Training Course on AI Risk Management and Governance Frameworks

Professional Development Training Course Outline

Category	Data Science	**Duration**	10 Days
Base Fee	$3,000 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

The rapid proliferation of Artificial Intelligence (AI) across industries presents unprecedented opportunities alongside complex challenges, particularly in **risk management** and **governance**. As AI systems become more sophisticated and integrated into critical operations, ensuring their **safety, ethical deployment, and regulatory compliance** is no longer optional but a strategic imperative. This comprehensive training course is designed to equip professionals with the essential knowledge and practical skills to navigate the evolving landscape of **AI risks**, establish robust **governance frameworks**, and develop effective **policies and processes for AI safety**.

Training Course on AI Risk Management & Governance Frameworks delves into the intricacies of **responsible AI**, emphasizing the critical need for proactive strategies to mitigate potential harms such as **algorithmic bias, data privacy breaches, security vulnerabilities, and unintended consequences**. Participants will learn to identify, assess, and manage AI-related risks across the entire AI lifecycle, fostering **trustworthy AI** implementations. Through practical case studies and interactive exercises, attendees will gain actionable insights into building a resilient AI ecosystem that aligns with emerging **AI regulations** and **ethical AI principles**, ensuring sustainable innovation and organizational resilience in the AI era.

Programme Curriculum

Training Course on AI Risk Management & Governance Frameworks: Developing Policies and Processes for AI Safety

Introduction

The rapid proliferation of Artificial Intelligence (AI) across industries presents unprecedented opportunities alongside complex challenges, particularly in **risk management** and **governance**. As AI systems become more sophisticated and integrated into critical operations, ensuring their **safety,**

ethical deployment, and regulatory compliance is no longer optional but a strategic imperative. This comprehensive training course is designed to equip professionals with the essential knowledge and practical skills to navigate the evolving landscape of **AI risks**, establish robust **governance frameworks**, and develop effective **policies and processes for AI safety**.

Training Course on AI Risk Management & Governance Frameworks delves into the intricacies of **responsible AI**, emphasizing the critical need for proactive strategies to mitigate potential harms such as **algorithmic bias, data privacy breaches, security vulnerabilities, and unintended consequences**. Participants will learn to identify, assess, and manage AI-related risks across the entire AI lifecycle, fostering **trustworthy AI** implementations. Through practical case studies and interactive exercises, attendees will gain actionable insights into building a resilient AI ecosystem that aligns with emerging **AI regulations** and **ethical AI principles**, ensuring sustainable innovation and organizational resilience in the AI era.

Course Duration

10 days

Course Objectives

1. Develop advanced capabilities in identifying and assessing diverse AI-specific risks, including **model risk, data integrity risk, and ethical AI risks**.
2. Construct comprehensive **AI governance frameworks** aligned with leading industry standards and **regulatory compliance** mandates (e.g., NIST AI RMF, ISO/IEC 42001).
3. Formulate practical and actionable **AI safety policies** that address critical areas like **algorithmic fairness, transparency, and accountability**.
4. Apply cutting-edge **AI security best practices** to protect AI systems from adversarial attacks, data poisoning, and unauthorized access.
5. Understand and interpret the nuances of emerging global **AI regulations** (e.g., EU AI Act, US Executive Order on AI) and their implications for organizational practices.
6. Develop strategies and implement tools for detecting and effectively **mitigating algorithmic bias** in AI models and datasets.
7. Integrate **explainable AI (XAI)** techniques to enhance the interpretability and transparency of AI decision-making processes.
8. Design and implement clear **AI accountability** structures and reporting mechanisms within an organization.
9. Master approaches to ensure **AI data privacy** and robust **data security** throughout the AI lifecycle, adhering to global privacy regulations.
10. Create effective **AI incident response plans** to address failures, breaches, or adverse events related to AI systems.
11. Champion the adoption of **ethical AI principles** and responsible innovation within organizational AI initiatives.
12. Perform thorough **AI impact assessments** to evaluate the societal and organizational implications of AI deployment.
13. Develop strategies to build **public trust** and stakeholder confidence in AI systems through transparent governance and risk management.

Organizational Benefits

- Proactively identify and mitigate AI-related risks, safeguarding business operations and reputation.
- Ensure adherence to evolving global AI regulations, minimizing legal and financial penalties.

- Foster trustworthy AI systems that provide reliable insights and support sound strategic decisions.
- Enable faster, safer, and more ethical development and deployment of AI solutions.
- Build confidence among customers, regulators, and the public through transparent and accountable AI practices.
- Differentiate by demonstrating a commitment to responsible AI, attracting top talent and fostering innovation.
- Efficiently allocate resources for AI development and deployment by understanding and prioritizing risks.
- Minimize the costs associated with AI failures, security breaches, and regulatory non-compliance.

Target Audience

1. Risk Managers & Compliance Officers.
2. AI/ML Engineers & Data Scientists.
3. Legal & Governance Professionals.
4. IT Security & Cybersecurity Specialists.
5. Business Leaders & Executives.
6. Product Managers & Solution Architects.
7. Auditors & Assurance Professionals
8. Policy Makers & Regulators.

Course Outline

Module 1: Foundations of AI Risk & Governance

- Introduction to Artificial Intelligence and its transformative impact.
- Understanding the unique risks posed by AI: technical, ethical, societal, and legal.
- Overview of the AI lifecycle and risk touchpoints.
- **Case Study**: The infamous Tay chatbot incident and its implications for ethical AI design.
- Defining AI governance: principles, objectives, and scope.

Module 2: Key AI Governance Frameworks & Standards

- Deep dive into the NIST AI Risk Management Framework (AI RMF).
- Exploring ISO/IEC 42001: AI Management System standard.
- Comparison of leading global AI governance initiatives (e.g., OECD AI Principles).
- **Case Study**: Applying the NIST AI RMF to a financial services AI lending model.
- Developing an organizational AI governance charter.

Module 3: Crafting AI Safety Policies

- Principles of policy development for responsible AI.
- Establishing policies for data collection, usage, and retention in AI systems.
- Defining acceptable use policies for generative AI and large language models (LLMs).
- **Case Study**: Designing a corporate policy for managing the risks of employee use of public LLMs.
- Integrating AI safety policies into existing organizational frameworks.

Module 4: AI Risk Identification & Assessment Methodologies

- Techniques for proactive AI risk identification (e.g., threat modeling for AI).

- Quantitative and qualitative AI risk assessment methods.
- Building an AI risk register and prioritizing risks.
- **Case Study**: Assessing privacy risks in an AI-powered healthcare diagnostic tool.
- Tools and platforms for automated AI risk assessment.

Module 5: Mitigating Algorithmic Bias & Fairness

- Understanding sources of algorithmic bias (data, design, deployment).
- Methods for detecting and measuring bias (e.g., disparate impact).
- Strategies for mitigating bias (e.g., data re-balancing, model debiasing).
- **Case Study**: Addressing gender bias in an AI-powered recruitment system.
- Fairness metrics and ethical considerations in AI development.

Module 6: AI Security: Protecting Against Adversarial Attacks

- Introduction to AI-specific security threats (e.g., data poisoning, adversarial examples, model inversion).
- Defense mechanisms against adversarial attacks on AI models.
- Secure AI development lifecycle (SecDevOps for AI).
- **Case Study**: Analyzing an adversarial attack on a self-driving car's perception system.
- Best practices for securing AI model deployment and inference.

Module 7: AI Data Privacy & Data Governance

- Navigating data privacy regulations (GDPR, CCPA, etc.) in the context of AI.
- Implementing privacy-enhancing technologies (PETs) for AI.
- Data anonymization, pseudonymization, and differential privacy techniques.
- **Case Study**: Ensuring data privacy for customer data used in an AI-driven personalization engine.
- Establishing robust data governance frameworks for AI systems.

Module 8: AI Explainability & Interpretability (XAI)

- The importance of XAI for accountability, trust, and debugging.
- Techniques for model interpretability (e.g., SHAP, LIME).
- Communicating AI decisions to non-technical stakeholders.
- **Case Study**: Explaining the decision of an AI system denying a loan application.
- Balancing explainability with model performance and complexity.

Module 9: AI Accountability & Human Oversight

- Establishing clear lines of responsibility for AI system outcomes.
- Designing effective human-in-the-loop and human-on-the-loop processes.
- Auditability and traceability of AI decisions.
- **Case Study**: Developing an accountability framework for an AI system used in judicial sentencing.
- Legal and ethical implications of AI autonomy.

Module 10: Regulatory Compliance in AI

- In-depth analysis of the EU AI Act and its classification of AI systems.
- Understanding the US Executive Order on Safe, Secure, and Trustworthy AI.
- Sector-specific AI regulations (e.g., healthcare, finance).

- **Case Study**: Adapting an AI product development roadmap to comply with the EU AI Act's high-risk requirements.
- Strategies for continuous regulatory monitoring and adaptation.

Module 11: AI Incident Response & Crisis Management

- Developing an AI incident response plan: detection, containment, eradication, recovery.
- Forensic analysis of AI system failures and anomalies.
- Crisis communication strategies for AI-related incidents.
- **Case Study**: Responding to a public relations crisis stemming from an AI system's biased output.
- Learning from AI incidents and implementing corrective actions.

Module 12: Ethical AI by Design & Responsible Innovation

- Integrating ethical considerations throughout the AI development lifecycle.
- Value alignment and human-centric AI design principles.
- Participatory design and stakeholder engagement in AI.
- **Case Study**: Designing an AI system for public transport with a focus on accessibility and fairness for all users.
- Fostering a culture of responsible innovation within the organization.

Module 13: Implementing AI Governance: Practical Steps

- Roadmap for establishing an AI governance office or committee.
- Roles and responsibilities for AI governance within an organization.
- Integrating AI governance into existing GRC (Governance, Risk, and Compliance) structures.
- **Case Study**: Developing a phased implementation plan for an AI governance framework in a large enterprise.
- Measuring the effectiveness of AI governance initiatives.

Module 14: AI Impact Assessments & Societal Implications

- Conducting comprehensive AI impact assessments (AIAs).
- Analyzing the societal implications of AI (e.g., employment, discrimination).
- Stakeholder engagement and public consultation for AI projects.
- **Case Study**: Assessing the socio-economic impact of deploying AI-powered automation in a manufacturing facility.
- Contributing to broader AI policy discussions and advocacy.

Module 15: Future Trends in AI Risk & Governance

- Emerging AI technologies and their potential risks (e.g., AGI, superintelligence).
- The role of AI in automating risk management and compliance.
- International cooperation and harmonization of AI governance.
- **Case Study**: Preparing for future regulatory shifts related to explainable AI and data sovereignty.
- Horizon scanning for new AI threats and opportunities in risk management.

Training Methodology

This course utilizes a blended learning approach to maximize engagement and knowledge retention:

- **Interactive Lectures & Discussions**: Expert-led sessions with ample opportunity for Q&A and peer-to-peer learning.
- **Real-World Case Studies**: In-depth analysis of historical and contemporary AI incidents and successful implementations to illustrate key concepts.
- **Practical Exercises & Workshops**: Hands-on activities, group discussions, and scenario-based problem-solving.
- **Templates & Checklists**: Provision of practical tools for developing AI policies, risk assessments, and governance frameworks.
- **Guest Speakers**: Insights from industry leaders, regulators, and AI ethicists.
- **Online Resources**: Access to curated readings, videos, and supplementary materials for self-paced learning.
- **Capstone Project (Optional)**: Participants can apply learned concepts to develop an AI risk management plan for their own organization.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call *+254769199797*

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
23 Nov 2026	04 Dec 2026	Online	$2,000
23 Nov 2026	04 Dec 2026	Physical	$3,000
23 Nov 2026	04 Dec 2026	Physical	$6,000
23 Nov 2026	04 Dec 2026	Physical	$6,000
23 Nov 2026	04 Dec 2026	Physical	$12,000
23 Nov 2026	04 Dec 2026	Physical	$9,000
23 Nov 2026	04 Dec 2026	Physical	$12,000
23 Nov 2026	04 Dec 2026	Physical	$12,000

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com