COURSE CURRICULUM:

AI GOVERNANCE & RISK

AI GOVERNANCE, RISK MANAGEMENT, PRIVACY & ETHICS AUDIT

S&M
INFOMYNT
PROFESSIONAL TRAINING

About Infomynt (An S&M Initiative)

Infomynt is the professional training brand of **S&M**, focused on building job-ready skills in IT audit, governance, risk, and compliance (GRC). We work with freshers, finance and IT graduates, and working professionals who want more than theory — our programs are built around real audit workpapers, real ERP screens, and the kind of practical judgment that clients and employers actually test for. Every course is designed and delivered by practitioners who have sat across the table in real audits, not just read about them.

Our courses currently span IT General Controls (ITGC), IT Application Controls (ITAC), Business Process Controls (BPC), SAP GRC, and now **AI Governance & Risk** — extending our practical, workpaper-driven teaching approach into the fastest-growing area of audit and controls advisory. Visit us at www.infomynt.in to learn more about our full course catalogue and upcoming batches.

Meet Your Trainers

Swathi — CISA, ISO 31000 CRM, ISO/IEC 42001 LA

Swathi is a co-founder and lead trainer, **CISA-certified**, a **Certified Risk Manager (ISO 31000)**, and an **ISO/IEC 42001 Lead Auditor**, with a background in IT audit, SAP/GRC controls, and IAM frameworks. She has designed and delivered training on ITGC, SOX, and application controls for professionals moving into audit and controls advisory careers, and is known for a practical, workpaper-driven teaching style that mirrors how real audit engagements actually run. Her ISO/IEC 42001 Lead Auditor credential directly anchors this course's approach to AI governance audit.

Manoj — CISA, ISO/IEC 27001, ISO/IEC 42001 LA

Manoj is a co-founder and trainer, **CISA-certified**, **ISO/IEC 27001 certified**, and an **ISO/IEC 42001 Lead Auditor**, with expertise in SAP and Oracle-driven business processes, control design, and risk assessment. He brings a strong process-owner perspective to the training, helping participants understand not just how a control is tested, but why it exists and how it fits into the broader business process — a perspective he now extends to how AI systems are governed within existing ERP-driven business processes, connecting AI risk to the finance, procurement, and operations realities teams already know.

AI GOVERNANCE & RISK

AI GOVERNANCE, RISK MANAGEMENT, PRIVACY & ETHICS AUDIT

S&M
INFOMYNT
PROFESSIONAL TRAINING

Course Overview

This course provides a practitioner's understanding of AI Governance and AI Risk Management, and their role in ensuring AI systems are adopted responsibly, safely, and in compliance with emerging global standards. It covers key concepts, frameworks, and audit methodologies used to evaluate AI governance programs, spanning strategy, risk, data privacy, and ethics.

Course Objectives

Upon completion of this course, participants will be able to:

- Distinguish AI Audit, AI Governance Audit, and AI Risk Management, and explain how they interlock
- Identify and assess AI-specific risks, including bias, model drift, and data privacy exposure
- Evaluate an organization's AI governance program against standards such as ISO/IEC 42001, NIST AI RMF, and the EU AI Act
- Review data governance and privacy controls (including DPIAs) applied to AI systems
- Prepare audit-ready workpapers, risk & control matrices, and governance deficiency write-ups

Who Should Attend

- Freshers and early-career professionals targeting IT Audit / Internal Audit roles
- IT Auditors and Risk Advisory professionals expanding into AI governance
- SAP / Oracle functional consultants moving into GRC or controls advisory
- CA / CMA / CS articleship students and finance graduates
- Working professionals in Risk Advisory, SOX Compliance, Data Privacy, or Internal Controls teams
- Professionals preparing for CISA, ISACA AAIA, or pursuing ISO/IEC 42001 Lead Auditor certification

AI Governance vs. AI Risk Management vs. Data Privacy & Ethics — Understanding the Difference

Every AI-enabled audit rests on three layers of control. Getting this distinction right is the foundation for this course — and for any AI governance audit interview.

	AI Governance	AI Risk Management	Data Privacy & Ethics
Definition	Policies, strategy, and organizational structures that direct how AI is adopted and controlled across the enterprise.	The process of identifying, assessing, and monitoring risks specific to AI systems throughout their life cycle.	Controls ensuring the data feeding AI systems, and the decisions they produce, respect individual privacy and ethical principles.
Scope	Entity-wide / program-level	System / model-specific	Data-specific and individual-impact specific
Examples	AI strategy, governance committee, policies & procedures, training programs	Risk registers, bias testing, model drift monitoring, incident response	Data classification, DPIA, anonymization, explainability, human oversight
Who Owns It	AI Governance Committee / Senior Leadership	Risk & Compliance function, Model Owners	Data Owners, Privacy Officer, Ethics Board
Reliance Logic	Foundation layer — if governance is weak, risk and privacy controls lack structure to operate within	Reliable only if governance defines clear risk appetite and ownership	Can partly compensate for weak technical controls through process discipline, at higher review effort
Testing Style	Policy review, interview, governance structure walkthrough	Risk register review, control testing, monitoring dashboard review	DPIA review, data lineage tracing, consent verification, bias/fairness sample testing

Memory hook: AI Governance sets the rules of the house. AI Risk Management watches for fires before they start. Data Privacy & Ethics makes sure nobody in the house gets hurt along the way.

AI Governance & Risk — Areas Covered

This course is organised around the core disciplines a governance or risk audit typically touches when evaluating an organization's AI adoption:

Data Governance & Quality

Data Governance covers how an organization manages the data feeding its AI systems as a controlled asset — from data quality and classification to lineage, ownership, and retention. Controls in this area are designed to ensure that training and inference data is accurate, appropriately classified, traceable to its source, and disposed of responsibly. Key control points include data quality checks before model training, classification of sensitive data feeding AI models, clearly assigned data ownership, and documented data lineage. Auditors typically focus on whether weak data governance upstream is quietly becoming biased or unreliable model behaviour downstream.

Privacy & Data Protection

The Privacy & Data Protection area governs how personal data is handled throughout the AI life cycle, from collection through to model training and eventual disposal. Strong controls here protect against unauthorized use of personal data, unlawful profiling, and privacy violations that can trigger regulatory penalties. This course covers core privacy principles (purpose limitation, data minimization, consent), Data Protection Impact Assessments (DPIAs) for high-risk AI use cases, and techniques such as anonymization and pseudonymization. Particular attention is given to AI-specific privacy risks, including re-identification and AI-inferred sensitive data.

Standards, Ethics & Compliance

The Standards, Ethics & Compliance area covers the external reference points and internal principles that define responsible AI. Controls in this area ensure the organization's AI governance program is benchmarked against recognized standards and genuinely reflects ethical principles in practice, not just on paper. This course covers ISO/IEC 42001, the NIST AI Risk Management Framework, the EU AI Act's risk-tiered approach, India's evolving AI governance landscape, and core ethical principles including fairness, transparency, human oversight, and accountability — with emphasis on how these translate into testable audit criteria.

How Auditing Happens — Governance vs. Risk & Privacy

	Governance & Standards Audit Approach	Risk, Data & Privacy Audit Approach
1. Scoping	Identify in-scope AI systems, governance structures, and applicable standards / regulations	Identify in-scope AI systems' data flows, risk categories, and personal data touchpoints
2. Walkthrough	Walk through the governance committee charter, policies, and approval workflows with process owners	Walk through the AI system's data pipeline and risk register with model and data owners
3. Test of Design (TOD)	Confirm policies and roles are designed to enforce accountability and risk appetite	Confirm risk assessment and DPIA processes are designed to catch bias, drift, and privacy risk before deployment
4. Test of Effectiveness (TOE)	Review evidence that the governance committee actually met, approved, and enforced policy over the period	Sample AI models/systems and test whether risk assessments, monitoring, and DPIAs were actually completed and kept current
5. Evidence	Committee minutes, policy documents, training completion records, approval logs	Risk registers, DPIAs, bias test results, monitoring dashboards, incident logs
6. Exception Handling	Trace gaps to missing policy, unclear ownership, or committee inactivity	Trace gaps to a specific model/dataset; assess if isolated or systemic across similar AI systems
7. Reporting	Deficiency linked to governance structure; remediation usually a policy update or role clarification	Deficiency linked to a specific AI system; remediation usually model retraining, retesting, or an added monitoring control

AI GOVERNANCE & RISK

AI GOVERNANCE, RISK MANAGEMENT, PRIVACY & ETHICS AUDIT

S&M
INFOMYNT
PROFESSIONAL TRAINING

Course Modules

Module 1: Foundations of AI Governance — Week 1

- AI types, Machine Learning models, algorithms, and the AI life cycle
- AI strategy and how it sets organizational guardrails
- AI-related roles & responsibilities (governance committee, model owners, data stewards)
- Policies & procedures, training & awareness, and program metrics

Module 2: AI Risk Management — Week 1–2

- AI-related risk identification: bias, hallucination, model drift, security, over-reliance
- AI risk assessment: likelihood, impact, and risk-based prioritization
- AI risk monitoring: performance tracking, incident logging, periodic re-assessment

Module 3: Privacy & Data Governance — Week 2–3

- Data governance: quality, classification, lineage, ownership, retention & disposal
- Core privacy principles and personal vs. sensitive personal data in AI
- Privacy by Design, DPIAs, anonymization vs. pseudonymization

Module 4: Ethics, Standards & Compliance — Week 3

- ISO/IEC 42001, NIST AI RMF, the EU AI Act, and India's evolving AI governance landscape
- Converting standards into testable audit criteria
- Core ethical principles: fairness, transparency, accountability, human oversight
- Human-in-the-Loop vs. Human-on-the-Loop, responsible AI culture, ethical dilemma case studies

Module 5: AI Governance Audit Simulation — Week 4

- Mock AI governance audit on a sample organization
- Building a Risk & Control Matrix (RCM) for AI systems
- Writing observations, deficiency classification, and remediation plans
- Mock interview preparation for AI audit / governance roles

AI GOVERNANCE & RISK

AI GOVERNANCE, RISK MANAGEMENT, PRIVACY & ETHICS AUDIT

S&M
INFOMYNT
PROFESSIONAL TRAINING

Course Details & Enrolment

Duration	4 weeks — weekend live online batches
Eligibility	Graduates in Commerce / Finance / IT; working professionals in audit, risk, compliance, or ERP functional roles; no prior AI or data science background required
Delivery	Live instructor-led sessions with practical, workpaper-driven exercises
Ideal Next Step	Pairs well with S&M's ITGC, ITAC & BPC, and SAP GRC tracks; strong preparation for ISACA AAIA and groundwork for ISO/IEC 42001 Lead Auditor certification

For enrolment and batch schedule, contact S&M at info@infomynt.in or 8919893463.