
FISMA training
by SECOND RENAISSANCE

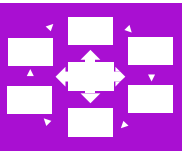
Organization

Logistics 

Navigating the course, technology, and materials

Legislation & Guidance 

Public Law and NIST-published Guidance

Risk Management Framework 

Phases of the Risk Management Framework, used as the methodology for addressing FISMA and managing cybersecurity best practices

Supplemental Information 

Procedures and activities related to the Risk Management Framework, FISMA, and cybersecurity best practices

Day 1 Agenda

Item No.	Topic	Start	End
1.1	Introduction & Logistics	9:00am	9:20am
1.2	FISMA Overview	9:20am	10:15am
	15 Minute Break	10:15am	10:30am
1.3	NIST Overview	10:30am	11:30am
	Lunch Break	11:30am	12:30pm
1.4	Risk Management Framework	12:30pm	2:30pm
	15 Minute Break	2:30pm	2:45pm
1.5	Security Roles	2:45pm	3:45pm
1.6	Daily Review	3:45pm	4:00pm
1.1	Introduction & Logistics	9:00am	9:20am
1.2	FISMA Overview	9:20am	10:15am

Day 2 Agenda

Item No.	Topic	Start	End
2.7	Daily Agenda	9:00am	9:05am
2.8	Step 0: Prepare	9:05am	10:00am
2.9	Information System Inventory	10:00am	10:30am
	15 Minute Break	10:30am	10:45am
2.10	Step 1: Categorize	10:45am	11:00am
2.11	FIPS 199, E-Auth, PIA	11:00am	12:30pm
	Lunch Break	12:30pm	1:30pm
2.12	Step 2: Select	1:30pm	2:30pm
	15 Minute Break	2:30pm	2:45pm
2.13	FedRAMP & Cloud	2:45pm	3:15pm
2.14	CDM Program	3:15pm	3:45pm
2.15	Daily Review	3:45pm	4:00pm

Day 3 Agenda

Item No.	Topic	Start	End
3.16	Daily Agenda	9:00am	9:05am
3.17	800-53 Overview	9:05am	10:05am
	15 Minute Break	10:05am	10:20am
3.18	Control Families	10:20am	12:00pm
	Lunch Break	12:00pm	1:00pm
3.19	Step 3: Implement	1:00pm	1:20pm
3.20	Writing an SP	1:20pm	2:20pm
	15 Minute Break	2:20pm	2:35pm
3.21	Step 4: Assess	2:35pm	3:15pm
3.22	Step 5: Authorize	3:15pm	3:45pm
3.23	Daily Review	3:45pm	4:00pm

Day 4 Agenda

Item No.	Topic	Start	End
4.24	Daily Agenda	9:00am	9:05am
4.25	Step 6: Continuous Monitoring	9:05am	9:35am
	15 Minute Break	9:35am	9:50am
4.26	Contingency Planning	9:50am	10:30am
4.27	Change Control	10:30am	11:00pm
4.28	Vulnerability Scanning	11:00am	12:00pm
	Lunch Break	12:00pm	1:00pm
4.29	POA&Ms	1:00pm	1:45pm
	15 Minute Break	1:45pm	2:00pm
4.30	Event Monitoring and IR	2:00pm	2:45pm
4.31	Daily Review	2:45pm	3:00pm
4.32	Course Review & Quiz	3:00pm	4:00pm

Overview of NIST

FISMAtraining

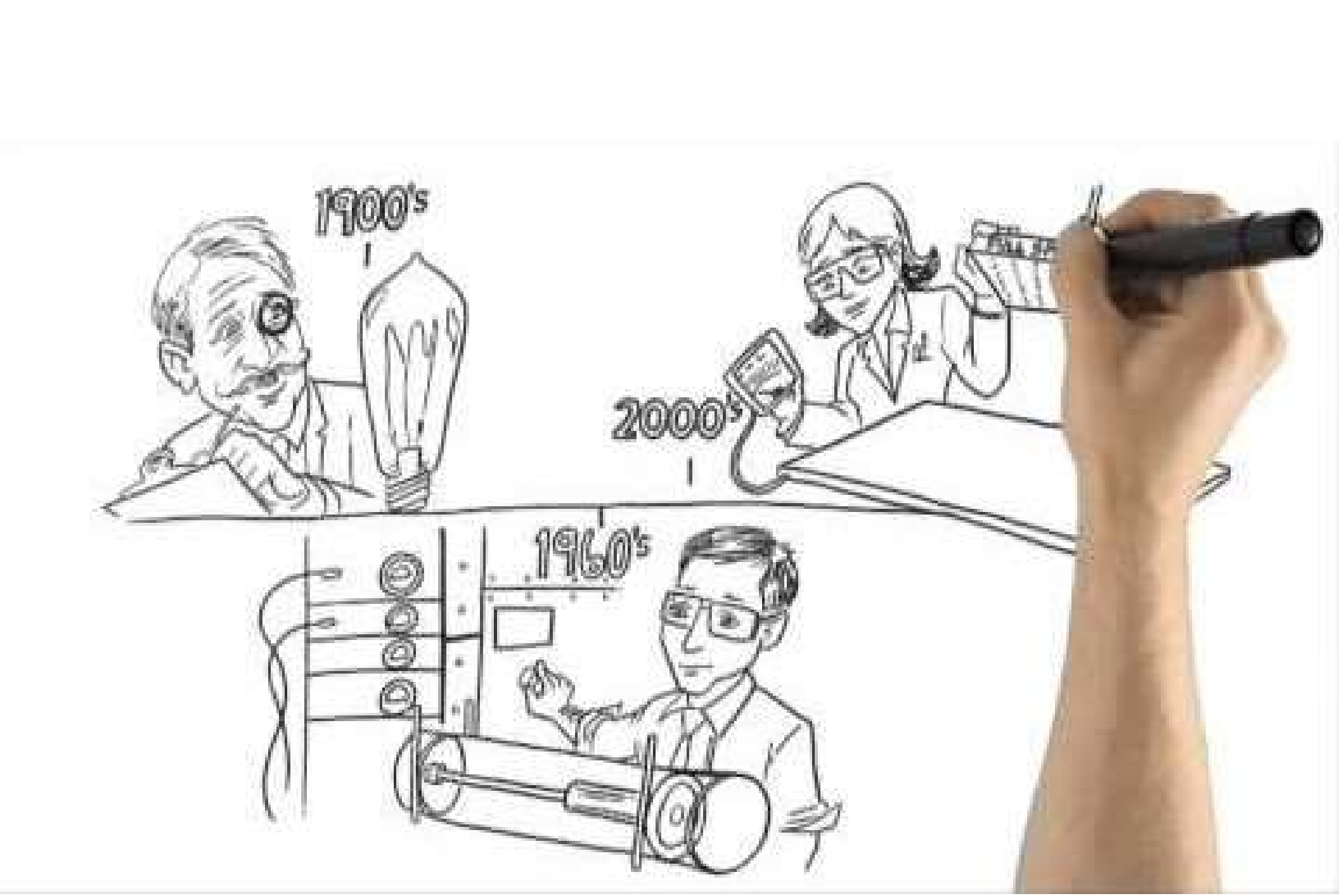
by SECOND RENAISSANCE

Agenda

- What is NIST
- How are they organized
- Types of guidance
- Resources beyond SPs
  - NVD
  - SCAP
  - Controls database
  - Configuration guides

Objective

- Understand the basic purpose and structure of NIST guidance, and its relevance to FISMA


1900's
2000's
1960's

NIST

- National Institute of Standards and Technology
- Founded in 1901 as the National Bureau of Standards
- NIST is a NON-regulatory federal organization within the Department of Commerce
- NIST's Mission - To promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life. (see www.nist.gov)
- Information Technology Lab/Computer Security Division

Relationship Between FISMA and NIST

- FISMA – Federal Information Security Management Act
  - Law enacted by Congress - part of the E-Gov Act of 2002
  - Applies to federal organizations and their contractors
  - Requires implementation of "information security protections commensurate with the risk and magnitude of the harm"
- NIST – National Institute of Standards and Technology
  - FISMA requires NIST to develop standards and guidelines to help federal organizations improve the security of federal information and information systems (and implement FISMA)
  - NIST publications – http://csrc.nist.gov/publications

Directives and NIST

- OMB – Office of Management and Budget
  - Directives in the form of Memos and Circulars (usually)
  - May mandate NIST guidance for use by federal organizations
- EOs and PDs – Executive Orders and Presidential Directives
  - Directives from the Executive Office of the President
  - May direct NIST to provide guidance or develop a standard
- HSPD – Homeland Security Presidential Directive
  - An Executive Order focused on ensuring homeland security with implementation usually managed by DHS
  - Example: HSPD-12 which calls for a common ID standard for federal employees and contractors

NIST/ITL/CSD Types of Publications

- Federal Information Processing Standards (FIPS)
  - Signed/approved by the Secretary of Commerce
  - FISMA made FIPS mandatory for federal organizations
- Special Publications (SPs)
  - Providing guidance to federal organizations on information technology security since 1990
  - Are not mandatory for use
- NIST Interagency Reports (NISTIRs)
  - Describe research of a technical nature to a specialized audience
- See them all at http://csrc.nist.gov

NIST/ITL/CSD Public Comment Process

- All publications produced by CSD go through the public comment process
- Receive notifications of newly posted drafts (and more) by subscribing at http://csrc.nist.gov/publications/subscribe.html
- Drafts are published at http://csrc.nist.gov/publications/PubsDrafts.html
- Lengths of public comment periods vary

Joint Task Force Transformation Initiative

A Broad-Based Partnership —

- National Institute of Standards and Technology
- Department of Defense
- Intelligence Community
  - Office of the Director of National Intelligence
  - 16 U.S. Intelligence Agencies
- Committee on National Security Systems

Standards/Guidelines for FISMA & RM

- FIPS - Federal Information Processing Standards
  - FIPS 199 – Standards for Security Categorization
  - FIPS 200 – Minimum Security Requirements
- SPs – Special Publications
  - SP 800-18 – Guide for System Security Plan development
  - SP 800-30 – Guide for Conducting Risk Assessments
  - SP 800-34 – Guide for Contingency Plan development
  - SP 800-37 – Guide for Applying the Risk Management Framework
  - SP 800-39 – Managing Information Security Risk
  - SP 800-53/53A – Security controls catalog/assessment procedures
  - SP 800-60 – Mapping Information Types to Security Categories
  - SP 800-128 – Security-focused Configuration Management
  - SP 800-137 – Information Security Continuous Monitoring
  - Many others for operational and technical implementations

NIST Resources

National Vulnerability Database

- Universal identifiers for application and OS vulnerabilities

- https://nvd.nist.gov/

Security Content Automation Protocol (SCAP)

- Standard for interoperability of cybersecurity tools

- https://csrc.nist.gov/projects/security-content-automation-protocol

800-53 Controls Database

- Searchable and exportable (CSV, XML) controls

- https://nvd.nist.gov/800-53

USGCB and NCP

- Application and OS hardening configuration guidance through:
  - United States Government Configuration Baseline
  - National Checklist Repository

- https://csrc.nist.gov/projects/united-states-government-configuration-baseline
- https://nvd.nist.gov/ncp/repository

Summary

- NIST is a non-regulatory federal organization within the Department of Commerce that promotes innovation by advancing measurement science, standards, and technology
- NIST sets guidance for securing information systems
- NIST is open to collaboration, and runs task forces and working groups to expand participation
- There are several resources beyond SPs that can be leveraged regularly, like the NVD

FISMAtraining is a 4-day cybersecurity bootcamp by Second Renaissance. For more information on the program and material, contact info@secondrenaissanceinc.com.

FISMAtraining

by SECOND RENAISSANCE