AI CERTs™

Executive Introduction to RSAIF

Program Detailed Curriculum

Executive Summary

This certification program provides an extensive understanding of AI governance, security, and ethical principles. It explores the Responsible & Secure AI for the Future (RSAIF) and NIST frameworks, focusing on the critical domains of AI risk management, including security, privacy, legal compliance, trust, and governance. Participants will examine real-world case studies to identify vulnerabilities like adversarial attacks, data poisoning, and bias, and learn how to address these risks. The program also emphasizes the executive's role in overseeing AI systems, ensuring they are ethically sound, transparent, and compliant, fostering trust and accountability in AI deployments across diverse industries

Course Prerequisites

- **Basic Understanding of Artificial Intelligence (AI) and Machine Learning (ML):** Familiarity with AI and ML concepts is essential for grasping governance, security, and ethical issues related to AI systems.
- **Knowledge of Regulatory Frameworks:** Understanding key regulations such as GDPR, HIPAA, and the upcoming EU AI Act is crucial for applying AI governance and compliance principles.
- **Cybersecurity Fundamentals**: A foundation in cybersecurity, including knowledge of adversarial attacks, data poisoning, and model security, is required to understand AI-specific vulnerabilities.
- **Ethical Considerations in Technology:** Awareness of ethical principles, such as fairness, transparency, and bias mitigation, is necessary to navigate AI's societal impacts.
- **Executive Leadership or Management Experience:** Familiarity with governance structures and executive decision-making is beneficial for understanding how to oversee and manage AI systems in an organization.

Module 1

AI Security Frameworks: Safeguarding AI Systems Across Industries

1.1 AI in the Modern World

Explore how AI drives transformation in energy, agriculture, transportation, and food systems. Understand how security lapses in these domains can lead to operational failures and national-scale risks.

1.2 Challenges in AI Security

Identify critical vulnerabilities unique to AI, including adversarial attacks, data poisoning, and model inversion. Examine how ethical, governance, and supply chain risks complicate secure AI implementation.

1.3 Consequences of Neglecting AI Security

Discover the organizational and societal consequences of ignoring AI security. Learn how weak oversight can result in operational breakdowns, data leaks, legal violations, and loss of trust.

1.4 Case Study: IBM Watson for Oncology

Examine how data bias, lack of validation, and poor explainability led to AI failure in healthcare. Understand parallels between clinical AI errors and cybersecurity automation pitfalls.

1.5 The Rise of AI Security Frameworks

Understand the emergence of AI-specific security frameworks in response to increasing threats. Learn how structured models guide secure, ethical, and compliant AI deployment across industries.

1.6 Key AI Security Frameworks and Standards

Study the NIST AI Risk Management Framework (AI RMF) and RSAIF MOSAIC framework. Learn their structures, principles, and applications for building trustworthy, resilient AI systems.

1.7 Comparative Overview: NIST vs. RSAIF

Compare NIST's process-driven approach with RSAIF's lifecycle and domain-based model. Understand how both frameworks complement each other to strengthen governance, privacy, and security.

1.8 Other Frameworks and Guidelines

Review other emerging models such as Google's Secure AI Framework (SAIF), financial sector initiatives like FINOS, and regulatory influences shaping the AI security landscape globally.

1.9 Case Studies and Real-World Applications

Analyze cross-sector adoption of AI frameworks. Learn from organizations like Workday, the City of San José, global banks, DeepMind, and healthcare institutions applying structured AI risk governance.

1.10 Recent AI Security Incidents (2023–2025)

Evaluate contemporary incidents like data leaks, prompt injection exploits, and deepfake fraud. Understand lessons learned that highlight the importance of comprehensive AI governance and safeguards.

1.11 Conclusion and Future Outlook

Summarize how AI frameworks foster responsible innovation and resilience. Recognize how collaboration across business, legal, and security teams ensures compliance and prepares organizations for emerging AI risks.

Module 2

Simplifying AI Governance

2.1 What is AI Governance?

Introduces the concept, scope, and significance of AI governance. Explains how structured policies, roles, and oversight ensure AI operates ethically, transparently, and in alignment with legal and organizational objectives.

2.2 Why AI Governance Matters

Explores why governance is critical in mitigating AI risks, ensuring compliance, and maintaining trust. Highlights how effective governance supports sustainable innovation while preventing bias, misuse, and regulatory breaches.

2.3 The Need for Ethical AI

Examines ethical challenges in AI development and deployment. Emphasizes fairness, accountability, privacy, and transparency as key governance principles ensuring responsible and trustworthy AI systems across sectors.

2.4 RSAIF MOSAIC Governance Domain

Presents the RSAIF framework's seven domains—Security, Privacy, Legal, Trust, Governance, Risk Management, and Oversight—showing how each ensures holistic, integrated, and secure AI governance across the entire lifecycle.

2.5 Why AI Governance Fails Without RSAIF

Analyzes common governance breakdowns like siloed operations, fragmented compliance, and lack of oversight. Demonstrates how the unified RSAIF framework addresses these challenges through cross-domain collaboration and structured accountability.

2.6 Interactive Activity: Mini Case Study Discussion - Case Study: Tesla's Autonomous Vehicle Governance

Analyzes Tesla's autonomous vehicle governance failures to illustrate the importance of ethical policies, oversight committees, and compliance with global AI safety standards for ensuring transparency, accountability, and responsible autonomous system development.

2.7 Conclusion and Executive Recap

Summarizes leadership's role in establishing AI governance as a strategic priority. Reinforces executive accountability for ethics, transparency, and compliance through structured, organization-wide RSAIF-aligned governance practices.

Module 3

The Executive's Role in AI Security

3.1 Responsibilities of Executives in AI Security, Risk Management, and Governance

Explains how executives oversee AI security, risk, and governance across the lifecycle. Focuses on establishing policies, managing risks, ensuring ethical deployment, and aligning AI initiatives with compliance and organizational objectives.

3.2 Top-Down Leadership

Explores how executive-led, top-down leadership drives ethical, secure, and transparent AI deployment. Emphasizes leadership accountability, alignment with organizational goals, and fostering a responsible AI culture across all business units.

3.3 RSAIF's Leadership and Oversight Functions: A Precise Overview

Describes RSAIF's executive-level oversight roles, including AI governance committees, audit readiness, performance monitoring, and accountability structures. Shows how leaders integrate RSAIF into strategy to ensure transparency, ethics, and compliance.

3.4 Interactive Activity: Role Play – Ensuring AI-Driven Credit Scoring Meets RSAIF-Aligned Governance Standards

An interactive simulation where executives collaborate to align an AI credit-scoring system with RSAIF governance standards. Focuses on bias detection, system security, regulatory compliance, and cross-departmental leadership accountability.

Module 4

Red Flags to Watch

4.1 Common Red Flags in AI Projects

Highlights major warning signs in AI development, such as lack of model cards, missing data sheets, shadow AI, and absence of audit trails. Explains how these issues compromise ethics, compliance, and accountability.

4.2 Indicators of Poor Governance in AI Projects: Missing Ownership or Change Logs

Explains how unclear ownership and missing change logs signal weak AI governance. Discusses their impact on accountability, compliance, and traceability, offering best practices for clear documentation and defined responsibilities.

4.3 Overview of RSAIF Control Integration in the AI Lifecycle

Describes integration of RSAIF governance controls across AI lifecycle stages—development, deployment, monitoring, and retirement—to ensure transparency, documentation, compliance, and ethical AI deployment through traceable, secure processes.

4.4 Interactive Activity: Risk Identification Exercise – RSAIF Governance

Engages participants in identifying AI project red flags, mapping them to RSAIF controls, and creating mitigation strategies. Builds practical understanding of governance principles through collaborative, real-world problem-solving exercises.

Module 5

Red Flags to Watch

5.1 Success Stories: Real-World Examples of Strong AI Governance

Explores successful AI implementations under robust governance frameworks. Demonstrates how ethical design, accountability, and compliance led to business growth, operational reliability, and societal impact in diverse sectors like insurance, aerospace, and healthcare.

5.2 Failures in AI: Lack of Oversight and Governance

Analyzes real-world AI failures caused by weak governance and oversight. Emphasizes the consequences of bias, poor ethical controls, and missing accountability in high-impact cases across hiring, social media, and image recognition.

5.3 RSAIF's Outcome-Based Approach

Explains RSAIF's MOSAIC outcome-based model for ensuring ethical, transparent, and secure AI. Describes how integrated governance, oversight, and risk management create measurable results that align AI performance with fairness and compliance standards.

5.4 Interactive Activity: RSAIF Maturity Assessment Interactive Walkthrough

An interactive guided exercise to assess an organization's AI maturity across RSAIF's seven domains. Participants identify governance gaps, analyze readiness levels, and create actionable improvement plans for responsible and secure AI implementation.

Module 6

Understanding the RSAIF MOSAIC Framework

6.1 RSAIF MOSAIC Framework

Explains the RSAIF MOSAIC Framework's role in developing responsible and secure AI systems through ethical principles, modular layers, and governance domains ensuring fairness, transparency, compliance, and trust across industries.

6.2 RSAIF's Integrated Controls: Application to Real-World AI Systems

Explores RSAIF's integrated controls—security, privacy, risk management, and governance—applied to real-world AI systems. Demonstrates their combined role in building resilient, ethical, and compliant AI ecosystems across diverse industries.

Use Case 6.1: Adversarial Robustness in Facial Recognition

Shows how AI systems use adversarial training to prevent spoofing attacks in facial recognition. Strengthens authentication processes, enhances model resilience, and ensures secure biometric identity verification in sensitive environments.

Use Case 6.2: Continuous Monitoring in Financial Fraud Detection

Describes AI-driven real-time monitoring in banking systems. Detects fraudulent transactions instantly, minimizes financial risks, enhances compliance with AML regulations, and improves customer confidence through proactive fraud prevention.

Use Case 6.3: Data Minimization in AI-Powered E-Commerce

Illustrates responsible AI personalization in e-commerce by collecting only necessary user data. Reduces privacy risks, ensures GDPR compliance, and enhances user trust through ethical data handling and transparency.

Use Case 6.4: Informed User Consent in Mobile Applications

Explains how AI-enabled mobile apps seek explicit user consent for data use. Promotes transparency, regulatory compliance, and trust by clearly communicating storage, analysis, and sharing practices.

Use Case 6.5: Managing Third-Party Risks in Retail AI Systems

Focuses on AI-driven retail inventory management reliant on third-party data. Implements risk evaluations, backup strategies, and monitoring to ensure operational continuity and reliable, ethical supply-chain automation.

Use Case 6.6: Risk Mitigation in AI-Powered Financial Trading

Highlights AI-based trading systems employing automated safeguards, stress testing, and continuous evaluation. Minimizes financial loss, enhances reliability, and maintains compliance during volatile market conditions.

Use Case 6.7: Stakeholder Engagement in Smart City AI

Details stakeholder collaboration in AI-driven smart city projects. Engages citizens, regulators, and experts to ensure ethical, transparent, and socially beneficial urban technology solutions aligned with community values.

Use Case 6.8: Regulatory Compliance in Financial AI Systems

Demonstrates governance controls in AI credit scoring and lending. Ensures fairness, transparency, and compliance with regulations like GDPR and AML, building public trust and preventing ethical violations.

Module 7

Governance, Oversight, and Compliance

7.1 RSAIF-MOSAIC Framework

Explains how RSAIF and MOSAIC integrate to ensure responsible, secure, and ethical AI systems. Covers governance, accountability, and compliance alignment with global standards like ISO 42001, NIST RMF, and the EU AI Act.

7.2 Self-Assessment: RSAIF Maturity Assessment Toolkit

Introduces the RSAIF Maturity Assessment Toolkit that helps organizations evaluate AI governance, privacy, and risk management maturity. Provides a step-by-step process for identifying gaps and aligning with global compliance standards.

7.3 Leveraging Assessment Results for Executive Decisions

Details how RSAIF Maturity Assessment results support executive planning and decision-making. Explains how maturity findings drive governance KPIs, budget allocations, and strategic initiatives to enhance responsible, transparent, and compliant AI governance.

Case Study 7.1: Healthcare AI – Enhancing Diagnostics

Explores a healthcare organization using AI diagnostics aligned with ISO 42001, NIST RMF, and EU AI Act. Demonstrates ethical oversight, bias reduction, and compliance in medical decision-making and data governance.

Case Study 7.2: Finance – AI for Credit Scoring

Examines financial institutions adopting AI for credit scoring under RSAIF-MOSAIC. Highlights fairness, bias mitigation, human oversight, and transparency to ensure responsible, compliant, and ethical lending practices.

Case Study 7.3: Autonomous Vehicles – Securing AI Systems

Analyzes autonomous vehicle governance using RSAIF-MOSAIC. Emphasizes safety, transparency, human oversight, and compliance with global standards to ensure secure, ethical, and accountable AI-driven navigation and decision-making systems.

Case Study 7.4: Retail – AI for Personalized Shopping

Demonstrates responsible AI deployment in e-commerce personalization. Focuses on ethical data handling, privacy compliance, fairness, and governance under RSAIF-MOSAIC to improve trust, transparency, and customer experience.

Case Study 7.5: Public Safety – AI in Surveillance Systems

Highlights AI-powered surveillance for public safety governed by RSAIF-MOSAIC. Ensures data privacy, ethical oversight, and compliance with the EU AI Act, balancing civil rights with advanced security intelligence.

Module 8

Identifying AI Risks and Red Flags

8.1 Spotting Red Flags

Explains key AI red flags—shadow AI, missing audit trails, and model bias. Emphasizes early detection of ethical, operational, and security risks to ensure compliant, transparent, and trustworthy AI systems.

8.2 Practical Application: Identifying Red Flags in an AI Project Case Study Based on RSAIF Controls

Teaches participants to apply RSAIF controls in real-world scenarios. Focuses on identifying shadow AI, audit trail gaps, and bias using responsible, secure AI and impact assessment principles.

Case Study 8.1: AI-Driven Credit Scoring System at FinServe Bank

Analyzes FinServe Bank's AI credit scoring system. Identifies red flags like bias, missing audit trails, and privacy risks. Recommends RSAIF-based mitigation for fairness, transparency, and regulatory compliance.

8.3 Creating an AI Risk Register

Introduces the AI Risk Register as a structured tool to document risks, assign ownership, and track mitigation actions, aligning with RSAIF–MOSAIC principles for transparent and accountable AI governance.

Case Study 8.2: AI-Driven Recruitment Tool

Demonstrates RSAIF–MOSAIC application in HR. Identifies model bias, missing documentation, and lack of explainability. Proposes retraining, audit logging, and fairness frameworks to ensure ethical, transparent recruitment practices.

Case Study 8.3: AI-Powered Marketing Campaign Optimization (Non-Financial Use Case)

Examines AI in marketing automation. Highlights risks such as biased targeting, shadow AI, and missing logs. Suggests governance alignment, human review, and fairness audits to ensure ethical marketing outcomes.

Module 8

Learning from Real-World Success and Failures

9.1 In-Depth Case Studies: Examine Successful and Failed AI Projects, with a Focus on Compliance and AI Governance Lessons

Analyzes real-world AI successes and failures to uncover key governance, ethical, and compliance lessons. Highlights transparency, accountability, and bias mitigation as critical pillars of responsible, trustworthy AI deployment.

Case Study 9.1: Successful AI Projects – Compliance and Governance Excellence

Showcases successful AI projects like IBM Watson, PayPal, Tesla, and DeepMind. Demonstrates ethical AI governance, compliance with regulations, and transparency, emphasizing fairness, trust, and long-term accountability.

Case Study 9.2: Failed AI Projects – Governance and Compliance Pitfalls

Explores failed AI initiatives including Amazon's Recruiting Tool and Clearview AI. Identifies issues like bias, discrimination, and privacy violations while recommending fixes through governance, transparency, and ethical oversight.

9.2 Personal Action Plan: AI Governance Aligned with RSAIF-MOSAIC

Guides participants to create a personalized AI governance plan using RSAIF-MOSAIC principles. Focuses on ethical AI development, data privacy, bias mitigation, transparency, and compliance through a structured five-step action plan.

Case Study 9.3: AI-Powered Hiring System

Applies the RSAIF-MOSAIC framework to an AI hiring system. Identifies bias, transparency gaps, and privacy issues while proposing fairness audits, explainable AI, and GDPR-compliant governance improvements.

9.3 Completion & Next Steps

Concludes Module 9, summarizing lessons from real-world AI successes and failures. Encourages RSAIF certification and 90-day reassessment using the Maturity Toolkit to strengthen governance and compliance practices.