

# 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)

DISCLAIMER: any mention of entities, equipment, materials, or services throughout this talk is for information only; it does not imply recommendation or endorsement by NIST, nor is it intended to imply best available solution for any given purpose.



# 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

### Module 1: The Fundamentals



#### Objectives for this module

- Distinguish between a requirement and a control
- Explain the purpose of security and privacy controls
- Identify the organization of the control catalog and the elements of the control structure
- Discuss different control implementation approaches
- Examine the concepts of trustworthiness and assurance for security and privacy controls



Module 1: The Fundamentals

This course is provided by the National Institute of Standards and Technology and is available free of charge at <https://nist.gov/rmf>

9

### Access Control (AC) Family



#### FIPS 200 Minimum Security Requirement

limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.

AC-1 Policy and Procedure	AC-6 Least Privilege
AC-2 Account Management	AC-7 Unsuccessful Logon Attempts
AC-3 Access Enforcement	AC-8 System Use Notification
AC-4 Information Flow	AC-9 Previous Logon Notification
AC-5 Separation of Duties	AC-10 Concurrent Session Control

#### SAMPLE REFERENCES

- [NIST SP 800-162](#), Guide to Attribute Based Access Control (ABAC) Definition and Considerations
- [NIST SP 800-192](#), Verification and Test Methods for Access Control Policies/Models



Module 2: The Controls

This course is provided by the National Institute of Standards and Technology and is available free of charge at <https://nist.gov/rmf>

21



# 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.

**Module 2: The Assessment Process**

Objectives for this module

- Review how an organization/system and assessment team prepare and plan for an assessment
- Explain the expected outcomes for assessment procedures
- Provide a structure for reporting the assessment findings, recommendations, and results
- Discuss how assessment results are analyzed to inform response actions for reported weaknesses

Module 2: The Assessment Process

This course is provided by the National Institute of Standards and Technology and is available free of charge at <https://nist.gov/rmf>

25

**Potential Assessment Methods and Objects**

Analogy: *medical check-up*

**EXAMINE  
INTERVIEW  
TEST**

Module 1: The Fundamentals  
Lesson 1: Assessment Procedures

This course is provided by the National Institute of Standards and Technology and is available free of charge at <https://nist.gov/rmf>

14




# 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.

**Lesson 3: Tailoring Control Baselines**  
**Tailoring Process and Tailoring Activities**

Tailoring process achieves solutions that support organizational mission and business needs and provide security and privacy protections commensurate with risk

**Tailoring Considerations**

- Security and privacy risks
- Mission or business process
- Internal and external threats
- Type of system
- Organizational risk tolerances


**Tailoring Activities**

Designate common controls	Apply scoping considerations	Select compensating controls
Assign ODP values	Supplement baselines	Provide implementation specifications


Module 1: The Fundamentals  
Lesson 3: Tailoring Control Baselines

This course is provided by the National Institute of Standards and Technology and is available free of charge at <https://nist.gov/rmf>

15

**Related Topics**  
**NIST Security and Privacy Control Overlay Repository (SCOR)**

Provides a platform for voluntarily sharing control overlays created by subject matter experts to share best practices for the information security and privacy community



<b>Government-wide</b>	Overlay submissions from federal, state, tribal, and local governments
<b>Public</b>	Overlay submissions from commercial, educational, or non-profit organizations
<b>NIST</b>	Overlays developed by NIST programs, projects, and subject matter experts

Related Topics

This course is provided by the National Institute of Standards and Technology and is available free of charge at <https://nist.gov/rmf>

30



## 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 availability 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

The screenshot displays the NIST SP 800-53 Introductory Course interface. The interface is divided into several sections:

- Top Left:** A red circle highlights a dark square icon with white glasses.
- Top Right:** A red circle highlights the "Marker Tools" and "Notes" buttons.
- Left Sidebar:** A list of 10 slides is visible, including "1. Security and Privacy Controls for Information Systems and...", "2. Course Navigation Instructions and Software Disclaimer", "3. Course Structure", "4. Course Goal and Learning Objectives", "5. Course Target Audience", "6. Introduction to Security and Privacy Controls", "7. NIST SP 800-53 Purpose", "8. Module 1: The Fundamentals", "9. Lesson 1: Requirements and Controls Requirements", and "10. Controls".
- Main Content Area:** The slide content includes the NIST logo, the title "Security and Privacy Controls for Information Systems and Organizations", and a subtitle "Based on NIST Special Publication (SP) 800-53, Security and Privacy Controls for Information Systems and Organizations". A red circle highlights a dialog box asking "Do you want to resume where you left off?" with "Yes" and "No" buttons. Another red circle highlights a "Course Authority" section stating: "Information in this course should be applied in accordance with legislative guidelines, standards, and requirements established by the Federal Government and your organization. This course is provided by the National Institute of Standards and Technology and is available free of charge at <https://nist.gov/rmf>".
- Bottom Left:** A red circle highlights a set of navigation controls including play, refresh, and volume icons.
- Bottom Right:** A red circle highlights the slide navigation controls showing "1 of 44", "PREV", and "NEXT" buttons.


# 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.

**Security and Privacy Controls Introductory Course**

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



**53**  
SECURITY AND PRIVACY CONTROLS  
FOR INFORMATION SYSTEMS  
AND ORGANIZATIONS  
RISK MANAGEMENT FRAMEWORK

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 availability 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](#)

### Download SP 800-53 Introductory Course Slides

Please provide your email address, review and accept the terms and conditions in order to access the SP 800-53 Introductory Course Slides. Email and acknowledgement of the agreement are required in order to access the slides.

jeremy.licata@nist.gov [Switch account](#)

\* Indicates required question

Email \*

Your email

In accordance with its statutory authorities, NIST maintains a research information center to support the research, publishing, and preservation needs required to fulfill the scientific and technical mission of NIST. NIST makes its SP 800-53 Introductory Course available to interested parties as a public service. Pursuant to 17 USC 105, works authored by NIST employees are not subject to Copyright protection within the United States; foreign rights are reserved on behalf of the Secretary of Commerce. To the extent that NIST may hold copyright or other rights in countries other than the United States, you are hereby granted the non-exclusive irrevocable and unconditional right to print, publish, prepare derivative works, and distribute, in any medium, or authorize others to do so on your behalf, on a royalty-free basis throughout the world. Downloads are made available as a courtesy of NIST. Please provide appropriate attribution to NIST, the creator of the courses.

The SP 800-53 Introductory Course is provided "AS IS." NIST makes NO WARRANTY of any kind, express or implied or statutory, including without limitation, the implied warranty of merchantability, fitness for a particular purpose, non-infringement or data accuracy.

Permission to use this material is contingent upon your acceptance of these terms.

☐ I have reviewed, understand and accept the terms of the agreement above.



# 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](mailto: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](mailto:sec-cert@nist.gov) with course(s) requested, format requested, and a valid email address for receiving the requested material

# Thank You



# 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

