INFOSECTRAIN
Educate. Excel. Empower.

ISACA Accredited Premium Partner

AAIR

Advanced in AI Risk

(AAIR) Certification Training



www.infosectrain.com

INFOSECTRAIN

Course Highlights

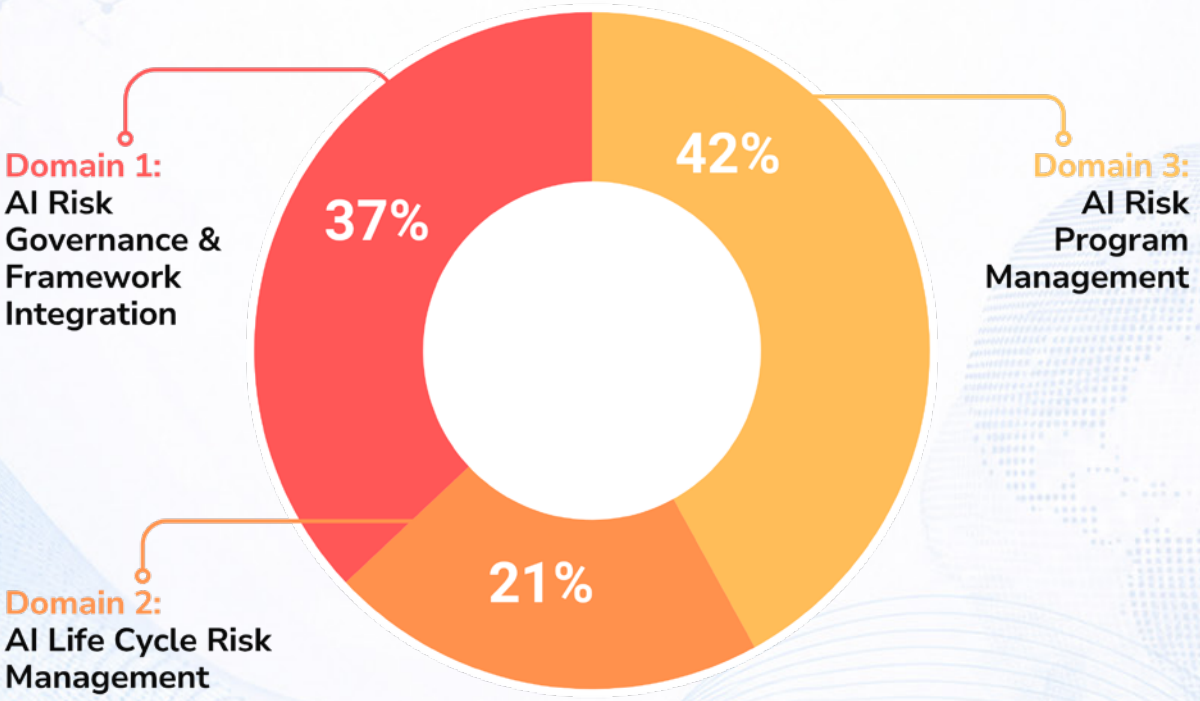
- **30-Hour LIVE** Instructor-Led Training
- ISACA Premium Training Partner
- Hands-on AI Risk Assessment, Treatment & Controls Management
- AI Model Training, Testing, Validation & Data Risk
- AI Lifecycle Risk Management & Governance Integration
- Enterprise AI Risk Program Management
- Exam-Aligned Coverage Across All Three AAIR Domains
- Delivered by Certified & Experienced AI GRC Experts
- Access to Recorded Sessions

INFOSECTRAIN

About Course

The Advanced in AI Risk (AAIR) credential validates a professional's ability to identify, assess, and manage risks associated with the development, deployment, and operation of AI systems. The course equips professionals with the knowledge and skills required to oversee the entire AI risk lifecycle, ensuring that AI initiatives align with organizational objectives, regulatory requirements, and ethical standards. AAIR focuses on three core practice areas: AI Risk Governance and Framework Integration, AI Lifecycle Risk Management and AI Risk Program Management.

AAIR domains & Weightage



INFOSECTRAIN

Course Objectives

Upon successful completion of the training, participants will be able to:

- Identify and Assess AI-Specific Risks Across Models, Data, and AI Operations
- Analyze AI Risks Including Bias, Data Integrity Issues, and Model Drift Scenarios
- Conduct AI-Specific Risk Assessments and Develop Comprehensive Risk Treatment Planning Strategies
- Integrate AI Risk Management Practices into Enterprise Governance, Risk, and Compliance Programs
- Navigate AI Regulatory Obligations, Ethical Considerations, and Responsible AI Frameworks Effectively
- Monitor AI Controls and Communicate Risk Insights and Reporting to Decision-Makers
- Extend AI Risk Management into Incident Response, Business Continuity, and Supply Chain Programs
- Establish Continuous AI Risk Monitoring, Reporting, and Improvement Processes Across the Enterprise

INFOSECTRAIN

Target Audience

The training is ideal for:

- Risk Management Professionals
- IT Auditors and Internal Auditors
- Information Security and Cybersecurity Professionals
- Governance, Risk, and Compliance (GRC) Practitioners
- AI Governance and Responsible AI Leaders
- Technology and Digital Transformation Managers
- Data Governance and Privacy Professionals
- Enterprise Risk Managers
- CRISC, CISA, CISM, CISSP, and CGEIT Certified Professionals
- Executives and Decision-Makers overseeing AI adoption

Pre-Requisites

- Active holders of industry-recognized certifications such as CISA, CISM, CRISC, CGEIT, CDPSE, and other relevant credentials seeking to expand their expertise in AI risk management.
- Experienced professionals working in IT risk, governance, compliance, audit, cybersecurity, consulting, or advisory roles who are responsible for assessing, managing, and mitigating technology-related risks.

INFOSECTRAIN

Exam Details

Certification Name	AAIR
Exam Duration	150 minutes
No. of Questions	90
Exam Format	Multiple Choice Questions
Passing Score	450
Exam Language	English, Spanish and Chinese



INFOSECTRAIN

Course Content

Domain 1

AI Risk Governance and Framework Integration | 37%

- AI Models, Frameworks, Strategies, and Use Cases
- AI Organizational Processes and Alignment
- AI Ownership, Oversight, and Accountability
- AI Policies, Procedures, and Organizational Training
- AI Regulatory Compliance and Legal Considerations
- AI Trustworthiness, Ethical and Societal Implications (e.g., ESG)

Domain 2

AI Life Cycle Risk Management | 21%

- AI Design, Development/Procurement, and Documentation
- AI Model Training, Testing, and Validation
- AI Implementation, Maintenance, and Decommissioning
- AI Data and Asset Management

INFOSECTRAIN

Domain 3

AI Risk Program Management | 42%

- AI Risk Scenario Identification and Assessment (e.g., threats, vulnerabilities, and attacks)
- AI Risk Treatment Strategies
- Controls Management (e.g., Evaluation, Selection, Validation)
- Risk Metrics, Monitoring, and Reporting
- Supply Chain Risk Management (e.g., third party resources)
- Incident Response, BIA, Business Continuity, and Disaster Recovery

Other Skills Tested

- Evaluate risk related to AI models/solutions including design, suitability, algorithms, training, drift, and AI life cycle.
- Facilitate the integration of AI risk management into an enterprise risk management framework and risk programs.
- Develop and implement an AI risk management framework, including roles and accountability, AI risk policies and procedures, and acceptable risk tolerance levels.
- Conduct risk assessments to identify and classify risks associated with AI.
- Develop and recommend risk treatment strategies for identified AI risks.
- Assess compliance with applicable AI-related regulations, laws, frameworks, standards, and guidelines.
- Integrate AI risk considerations into existing governance programs.
- Evaluate AI use cases based on the organization's risk appetite
- Monitor and test organizational processes to identify AI risks.

- Collaborate with stakeholders to develop and integrate AI risk concepts into enterprise-wide awareness training.
- Capture AI risk considerations in enterprise risk metrics and reporting (e.g., board, management, operations).
- Conduct and/or evaluate threat and vulnerability assessments on AI projects/programs.
- Collaborate with stakeholders to integrate AI risk scenarios into the enterprise incident management program.
- Continuously assess and monitor the risk landscape for emerging AI risk.
- Evaluate controls to manage AI-related risk within the organization's risk tolerance.
- Advise on AI-related risk within contracts and service agreements, including data usage and intellectual property.
- Evaluate AI risk as part of supply chain risk management.
- Collaborate with stakeholders to address AI trustworthiness and impacts including ethics, bias, privacy, safety, and environmental, social, and governance (ESG) implications.
- Leverage AI to support the risk management program (e.g., risk profile, reporting, evaluation, risk models, and analysis).
- Integrate AI-related risk considerations into the change management process.
- Incorporate AI-related risk considerations into incident response, BIAs, the BCP, and DRP.
- Assess human oversight controls at critical decision points for risk and AI impact.

INFOSECTRAIN
Educate. Excel. Empower.



Contact us

www.infosectrain.com
sales@infosectrain.com

Follow us on