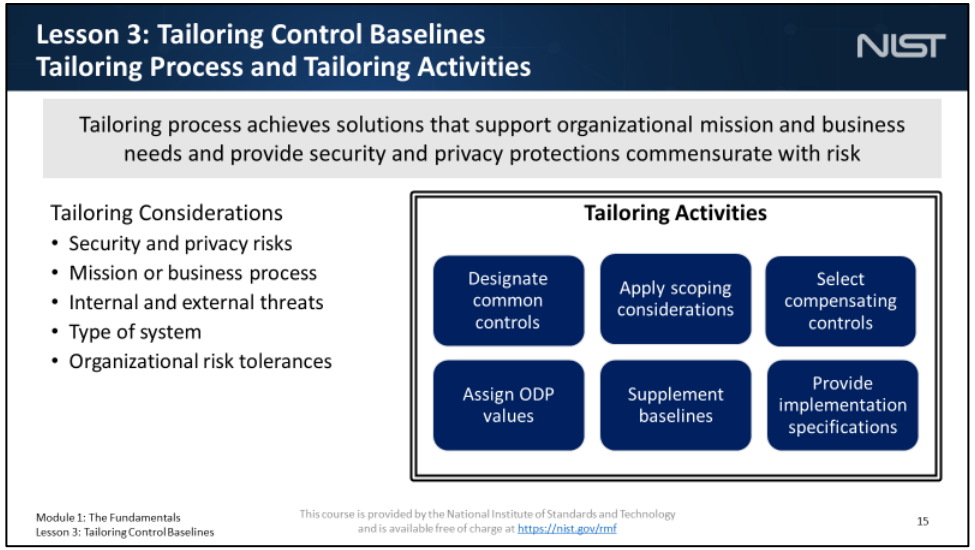


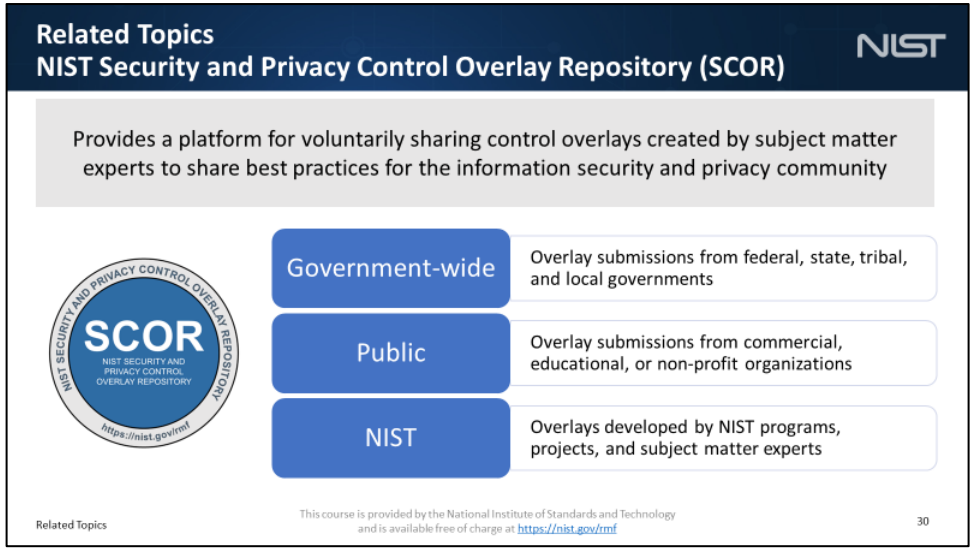


Control Baselines

Control Baselines for Information Systems and Organizations Introductory Course

Based on SP 800-53B, *Control Baselines for Information Systems and Organizations*, provides an overview of the security and privacy control baselines and guidance for tailoring security and privacy control baselines to best support the management of organizational and system risks.





Course Basics

On-demand

- https://csrc.nist.gov/Projects/risk-management/rmf-courses
- Free of charge and no registration required
- Course player viewable on laptops, tablets, and smart phones

Self-paced / Self-guided

- No defined order for completing the courses
- No quizzes -- provided for informational purposes only
- Transcript of the narration is available

Certificate of Completion

- Certificate of course completion is provided as a courtesy
  - Does not attest to any qualifications, knowledge, or skill level
  - NIST does not issue CEC or CPE credits

Course materials

- Organizations may integrate course materials into Awareness and Training program
  - Download PowerPoint presentation
  - Request Learning Management System (LMS) format

Course Access

https://csrc.nist.gov/Projects/risk-management/rmf-courses

Online Introductory Courses

+expand all

- RMF Introductory Course
- Security and Privacy Controls Introductory Course
- Assessing Security and Privacy Controls Introductory Course
- Control Baselines Introductory Course

Frequently Asked Questions

+expand all

- Course Logistics
- Course Topics and Content
- Course Player Technical Issues
- Certificate of Completion / Course Credit
- Course Material Availability
- Software Disclaimer

Security and Privacy Controls Introductory Course

NIST SP 800-53, Security and Privacy Controls for Information Systems and Organizations

NIST SP 800-53 provides a comprehensive catalog of outcome-based security and privacy controls. The controls can be implemented in organizations of all types and sizes, as well as any type of system. The controls provide the safeguards to protect the confidentiality, integrity, and available of the systems and information, and manage privacy risks.

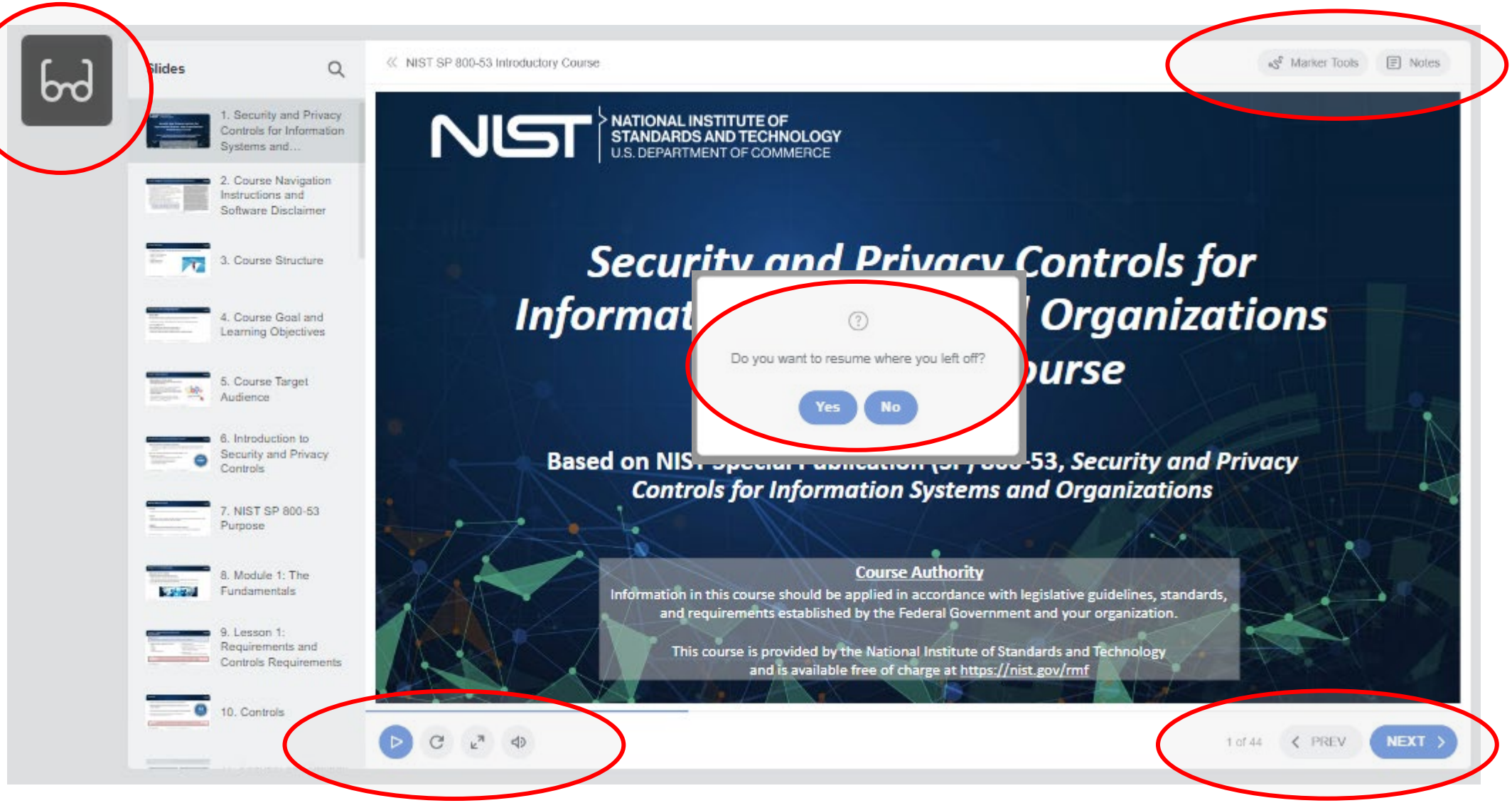
This course introduces the structure and organization of the security and privacy controls in Revision 5 of the catalog. It also describes key considerations for the implementation of controls as part of an organization-wide risk management program.

Course Duration: ONE Hour

Launch SP 800-53 Introductory Course

Download SP 800-53 Introductory Course Slides

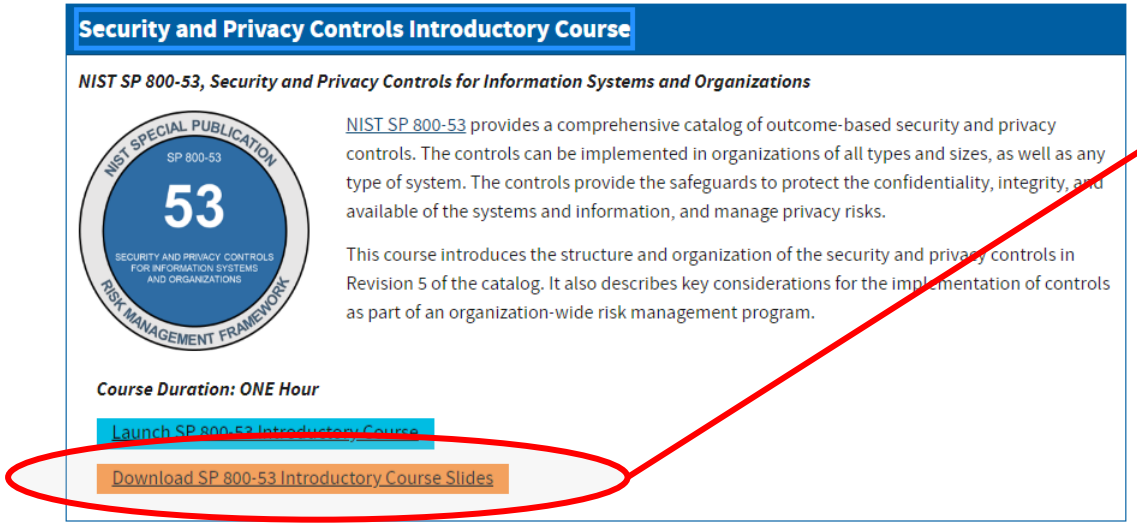
Online Course Interface

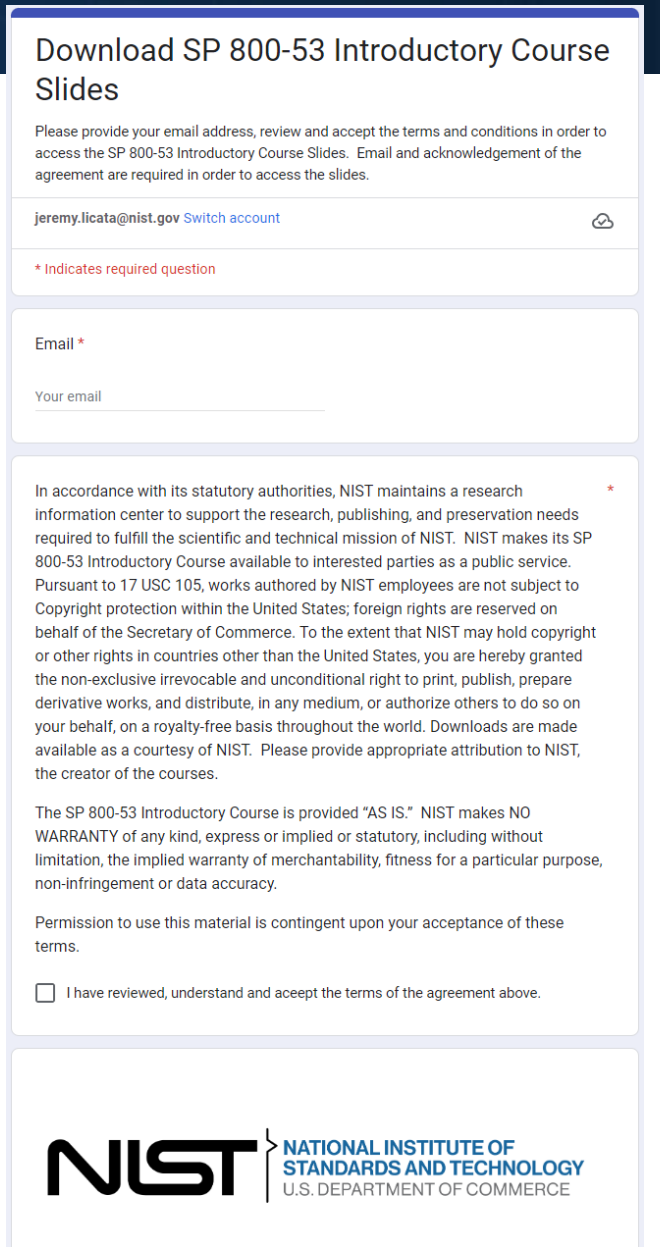


Requesting the Course Materials

Downloadable version (PowerPoint)

- Does not include the certificate of completion
- Users must review and agree to the terms of use for each course.





Requesting the Course Materials

If you are unable to access the Google Form to access the terms of use

- Download and submit the PDF form and submit to sec-cert@nist.gov
- *Please allow up to 5 business days for response if you submit the PDF form*

Learning Management System (LMS) formats

- The narrated course content is available in AICC, cmi5, Experience API (xAPI), and SCORM (1.2, 2004)
- Submit request to sec-cert@nist.gov with course(s) requested, format requested, and a valid email address for receiving the requested material

Thank You

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Backup Slides

Risk Management Framework

Security and Privacy Controls for Information Systems and Organizations Introductory Course

Based on NIST SP 800-37, *Risk Management Framework (RMF) for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, provides an overview of a methodology for managing organizational risk

Course Structure

Completing the entire course should take approximately 3 hours. The breakdown in time for each module is as follows:

- **Welcome and Overview (9 minutes)**
- **Module 1: Federal Legislation and Policy (8 minutes)**
- **Module 2: NIST Special Publication 800-37 Background and Update Overview (10 minutes)**
- **Module 3: The Fundamentals (75 minutes)**
  - Lesson 1: Organization-wide Risk Management
  - Lesson 2: Risk Management Framework Steps and Structure
  - Lesson 3: Information Security and Privacy in the RMF
  - Lesson 4: System and System Elements
  - Lesson 5: Authorization Boundaries
  - Lesson 6: Authorization Types and Decisions
  - Lesson 7: Requirements and Controls
  - Lesson 8: Security and Privacy Posture
  - Lesson 9: Supply Chain Risk Management
  - Lesson 10: Risk Management Roles and Responsibilities
- **Module 4: The Risk Management Framework (59 minutes)**
  - Lesson 1: Overview of the Risk Management Framework
  - Lesson 2: Risk Management Framework Steps
- **Conclusion and Contact Information (3 minutes)**

Lesson 2: Risk Management Framework Steps

Organizations are expected to execute all steps and tasks in the RMF. Organizations have significant flexibility in how the RMF steps and tasks are carried out, if applicable requirements are met, and security and privacy risk is managed.

- There are seven steps in the RMF: a preparatory step to ensure that organizations are ready to execute the process and six main steps
- The RMF Steps are listed in sequential order, but the steps following the **Prepare** step can be carried out in a nonsequential order