Implement the New NIST RMF Standards and Meet the 2022/2023 FISMA Metrics

September 14-15, 2022 · Online Virtual Class

AGENDA

Day 1: Wednesday, September 14, 2022

8:00AM Seminar Overview and Introductions

8:30AM Review of New Requirements – Presidential, OMB, DHS and NIST

- President's Executive Order 14028
- OMB Memos and Directives – 2022 FISMA Guidance, Privacy Reporting and On-Going Authorization, A-130
- DHS Binding Operational Directives (BODs) and Emergency Directives (EDs)
- Risk Management Framework (RMF) – SP800-37
- Cybersecurity Framework (CSF) – NIST CSF
- System Development Lifecycle (SDLC) – SP800-64
- System Security Engineer Framework (SSEF) – SP800-160
- High Value Assets (HVA) and Unclassified Controlled Information (UCI) Frameworks – OMB M-17-09 and SP800-171

9:50AM Break

10:00AM NIST Special Publications Update

Guest Speaker: **Ned Goren, CISSP,** *Information Security Specialist, National Institute of Standards and Technology (NIST)*

10:10AM Authorization Boundary Identification

- Attendee Real-World System Identification
- Authorization Boundary Identification Exercise

12:00AM Lunch

1:00PM System Categorization

- Categorize Real-World System Exercise
- Boundary and Control Review

1:50PM Break

2:00PM DHS Cybersecurity Initiatives Update

Guest Speaker: **Fabion (Frank) Husson, CISSP,** *Insights Branch Chief, Cyber Security Division (CSD), U.S. Department of Homeland Security (DHS)*

2:50PM Break

3:00PM Simplified Risk Assessments

- Risk Modeling: Quantitative, Qualitative, and Hybrid – SP800-30/SP800-39
- Categorization – FIPS-199/SP800-60
- System Maximum Impact Level – SP800-30/SP800-39/SP800-60
- Security Control Baseline/Best Practices – FIPS 200/SP800-53
- Zero-Trust Architecture

4:00PM Adjourn

Note: Many products will be identified, but identifying them is not an endorsement.

Implement the New NIST RMF Standards and Meet the 2022/2023 FISMA Metrics

September 14-15, 2022 · Online Virtual Class

AGENDA

Day 2: Thursday, September 15, 2022

8:00AM Security Controls – SP800-53 and SP800-53B

- Families
- Specific, Common and Hybrid
- Tailoring

9:00AM Security Control Exercises

- Specific, Common and Hybrid Security Control Exercises

10:00AM Break

10:10AM Tailoring and Compensating Control Exercises

11:00AM Leverage Government Initiatives

- Security Content Automation Protocol (SCAP)
- DoD Host-Based Security System (HBSS) Solutions
- Assured Compliance Assessment Solution (ACAS)
- Continuous Diagnostics and Mitigation (CDM) Program
- Continuous Monitoring Dashboard
- Bonding Operational Directives (BOD), EINSTEIN, Trusted Internet Connection (TIC), Managed Trusted Internet Protocol Services (MTIPS), and DHS Cybersecurity Hygiene Reviews

12:00PM Lunch

1:00PM Clouds and Security Services

1:30PM Cloud Accreditation and Reaccreditation Processes - FedRAMP

Guest Speaker: ***Ryan Hoesing,*** *Customer Success, Technology Transformation Service,* ***Federal Risk Accreditation Management Program (FedRAMP) Office***

2:15PM Break

2:30PM Security Plans – SP800-18

- Operations Manual and System Security Plan (SSP) – SP800-18
- Security-focused Configuration Management Plan (SecCMP) – SP800-128
- Patch Management Plan (PMP) – SP800-40
- Information Security Control Monitoring Plan (ISCMP) – SP800-137
- Incident Response Plan (IRP) – SP800-61/SP800-83
- Contingency Plan (CP) – SP800-34
- Cybersecurity Framework and Privacy Control Framework

3:30PM Detection and Response

- Endpoint Detection and Response (EDR)
- Cybersecurity Incident & Vulnerability Response Playbooks.

3:50PM Summary

4:00PM Adjourn

Note: Many products will be identified, but identifying them is not an endorsement.

Instructor

James Litchko, CISSP-ISSEP, CAP, MBCI, CMAS, Senior Security Expert, Litchko & Associates, Inc.

Mr. Litchko has been working as a security expert for over 40 years. Jim created and taught the first graduate computer security course as an adjunct professor at Johns Hopkins University for ten years, military officer for twenty years, and was a project manager and executive at NSA for five years. He has supervised and supported the securing of over 300 military, government and commercial IT systems. For 40 years, he successfully supported the development and sales of security products and service for seven companies, including Symantec, Telos, Security Solutions Corporation, Trusted Information Systems (acquired by Network Associates), System Research and Development (acquired by IBM), MountainWave (acquired by Symantec), and Internet Security Advisors Group (acquired by HP). Currently, he is a senior security expert for Litchko & Associates and is a Certified $(ISC)^2$ Instructor teaching the CISSP, Engineering Professional (ISSEP), and Certified Authorization Professional (CAP) review courses, and the DIACAP and Continuous Monitoring courses for $(ISC)^2$, Global Knowledge, Digital Government Institute, and Johns Hopkins University. A student of Ken Blanchard, Ph.D., the author of The One-Minute Manager®, Jim holds a Master's degree from Johns Hopkins University and has authored five books on security and management topics, to include: FY2010-2021 *DoD RMF Manuals, FY2010-2022 FISMA Authorization Process Guide: A Review for the $(ISC)^2$® CAP® Certification Exam, KNOW IT Security, KNOW Your Life, 2010 Official DIACAP for Global Knowledge,* and co-authored *$(ISC)^2$'s Official Information System Security Management Professional, Cyber Threat Levels Response Handbook, Know IT Security*, and *Know Cyber Risk.* Teaching virtual courses Internationally for 9 years.

Note: Many products will be identified, but identifying them is not an endorsement.