Day 4

Generative AI
Security

Purpose of an AI Security Governance Board:

An AI Security Governance Board is a senior group of stakeholders who oversee how AI is designed, built, deployed, and monitored in an organization. They ensure that AI is safe, secure, compliant, ethical, and aligned with business goals.

It acts as the “control tower” for all AI activities.

Why organizations need an AI governance board?

Organizations need this board because:

1. AI introduces new risks
2. AI systems are high-impact
3. Growing legal and regulatory requirements
4. To avoid chaotic and unauthorized AI use

How the board supports secure AI development?

The board ensures the AI development process is:

1. Secure

- Approves threat modeling requirements
- Demands security controls (mTLS, OAuth, data isolation)
- Reviews incident reports
- Ensures adversarial testing and red teaming

2. Compliant

- Ensures every AI system meets relevant laws
- Reviews documentation, risk assessments, DPIAs, AIAs
- Ensures explainability and transparency obligations

3. Accountable

- Assigns RACI responsibility
- Defines who owns risks (business unit vs. security team)
- Forces justification for high-risk systems

4. Consistent

- Standard templates, checklists, documentation
- Centralized approval workflow
- Prevents random, inconsistent project decisions

AI Governance Board vs. Traditional Cyber Governance Board

AI Governance Board	Cyber Governance Board
Focuses on AI risks (bias, model drift, prompt injection, hallucinations, ethical issues)	Focuses on general IT/cyber risks (network, identity, vulnerabilities)
Approves AI use cases and model lifecycle	Approves security policies and cyber investments
Requires ML, data science, ethics, compliance experts	Requires traditional IT and security experts
Monitors model behavior and AI-specific incidents	Monitors cyber incidents, breaches, vulnerabilities
Deals with algorithmic transparency, fairness, compliance	Deals with security frameworks, controls, and threat defense

Scope of Authority:

The board ensures AI is developed with the same discipline as other critical technologies. The AI Security Governance Board typically has the power to:

1. Approve AI use cases
2. Define AI security policies
3. Oversee risks and compliance
4. Monitor high-risk AI systems
5. Ensure alignment with enterprise goals

Roles and Responsibilities in the AI Security Governance Board:

An AI Security Governance Board brings together executive, technical, security, legal, and operational experts. Each member has a specific responsibility to ensure AI is safe, secure, compliant, ethical, and aligned with business goals.

Executive & Strategic Roles:

1. **CISO (Chief Information Security Officer)**

The CISO is the security leader for all AI systems. Responsibilities: Oversees AI security strategy, Approves AI security controls, leads AI incident response, Monitors AI risk posture across the organization.

2. **CTO / CIO**

These roles ensure AI fits with the technology and business architecture. Responsibilities

- Approves AI platforms and tools (LLM platforms, vector databases, MLOps systems)
- Ensures scalability, performance, and reliability

- Aligns AI projects with enterprise technology strategy
- Ensures infrastructure supports secure AI development
- Ensures proper integration with cloud, APIs, DevOps pipelines

CTO/CIO = “technology owner” for AI.

Risk & Compliance Roles:

1. **Data Protection Officer (DPO)-** Responsible for privacy and data protection compliance.
2. **Risk Management Team –** They evaluate the risks for every AI system.
3. **Legal / compliance team -** They ensure all legal and regulatory requirements are followed.

Technical & Operational Roles:

1. **ML Engineers / MLOps Engineers** - They build and operate the model.
2. **AI product owners** - They ensure AI serves the right business purpose
3. **AI Security Lead / Security Architects -** They design how to protect AI systems.

Basically, Each role has a different responsibility:

- **CISO:** leads AI security and incident response
- **CTO/CIO:** approve tools and architecture
- **DPO:** ensures privacy compliance
- **Risk team:** assesses AI risks
- **Legal:** checks regulations and contracts
- **ML/MLOps:** build and operate models
- **AI Product Owner:** ensures AI solves a real business need
- **AI Security Lead:** designs protection controls
- **Data engineers, SOC, red team:** support security and monitoring