Training Course on ML Model Governance and Versioning

Professional Development Training Course Outline

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

Course Introduction

In today's data-driven landscape, **Machine Learning (ML) models** are at the core of innovation, driving critical business decisions and automating complex processes. However, as organizations increasingly adopt ML, ensuring the reliability, fairness, and accountability of these models becomes paramount. Training Course on ML Model Governance & Versioning: Managing Model Lifecycle and Reproducibility delves into the crucial concepts of **ML Model Governance** and **Versioning**, equipping professionals with the essential skills to manage the entire **model lifecycle** effectively, from development and deployment to monitoring and retirement. Participants will learn to establish robust frameworks that guarantee **reproducibility**, minimize **model risk**, and foster **ethical AI practices**, ultimately enhancing organizational trust and compliance.

The proliferation of sophisticated ML models necessitates a structured approach to their management. Without proper **governance frameworks** and meticulous **version control**, organizations face significant challenges, including **model drift**, regulatory non-compliance, and difficulties in debugging or replicating past results. This course addresses these critical pain points by providing practical methodologies and industry best practices for building a **reproducible AI pipeline**. By mastering the art of model governance and versioning, participants will gain the confidence to implement scalable and secure ML solutions, ensuring long-term **model integrity** and maximizing the return on their AI investments.

Programme Curriculum

Training Course on ML Model Governance & Versioning: Managing Model Lifecycle and Reproducibility

Introduction

In today's data-driven landscape, **Machine Learning (ML) models** are at the core of innovation, driving critical business decisions and automating complex processes. However, as organizations

increasingly adopt ML, ensuring the reliability, fairness, and accountability of these models becomes paramount. Training Course on ML Model Governance & Versioning: Managing Model Lifecycle and Reproducibility delves into the crucial concepts of **ML Model Governance** and **Versioning**, equipping professionals with the essential skills to manage the entire **model lifecycle** effectively, from development and deployment to monitoring and retirement. Participants will learn to establish robust frameworks that guarantee **reproducibility**, minimize **model risk**, and foster **ethical AI practices**, ultimately enhancing organizational trust and compliance.

The proliferation of sophisticated ML models necessitates a structured approach to their management. Without proper **governance frameworks** and meticulous **version control**, organizations face significant challenges, including **model drift**, regulatory non-compliance, and difficulties in debugging or replicating past results. This course addresses these critical pain points by providing practical methodologies and industry best practices for building a **reproducible AI pipeline**. By mastering the art of model governance and versioning, participants will gain the confidence to implement scalable and secure ML solutions, ensuring long-term **model integrity** and maximizing the return on their AI investments.

Course Duration

10 days

Course Objectives

1. Master the fundamentals of MLOps (Machine Learning Operations) and its critical role in the modern AI lifecycle.
2. Design and implement robust ML Model Governance frameworks for accountability and compliance.
3. Develop strategies for effective model versioning, including data, code, and artifact management.
4. Ensure model reproducibility across diverse environments and throughout the development pipeline.
5. Mitigate AI risks, including bias, fairness, and explainability, through targeted governance practices.
6. Implement automated model validation and continuous integration/continuous deployment (CI/CD for ML) pipelines.
7. Understand and apply best practices for model monitoring and drift detection in production.
8. Establish clear model documentation standards for transparency and auditability.
9. Leverage ML model registries for centralized management and discovery.
10. Integrate ethical AI principles into the entire model lifecycle.
11. Optimize resource management and cost efficiency through effective model lifecycle strategies.
12. Navigate regulatory compliance requirements related to AI governance and data privacy.
13. Foster cross-functional collaboration between data scientists, engineers, and business stakeholders for seamless MLOps adoption.

Organizational Benefits

- Reduced Model Risk.
- Enhanced Compliance.
- Improved Reproducibility & Auditability.
- Accelerated MLOps Maturity.
- Increased Model Trust & Transparency.
- Optimized Resource Utilization.

- Faster Time-to-Market
- Scalable AI Initiatives.
- Stronger Collaboration.
- Competitive Advantage.

Target Audience

1. Data Scientists.
2. ML Engineers
3. MLOps Engineers
4. AI/ML Team Leads & Managers
5. Software Engineers working with AI
6. Compliance & Risk Officers
7. Researchers in AI/ML.
8. Anyone involved in the deployment or management of ML systems

Course Outline

Module 1: Introduction to ML Model Governance & MLOps

- Defining ML Model Governance: Principles, importance, and scope.
- Overview of the ML Model Lifecycle: From ideation to retirement.
- Introduction to MLOps: Bridging the gap between ML development and operations.
- Key challenges in deploying and managing ML models at scale.
- **Case Study:** Discussing a financial institution's struggle with inconsistent model predictions due to lack of governance and how MLOps principles could have prevented it.

Module 2: Foundations of Model Versioning

- Understanding the need for version control in ML: data, code, and models.
- Concepts of model artifacts and metadata.
- Strategies for versioning training data and feature sets.
- Code versioning best practices for ML projects (e.g., Git).
- **Case Study:** Analyzing a retail company's difficulty in replicating a successful recommendation model due to untracked data and code changes.

Module 3: Data Versioning for Reproducibility

- Tools and techniques for data version control (e.g., DVC, LakeFS).
- Tracking data lineage and transformations.
- Managing data drifts and their impact on model performance.
- Ensuring data integrity and immutability for experiments.
- **Case Study:** A healthcare provider struggling to reproduce a diagnostic model's results due to unversioned and evolving patient datasets, highlighting the importance of data versioning.

Module 4: Experiment Tracking & Reproducibility

- Logging and tracking ML experiments: parameters, metrics, and models.
- Tools for experiment management (e.g., MLflow, Weights & Biases).
- Establishing a single source of truth for ML experiments.
- Strategies for reproducing past experimental results.
- **Case Study:** A research team's inability to reproduce published ML research findings due to incomplete experiment metadata and untracked dependencies.

Module 5: Model Registries and Centralized Management

- The role of model registries in MLOps.
- Centralized storage and management of trained models.
- Versioning and cataloging model metadata, lineage, and documentation.
- Facilitating model discovery and reuse across teams.
- **Case Study:** How a large e-commerce platform utilized a centralized model registry to manage hundreds of deployed models, improving governance and accelerating new product features.

Module 6: Model Deployment & Orchestration

- Deployment strategies: batch, real-time, edge.
- Containerization for consistent deployment (e.g., Docker, Kubernetes).
- Orchestrating ML pipelines for automated training and deployment.
- Managing model dependencies and environments.
- **Case Study:** A telecommunications company's challenges with deploying inconsistent models across different environments, solved by containerization and automated orchestration.

Module 7: Continuous Integration/Continuous Delivery (CI/CD) for ML

- Adapting CI/CD principles for machine learning workflows.
- Automated testing of ML models: unit, integration, and performance tests.
- Automating model retraining and redeployment.
- Setting up continuous monitoring in CI/CD pipelines.
- **Case Study:** A self-driving car company implementing CI/CD for their perception models to ensure continuous improvement and rapid deployment of updates.

Module 8: Model Monitoring & Drift Detection

- Importance of continuous model monitoring in production.
- Detecting model drift, data drift, and concept drift.
- Metrics for performance monitoring: accuracy, latency, fairness.
- Alerting and remediation strategies for model degradation.
- **Case Study:** A fraud detection system experiencing a sudden drop in accuracy due to concept drift in transactional data, emphasizing the need for robust monitoring.

Module 9: Explainable AI (XAI) and Interpretability

- The importance of model interpretability for governance and trust.
- Techniques for explaining model predictions (e.g., SHAP, LIME).
- Integrating XAI into the model development and monitoring stages.
- Communicating model insights to non-technical stakeholders.
- **Case Study:** A bank facing regulatory scrutiny over biased loan approval decisions, mitigated by using XAI techniques to explain individual model predictions.

Module 10: Ethical AI and Fairness in ML Governance

- Understanding ethical considerations in AI development.
- Identifying and mitigating algorithmic bias.
- Developing fairness metrics and evaluation strategies.
- Implementing responsible AI principles throughout the lifecycle.
- **Case Study:** A recruitment platform identifying and correcting gender bias in its resume screening algorithm through ethical AI audits and fairness interventions.

Module 11: Model Risk Management & Compliance

- Assessing and managing risks associated with ML models.
- Regulatory landscape for AI (e.g., AI Act, industry-specific regulations).
- Establishing clear accountability and ownership for models.
- Conducting internal and external audits of ML systems.
- **Case Study:** A pharmaceutical company navigating strict regulatory requirements for drug discovery models, implementing rigorous risk management and compliance frameworks.

Module 12: Security in ML Models

- Threats to ML models: adversarial attacks, data poisoning.
- Securing the ML pipeline: data, code, and infrastructure.
- Best practices for model integrity and robustness.
- Implementing access control and secure deployment practices.
- **Case Study:** A cybersecurity firm developing an anomaly detection system, showcasing strategies to protect it from adversarial attacks and ensure data integrity.

Module 13: Documentation and Collaboration for Governance

- Creating comprehensive model documentation: model cards, data sheets.
- Establishing clear communication channels for ML teams.
- Tools and processes for collaborative ML development.
- Version controlling documentation alongside code and models.
- **Case Study:** A global tech company improving cross-functional collaboration and knowledge sharing by implementing standardized model documentation templates and collaborative MLOps platforms.

Module 14: Advanced Topics in ML Model Governance

- Federated learning and its governance implications.
- Model lineage and provenance tracking.
- Automated governance tools and platforms.
- Future trends in AI governance and regulation.
- **Case Study:** Exploring a consortium of hospitals using federated learning for medical image analysis and the unique governance challenges involved in distributed model training.

Module 15: Building a Sustainable ML Governance Strategy

- Developing an organizational roadmap for ML governance.
- Integrating governance into existing MLOps workflows.
- Measuring the effectiveness of governance initiatives.
- Continuous improvement and adaptation of governance frameworks.
- **Case Study:** A large financial institution successfully transforming its ML development culture by implementing a phased and sustainable ML governance strategy, leading to significant cost savings and reduced risks.

Training Methodology

This training program will utilize a **blended learning approach** combining:

- **Instructor-Led Sessions:** Interactive lectures, discussions, and Q&A.
- **Hands-on Labs & Exercises:** Practical implementation of concepts using industry-standard tools (e.g., MLflow, DVC, common cloud ML platforms).
- **Case Study Analysis:** In-depth examination of real-world scenarios and their solutions.

- **Group Discussions & Collaborative Problem-Solving:** Fostering peer learning and diverse perspectives.
- **Live Demos:** Demonstrations of tools and techniques in action.
- **Q&A and Troubleshooting Sessions:** Addressing specific challenges and questions.
- **Quizzes and Assessments:** To gauge understanding and retention.

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

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