INFOSEC Skills
LIVE BOOT CAMPS

Get live, expert instruction from anywhere.

Risk Management Framework (RMF) Boot Camp

Infosec's Risk Management Framework (RMF) Boot Camp is a four-day course in which you delve into the IT system authorization process and gain an understanding of the Risk Management Framework.

Course description

Infosec offers the most in-depth course available for students looking to learn about the Risk Management Framework for information technology. Risk Management Framework (RMF) describes the process for identifying, implementing, assessing and managing cybersecurity capabilities and services, expressed as security controls and authorizing the operation of information technology systems.

RMF brings a risk-based approach to the implementation of cybersecurity, supports cybersecurity integration early and throughout the system life cycle, promotes reciprocity to the maximum extent possible and stresses continuous monitoring. RMF replaces the DoD Information Assurance Certification and Accreditation Process (DIACAP) and adopts the term cybersecurity in place of information assurance.

Who should attend

The Risk Management Framework (RMF) Boot Camp is meant for IT-focused employees and contractors and their supporting vendors and service providers.

Boot camp at a glance

What you'll learn

- Risk Management Framework for DoD IT authorization process
- Key roles, responsibilities and regulatory requirements
- How to apply principles to real-world situations

Delivery methods

- Online
- In person
- Team onsite

Training duration

- Immediate access to Infosec Skills
- 4-day boot camp
- 90-day extended access to all boot camp materials

The hands-on cybersecurity training platform that moves as fast as you do

Infosec Skills boot camps are engineered to match the way today's cybersecurity professionals prefer to learn. In addition to days of live training from an experienced pro, you'll get unlimited access to 100s of additional hands-on cybersecurity courses and cyber ranges to help you advance your skills before, during and after your boot camp. Your Infosec Skills access extends 90 days past your boot camp, so you can take additional time to prepare for your exam, or get a head start on your next certification goal.

Start training immediately

Prepare for your boot camp with immediate access to the Infosec Skills on-demand training library.

Learn by doing in the cyber range

Put what you've learned into practice with 100s of browser-based labs and hands-on projects.

Get unlimited custom practice exams

Uncover knowledge gaps with unlimited practice exams attempts and skill assessments.

700+ IT and security courses

Earn CPEs and build new skills with 100s of additional training courses.

What's included

- Four days of expert, live DOD RMF training
- 100% Satisfaction Guarantee
- Free 90-day Infosec Skills subscription (access to 1,400+ additional courses and labs)
- 90-day extended access to all boot camp video replays and materials
- Knowledge Transfer Guarantee

Benefits and goals

This boot camp blends lecture, discussion and hands-on exercises to educate you about RMF methodology. You'll leave prepared to implement the Risk Management Framework for your IT systems as prescribed in the updated NIST series of publications.

You'll learn the RMF process and methodology for categorizing information systems, selecting and implementing applicable security controls, and establishing a Continuous Monitoring program. This boot camp breaks down the RMF into steps, tasks, outputs and responsible entities and includes informative lectures, discussions and exercises. These sessions will provide a functional understanding of cybersecurity and risk management and the proper selection, implementation and validation of the new security controls as outlined on the RMF Knowledge Service and corresponding NIST Special Publications.

Boot camp objectives

After completing Infosec's DoD RMF Boot Camp, you will be able to:

- Understand the Risk Management Framework for DoD IT authorization process
- Understand FISMA and NIST processes for authorizing Federal IT systems
- Explain key roles and responsibilities
- Explain statutory and regulatory requirements
- Apply these principles to real-world activities and situations
- Learn from experts

Learn from experts

We don't just have great instructors, our instructors have years of industry experience and are recognized as experts. Over the past 15 years, we've helped tens of thousands of students get certified and advance their careers.

Skill up and get certified, guaranteed

100% Satisfaction Guarantee

If you're not 100% satisfied with your training at the end of the first day, you may withdraw and enroll in a different online or in-person course.

Knowledge Transfer Guarantee

If an employee leaves within three months of obtaining certification, Infosec will train a different employee for free for up to one year.

What our students are saying

I really appreciate that our instructor was extremely knowledgeable and was able to provide the information in a way that it could be understood. He also provided valuable test-taking strategies that I know not only helped me with this exam, but will help in all exams I take in the future.

Michelle Jemmott
Pentagon

Excellent! Our instructor had a vast background and related the materials to real life. Much better than just teaching the materials to pass an exam … but he did that as well. He went out of his way in class. The extra materials really benefited us when we returned to our real jobs! Great experience!

John Peck
EPA

Very impressed with Infosec. My instructor did a great job delivering the information strategically and in a way for all to understand. I would definitely take another class/certification prep course.

Sylvia Swinson
Texeltek

The instructor was able to take material that prior to the class had made no sense, and explained it in real-world scenarios that were able to be understood.

Erik Heiss
United States Air Force

The course was extremely helpful and provided exactly what we needed to know in order to successfully navigate the exam. Without this I am not confident I would have passed.

Robert Caldwell
Salient Federal Solutions

RMF Boot Camp details

Our instructors give you 100% of their time and dedication to ensure that your time is well spent. You receive an immersive experience with no distractions! The typical daily schedule is:

	Day 1	Day 2	Day 3	Day 4
Morning session	Introduction Legal and regulatory organizations	System development life cycle	RMF phase overview	RMF phase overview (cont)
Afternoon session	Integrated organizational-wide risk management	RMF key roles and responsibilities	RMF phase overview (cont)	RMF review
Evening session	Optional group & individual study	Optional group & individual study	Optional group & individual study	

Schedule may vary from class to class

Before your boot camp

Start learning now. You'll get immediate access to all the content in Infosec Skills, including an in-depth RMF prep course, the moment you enroll. Prepare for your live boot camp, uncover your knowledge gaps and maximize your training experience.

During your boot camp

Legal and regulatory organizations

- White House (Executive Orders)
- NIST (National Institute of Standards and Technology)
- OMB (Office of Management and Budget)
- CNSS (Committee of National Security Systems)

Laws, policies and regulations

- Privacy Act
- Computer Fraud & Abuse Act (CFAA)
- Electronic Communications Privacy Act (ECPA)
- Computer Security Act
- Information Technology Management Reform Act
- Clinger-Cohen Act
- USA PATRIOT ACT
- Federal Information Security Management Act (FISMA)
- Federal Information Security Modernization Act (FISMA)
- Other laws (GLBA, SOX, HIPAA, HITECH)

Integrated organizational-wide risk management

- Categories of business risk
- Overview of risk management
- Risk management objectives
- Potential risk impacts
- Potential security impacts

- Risk assessment process
- Risk assessment steps
  - Prepare
  - Conduct
  - Report and communicate
  - Maintain

System development life cycle

RMF key roles and responsibilities

- Authorizing official/DAA
- AO designated representative
- Chief information officer
- Senior agency information security officer
- Information system owner
- Program manager
- Common control provider
- Information owner or steward
- Information system security manager
- Information system security officer
- Information security architect
- Information system security engineer
- Control assessor, aka third-party assessment organization (3PAO)
- System user

RMF phase overview

- Security authorization process
  - Organization level
  - System level
- Prepare
  - Risk management roles
  - Risk management strategy
  - Risk assessment — organization
  - Organizationally-tailored control baselines and cybersecurity framework profiles (optional)
  - Common control identification
  - Impact-level prioritization (optional)
  - Continuous monitoring strategy — organization
  - Mission or business focus
  - System stakeholders
  - Asset identification
  - Authorization boundary
  - Information types
  - Information life cycle
  - Risk assessment — system
  - Requirements definition
  - Enterprise architecture
  - Requirements allocation
  - System registration
- Categorization
  - System description
  - Security categorization
  - Security categorization review and approval
- Selection
  - Control selection
  - Control tailoring
  - Control allocation
  - Documentation of planned control implementations
  - Continuous monitoring strategy — system
  - Plan review and approval
- Implementation
  - Control implementation
  - Update control implementation information
- Assessment
  - Assessor selection
  - Assessment plan
  - Control assessments
  - Assessment reports
  - Remediation actions
  - Plan of action and milestones
- Authorization
  - Authorization package
  - Risk analysis and determination
  - Risk response

- Authorization decision
- Authorization reporting

- Monitoring
  - System and environment changes
  - Ongoing assessments
  - Ongoing risk response
  - Authorization package updates
  - Security and privacy reporting
  - Ongoing authorization
  - System disposal

After your boot camp

Your Infosec Skills access extends 90 days past your boot camp, so you can take additional time to prepare for your exam, get a head start on your next certification goal or start earning CPEs.

About Infosec

Infosec's mission is to put people at the center of cybersecurity. We help IT and security professionals advance their careers with skills development and certifications while empowering all employees with security awareness and phishing training to stay cyber-safe at work and home. Learn more at infosecinstitute.com.

INFOSEC