

Risk Management Framework (RMF) for Federal Systems In-Depth 4 Day

SecureNinja (4) four day Federal Information Security Management Act (FISMA) training provides students with a fundamental knowledge of the requirements for meeting FISMA requirements, as well as an in-depth look of the Federal system authorization process and Risk Management Framework (RMF). This training equips the students with an in-depth indoctrination into the RMF and they will learn the requirements for managing risk, and ensuring that the confidentiality, availability and integrity of federal information and information systems is protected at a level commensurate with the security requirements of the information and the information system. Students will participate in a series of scenario-based hands-on exercises to enhance understanding of the processes used for system authorization, including all of the elements of the Risk Management Framework. These exercises will include the development of Systems Security Plans (SSPs), Security Assessment Reports (SARs), and Plans Of Action and Milestones (POA&Ms) for Federal Information Systems. This training is a CNSS approved course that deals with the new C&A transformation. Please note - this course has been aligned with NIST SP 800-37 Revision 1 and is the new process under the C&A transformation.

The FISMA In-Depth Course covers the requirements and the use of FIPS 199, NIST SP 800-60, NIST SP 800-37 Revision 1, NIST SP 800-39, NIST SP 800-30, NIST SP 800-34, NIST SP 800-53 Revision 4, and NIST SP 800-53A.

Modules

- Critical Definitions and Policies
- C&A Transformation/Transition Overview
- The IC and the Transformation
- Roles and Responsibilities
- Accreditation Boundary
- System Categorization
- Select Security Controls
- Implement, Document & Assess Security Controls
- Authorize Information System
- Monitor Information System
- Reciprocity

All FISMA/NIST classes include the following takeaway items: a printed training book and a CD that includes reference materials pertaining to the course.

Course Length

32 Hours

Training above the Rest

All courseware meets all of the elements of the Committee on National Security Systems

(CNSS) for Information Systems Security (INFOSEC) Professionals, NSTISSI No. 4011 National Training Standard.

Our specialized Cyber Security and Information Assurance Training rivals our competitors in several ways:

1. As opposed to what you find with similar training offered by many competitors, our Information Assurance Training Courseware has been evaluated and certified by the National Security Agency (NSA) and Committee on National Security Systems (CNSS). We continually update and enhance our courseware in order to stay current and as a part of our ISO 9001 process.
2. Our instructors are only certified to teach our courses after they have demonstrated real life experience and then after having been through the coursework themselves. We ensure you have the best possible training possible.
3. We have a passion for training everyone that wants to learn or needs to know Information Assurance or Cyber Security. Our customers consistently rate our courses as the best Information Assurance, C&A, Cyber Security, and Government sponsored courses they have taken. We alone cannot tackle all the cyber security issues and threats - but we can help train the US workforce to better identify, respond, mitigate, and recover from the ongoing and ever-changing attacks.
4. We are experts in Information Assurance and Cyber Security - all of our instructors also support customers and deal with the same issues as you do in the ever-changing arena of cyber security and the information security landscape. Our approach to training is not purely academic, we understand the varying degree of knowledge and experience of our students, the many faces of the threat environment, as well as the plethora of compliance issues. We tailor our courses to the audience. We not only understand "one size does not fit all," we live it. We provide lessons learned and the "how to" that comes from real hands-on practical implementation. Our coursework and class exercises prepare our students to succeed.
5. We are a well established, respected, and award winning Information Assurance / Cyber Security company providing training, consulting, and solutions. We have been successfully providing security program and security engineering support for some the largest and most successful Federal, DoD, IC, and Fortune 500 customers in the world.
6. IT and generalized training and consulting companies may be able to help train you on how to build a web server, but don't rely on them to provide in-depth training on how to secure it or ask them to provide specialized IA and cyber security training. Information Assurance and Cyber Security training is not something you can take lightly - we don't take it lightly either.
7. We will tailor our Information Assurance and Cyber Security Training Modules to your specific IA, Component, and Cyber Security requirements:
 - U.S. Army Specific materials that include APMS, AR 25-2, AR 380-5, Army Certificate of Networthiness (CON), Army Gold Master, ACA Scoping Document, Best Business Practices, and any Army specific artifacts.
 - U.S. Air Force Specific materials that include: Enterprise Information Technology Data Repository (EITDR), AFI 31-401, AFI 31-501, AFI 33-202, AFI 33-211, AFI 33-204, Air Force ATC, and Air Force specific artifacts.

- U.S. Navy DIACAP Specific Material that includes: ITPR-DON, DON DIACAP Handbook, and Navy Specific Requirements.
- U.S. Marine Corps DIACAP Specific materials.
- DISA Security Technical Implementation Guides (STIG), Security Readiness Reviews (SRR), Gold Disk, and Retina.
- COCOM / Joint and external Requirements that include: OMB, DNI, CNSS 1199, CNSS 1253, FISMA, NIST SP 800-53, NIST SP 800-37, NIST 800-39, ICD 503, DCID 6/3, JFAN 6/3, CJCSI 6510.01E, CENTCOM and SOCOM specific requirements.