



Module 9

Workshop 2: Governance and compliance simulation: Building a regulatory-ready ML system



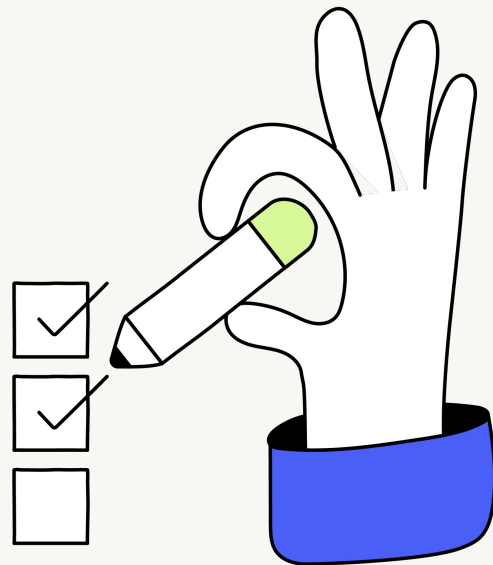
Icebreaker

Scramble for compliance

Rearrange the following letters to uncover a key ML compliance risk—and explain how regulatory compliance or governance in ML systems can help mitigate it.

I – B – S – A

Drop your answers in the chat.





Module 9

Workshop 2: Governance and compliance simulation: Building a regulatory-ready ML system



Agenda

- **Review:** Recap key concepts from async units 2 and 3.
- **Practice:** Building a compliance plan for LearnSmart.
- **Closing:** Key takeaways and next steps.



Learning objectives

- **Analyse how governance frameworks** (e.g., AREA, SAFE-D) shape compliant ML data strategies and operations.
- **Apply regulatory requirements** (e.g., GDPR, AI Act) to design compliant ML system practices, including data minimisation, access control, and transparency measures.
- **Create compliance artifacts** (e.g., risk matrices, audit checklists) that demonstrate readiness for external audits and regulatory reviews.
- **Design escalation protocols** for responding to compliance breaches in ML systems.

Async review: Units 2 and 3

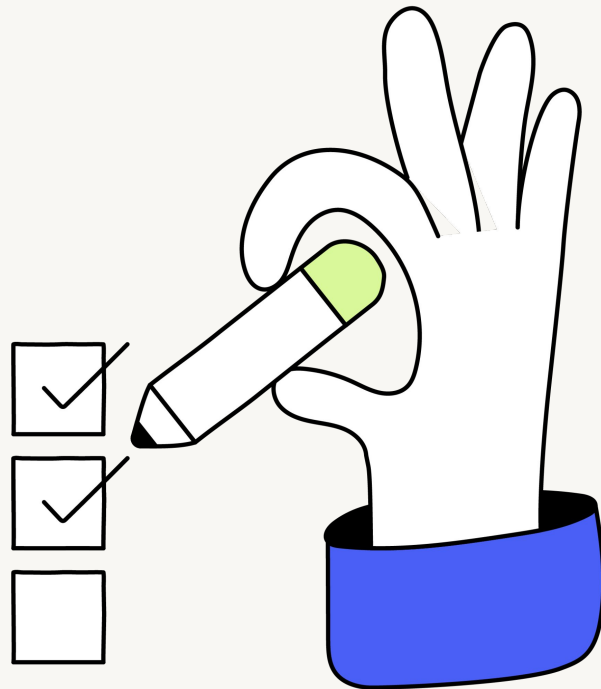
Go to My Multiverse, Module 9
Workshop 2



Navigate to the **"Async review"** page



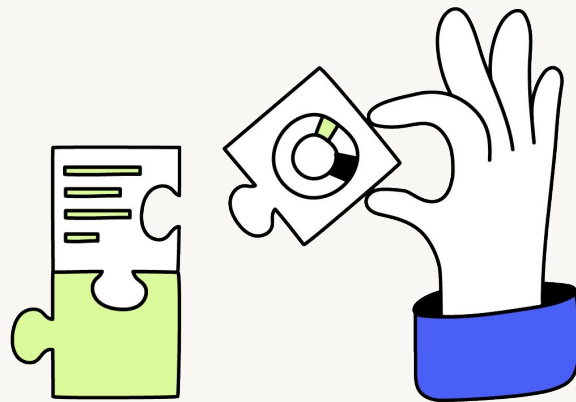
Review the summary of Units 2 and 3





Unit 2: Data Privacy and Governance in Machine Learning

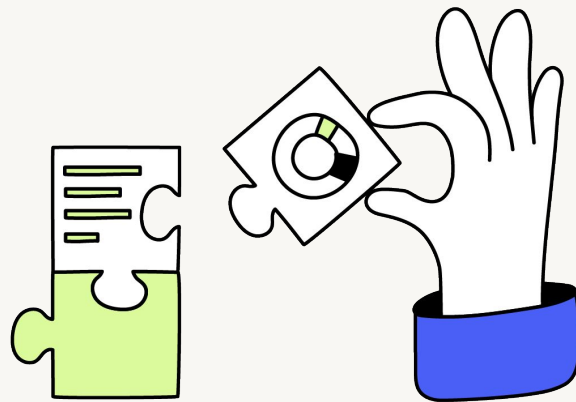
- **Privacy and ethical foundations** – Key regulations such as GDPR, HIPAA, and CPRA, and the importance of privacy-by-design when handling sensitive ML data.
- **Governance frameworks** – AREA and SAFE-D as tools to embed accountability, fairness, and explainability across ML systems.
- **Compliant data strategies** – Practices for data minimisation, metadata tracking, retention limits, and access control to meet legal and ethical standards.





Unit 2: Data Privacy and Governance in Machine Learning

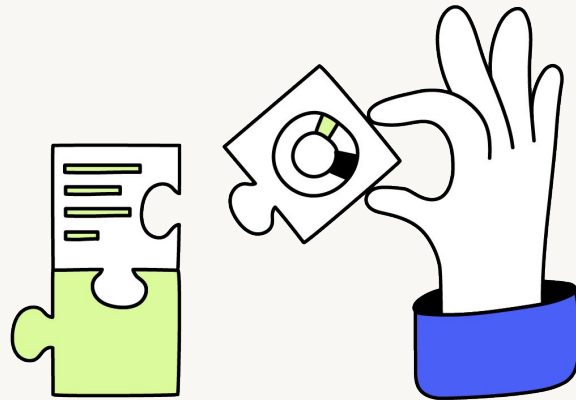
- **Quality and fairness** – Frameworks to assess data completeness, consistency, and bias, and ensure equitable model performance across user groups.
- **Trust through transparency** – How strong governance, clear documentation, and inclusive review practices build confidence in ML system outcomes.





Unit 3: Regulatory Compliance and Risk Management in Machine Learning

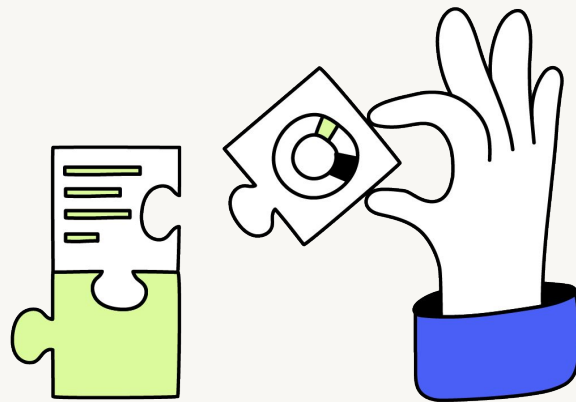
- **ML compliance frameworks** – Key regulations and standards including the EU AI Act, ISO/IEC 23053, and NIST AI RMF, and how they guide safe, transparent ML development.
- **System-level risk** – Common vulnerabilities across the ML lifecycle, from third-party dependencies and infrastructure gaps to model failure and versioning issues.
- **Mitigation and escalation** – Proactive practices like workflow gating, anomaly thresholds, and peer reviews, alongside tiered escalation protocols to manage incidents.





Unit 3: Regulatory Compliance and Risk Management in Machine Learning

- **Audit readiness** – Documentation and processes needed to demonstrate compliance, including model cards, access logs, and risk registers.
- **Organisational accountability** – Responsibility mapping across roles, ensuring risks are owned and addressed across development, deployment, and monitoring stages.

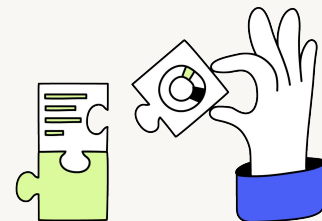




What's at risk in ML systems?

Common compliance risks in real-world ML projects:

- Privacy breaches from poor data governance.
- Fairness gaps due to unrepresentative or biased data.
- Lack of transparency in how models make decisions.
- Missing controls for access, auditability, or incident response.

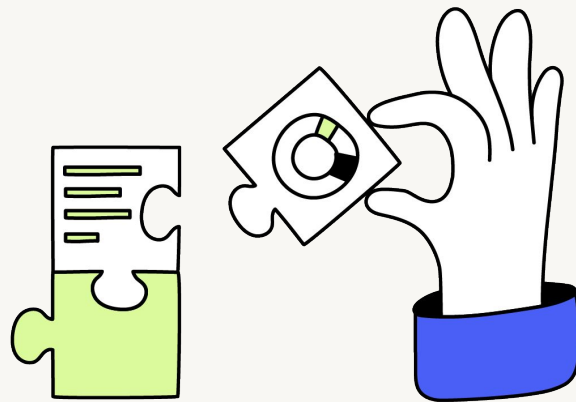




Governance and compliance foundations in ML

Core frameworks shaping ML practices:

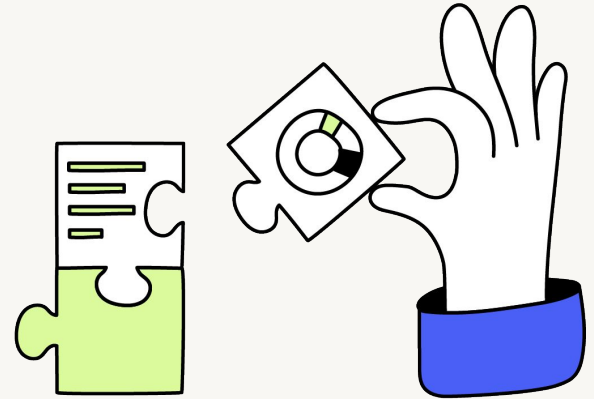
- Regulations: GDPR, AI Act, HIPAA, CCPA – define boundaries for privacy, fairness, and data use.
- Standards: ISO/IEC 23053, NIST AI RMF – guide system interoperability, risk control, and continuous monitoring.
- Frameworks: AREA and SAFE-D – support accountability, explainability, fairness, and ethical oversight across the ML lifecycle.





Compliance artifacts

Key artifacts like **risk matrices**, **audit checklists**, and **escalation plans** help teams anticipate and manage compliance risks.



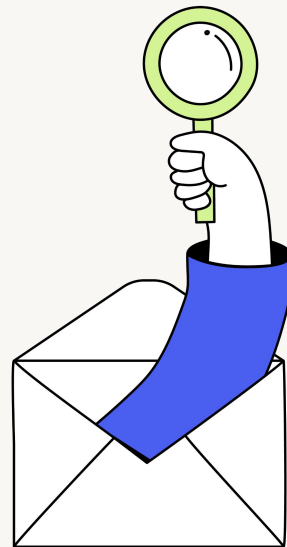


Skills application: Building a compliance plan



Skills application introduction

- **Objective:** In this skills application, your team must develop a compliance plan that proactively addresses these issues and prepares LearnSmart for external review.
- **You'll need to to:**
 - Review the LearnSmart compliance case.
 - Collaborate with your team to develop your compliance plan.
 - Share your plan with the other groups.





Access the skills application

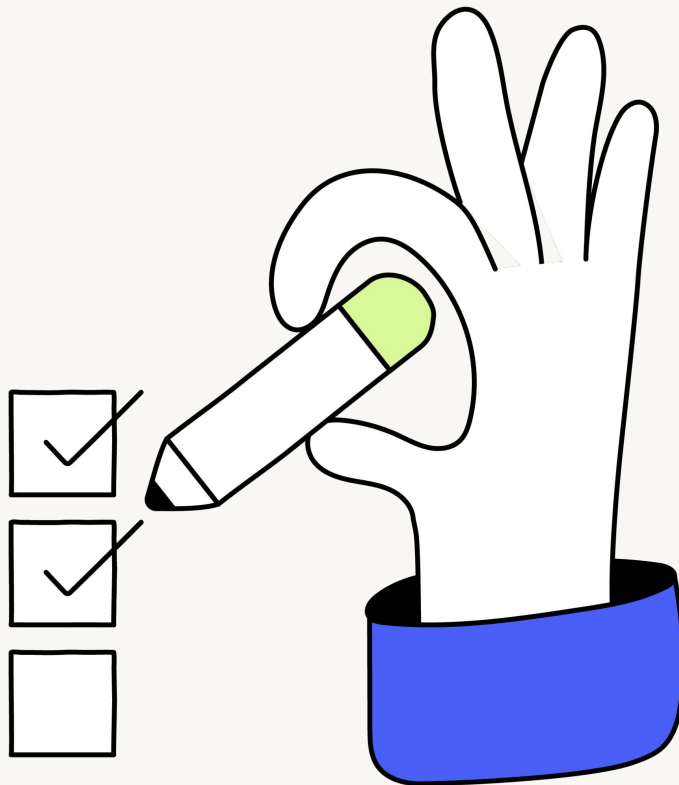
Go to My Multiverse, Module 9
Workshop 2



Go to the Skills application page and
follow the instructions provided



Be prepared to discuss your learnings
when we come back together





Skills application debrief



Skills application debrief

What risks did you identify and what steps did you take to secure them?





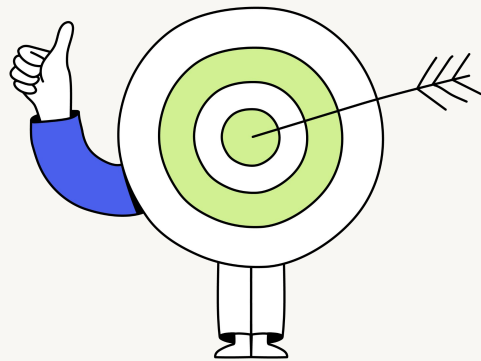
Key takeaways

1 **Compliance isn't just a checkbox — it's an ongoing practice.**

Designing risk matrices, audit checklists, and escalation workflows helps you embed governance and accountability into every stage of your ML system, making it resilient and audit-ready from day one.

2 **Clear roles and documented processes build trust and reduce risk.**

By assigning ownership for each risk and defining structured response protocols, you ensure your system can handle breaches effectively — protecting both users and your organisation's reputation.





Applying **key** **takeaways** to your organisation



Applying key takeaways

- 1 Where in your ML projects could clearer documentation or escalation protocols strengthen compliance and stakeholder trust?
- 2 How might adopting a governance framework like AREA or SAFE-D help your team proactively manage risk and regulatory expectations?



Share your plan to apply new skills

Go to My Multiverse, Module 9
Workshop 2



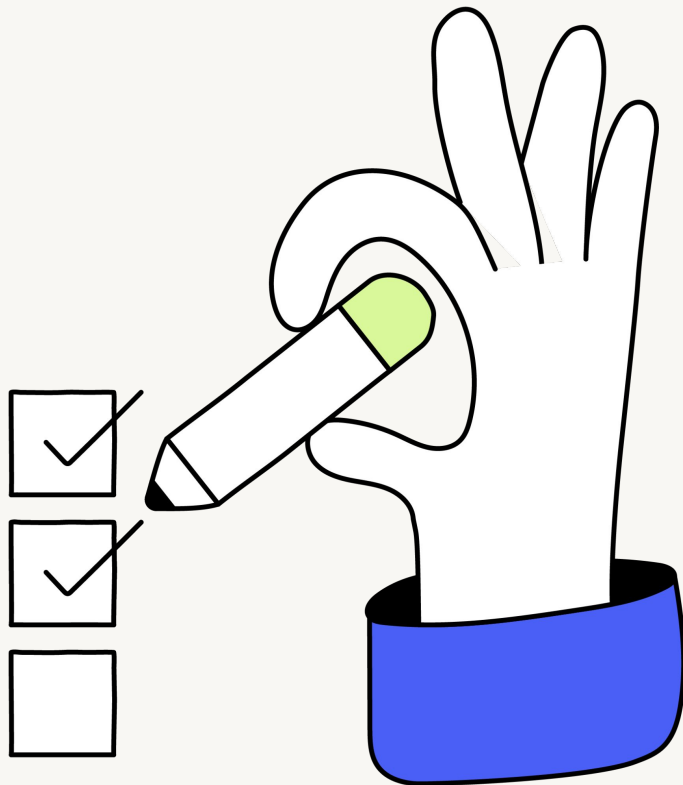
On the Apply new skills to your role
page, find the discussion activity



Take 2 minutes to share how you will
apply this skill in your role.



Take time this week to read what
others have written and get new ideas!





Closing out

- **Next workshop:** Module 9 Wrap up
- **Have questions?**
 - Chat with Atlas
 - Reach out to your Cohort Coach
 - Sign up for Tutoring
- **Log your OTJ hours**
- **Take the Workshop Survey** on My Multiverse

multiverse