

NIST AI Risk Management Framework Bootcamp

Build Practical AI Risk & Governance
Programs

8 CPEs

Hands-On AI Risk Assessment

Real-World AI Risk Insights

(A Brand of Azpirantz Technologies LLP)



Why Attend?

AI adoption is accelerating across business, security, compliance, and operations, but unmanaged AI can introduce serious risks. This bootcamp helps professionals apply the NIST AI Risk Management Framework to identify, assess, govern, and monitor AI risks using practical templates, risk matrices, profiles, and governance-focused implementation approaches.

What Sets This Training Apart

NIST AI RMF Focus Learn the NIST AI Risk Management Framework in a practical way	Scenario-Led AI Risk Learning Understand AI risks through real-world business scenarios
Hands-On Framework Application Apply the NIST AI RMF to practical AI risk and governance scenarios	Responsible AI Coverage Explore fairness, transparency, accountability, safety, and privacy
Risk-Based Implementation Approach Learn how to assess, prioritize, and manage AI risks	Career-Oriented Learning Earn 8 CPEs, build AI governance skills for GRC, audit, risk, and security roles

Key Takeaways

✓ Apply NIST AI RMF Practically	✓ Identify and Prioritize AI Risks
✓ Build AI Risk Assessment Workflows	✓ Create AI RMF Implementation Profiles
✓ Design AI Governance Roles & Controls	✓ Earn 8 CPE Credits

Meet the Expert



Sujay P.

25+ Years of Experience

CISO | CCSP | CISSP | ISO 42001 | ISO 27001 | CTO | CSOA

Sujay is a cybersecurity and technology leader with 25+ years of experience in cloud security, enterprise risk management, cybersecurity governance, and AI-driven security. He has implemented SOC centers, SIEM solutions, ISO 42001/27001 programs, cloud security strategies, and large-scale cybersecurity projects, bringing practical expertise to AI risk and governance implementation.

His specializations include:

- AI security governance and risk management aligned with ISO 42001 and emerging AI assurance practices
- Cloud security architecture, secure cloud migrations, and hybrid/multi-cloud risk management
- Cybersecurity governance, compliance audits, SOC 2, GDPR, data protection, and enterprise risk management
- SOC implementation, SIEM deployment, security monitoring, and incident response programs
- Threat modeling, vulnerability assessments, penetration testing, and red team/blue team practices
- ISO 27001 implementation, security control design, and governance framework adoption
- AI-driven threat intelligence, security automation, and cloud-native security operations

Bootcamp Agenda

🔑 Day 1: AI Risk Foundations & NIST AI RMF Structure

Module 1: Understanding AI Risks in Modern Organizations

- What qualifies as an AI system
- Key risks across AI, GenAI, automation, and decision-support systems
- Business, legal, ethical, privacy, security, and operational risk areas
- Why traditional risk management needs to evolve for AI

Module 2: Responsible and Trustworthy AI Concepts

- Core principles of responsible AI governance
- Fairness, transparency, accountability, privacy, safety, and reliability
- Trustworthy AI characteristics in business contexts
- Common gaps in responsible AI adoption

Module 3: Introduction to the NIST AI Risk Management Framework

- Purpose and structure of the NIST AI RMF
- Core framework components: Functions, Categories, and Profiles
- How the framework supports AI risk and governance programs
- Using NIST AI RMF across AI development, deployment, and monitoring

Module 4: GOVERN Function: Building AI Governance Foundations

- AI governance roles, responsibilities, and accountability
- Policies, oversight mechanisms, and approval workflows
- Aligning AI governance with business objectives and risk appetite
- Governance for internal and third-party AI systems

Module 5: MAP Function: Understanding AI Context & Impact

- Identifying AI system purpose, users, data, and environment
- Mapping stakeholders, dependencies, and impacted groups
- Assessing business, process, data, and outcome-level impact
- Documenting assumptions, limitations, and risk context

🔑 Day 2: AI Risk Assessment, Response, Profiles & Implementation

Module 6: MEASURE Function: Assessing AI Risks

- Defining measurable AI risk indicators
- Evaluating bias, accuracy, reliability, privacy, and security concerns
- Using risk scoring and assessment matrices
- Linking measurement results to governance decisions

Module 7: MANAGE Function: Treating and Monitoring AI Risks

- Prioritizing AI risks based on likelihood, impact, and business criticality
- Selecting mitigation actions and controls
- Monitoring AI systems after deployment
- Escalating and communicating high-impact AI risks

Module 8: Creating NIST AI RMF Profiles

- Understanding current-state and target-state AI RMF Profiles
- Using profiles to prioritize governance improvements
- Applying profiles across AI use cases and maturity levels
- Translating profiles into an implementation roadmap

Module 9: Applying NIST AI RMF to Real-World AI Use Cases

- AI risk considerations for enterprise and GenAI tools
- Governance challenges in vendor-provided AI systems
- Lessons from AI adoption and governance failures
- Preparing for audits, assurance, and regulatory expectations

Module 10: Bootcamp Wrap-Up & AI Governance Action Plan

- Key lessons from the NIST AI RMF
- Common AI governance implementation challenges
- Building a practical AI risk and governance roadmap
- Q&A and guided discussion

***Note:** Participants will have access to session recordings for a period of 60 days.

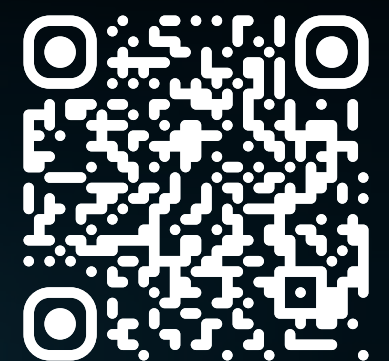


Get In Touch

 sales@infosectrain.com

 www.infosectrain.com

(A Brand of Azpirantz Technologies LLP)



Scan to Know More