AI GOVERNANCE OPERATING MODEL

1. INTRODUCTION

1.1 Purpose of This Operating Model:

The AI Governance Operating Model defines the structure, roles, processes, controls, and decision-making mechanisms required to safely and responsibly deploy AI across the organisation.

1.2 Scope:

This model applies to:

- All AI/ML/GenAI systems
- Internal and external AI tools
- Third-party models (SaaS, APIs)
- All business units

2. AI GOVERNANCE PRINCIPLES

These principles guide all AI development and deployment:

- Accountability: clear ownership of AI decisions
- Transparency: explainability and documentation
- Fairness: prevent discrimination or harm
- Safety: avoid harmful outcomes
- Security: protect models from adversarial attacks
- Privacy: protect personal data
- Human Oversight: meaningful human control
- Lifecycle Governance: continuous monitoring

3. GOVERNANCE STRUCTURE

3.1 AI Governance Board

3.1.1 **Role:** Highest governing body for AI risk, ethics, and compliance.

3.1.2 Responsibilities:

- Approve high-risk use cases
- Approve AI policies and standards
- Oversee enterprise AI risk
- Resolve ethical escalations
- Review periodic AI performance and incidents

3.1.3 Members: CTO / CIO / CISO / DPO / Head of Legal / Head of Risk / AI Governance Lead (hierarchy of decision-making bodies)

3.2 AI Program Management Office (AI PMO)

3.2.1 Role: Operational governance and coordination.

3.2.2 Responsibilities:

- Manage AI documentation
- Maintain the AI Controls Catalogue
- Coordinate risk assessments
- Enforce AI lifecycle processes
- Support audits

3.3 AI Risk Management Function

3.3.1 Role: Own and operate AI risk management.

3.3.2 Responsibilities:

- Evaluate each use case for risk
- Maintain AI Risk Register
- Validate AI controls

- Validate MITRE ATLAS security mapping
- Issue risk acceptance or rejection

3.4 Data Protection Officer (DPO)

Ensures privacy and regulatory compliance.

Reviews:

- Data Cards
- Sensitive data usage
- Legal basis
- PDPA/GDPR compliance

3.5 Security & Red Team Function

Handles:

- Adversarial testing
- Prompt-injection protection
- Model extraction protection
- Penetration testing
- ATLAS threat control validation

3.6 Model Owners

Business or IT owners of a specific AI model.

Responsibilities:

- Performance monitoring
- Fairness monitoring
- Updating documentation
- Managing incidents

3.7 Human-in-the-Loop (HITL) Reviewers

Review high-risk decisions before execution.

4. AI LIFECYCLE GOVERNANCE

This is the core process which is mandatory for all AI initiatives.

4.1 Stage 1 - Use Case Intake

- **Required Template:** AI Use Case Intake Form
- **Activities:**
  - Problem definition
  - Value assessment
  - Data availability check
  - Initial risk screening

4.2 Stage 2 — Feasibility & Risk Assessment

- **Required Templates:**
  - Data Card
  - Model Card
  - AI Risk Assessment Form
- **Activities:**
  - Data readiness
  - Fairness evaluation
  - Privacy review
  - MITRE ATLAS threat assessment
  - Explainability feasibility
- **Decision:**
  - Low-risk → continue
  - Medium-risk → additional checks
  - High-risk → AI Governance Board review

4.3 Stage 3 — Model Development

- **Activities:**
    - Data preparation
    - Feature engineering
    - Model training
    - Bias testing
    - Explainability testing
    - Security control implementation
- **Deliverables:**
    - Updated Model Card
    - Fairness test report
    - Security test report

4.4 Stage 4 — Validation & Testing

- **Activities:**
    - Independent model validation
    - Bias validation
    - Performance validation
    - Stress and adversarial tests
    - Red-teaming
- **Deliverables:**
    - Model validation report
    - ATLAS threat validation report

4.5 Stage 5 — Approval & Sign-Off

- **Required Template:** AI Model Approval Form
- **Stakeholders:**
    - AI PMO
    - AI Risk Manager
    - Security Lead
    - DPO
    - AI Governance Board (for high-risk models)

4.6 Stage 6 — Deployment

- **Controls required:**
  - Access control
  - Fallback mechanism
  - Safe mode failure
  - API security
  - Logging & monitoring enabled

4.7 Stage 7 — Monitoring & Review

- **Continuous monitoring requirements:**
  - Performance drift
  - Data drift
  - Fairness by group
  - Hallucination rate (for LLMs)
  - Security anomalies
  - Incident logging
- **Required Template:** AI Audit Log
- **Periodic reviews:**
  - Monthly monitoring
  - Quarterly governance review
  - Annual model recertification

5. RACI MATRIX

Task / Deliverable	Model Owner	AI PMO	AI Risk	Security	DPO	AI Board
Use Case Intake	R	A	C	C	C	I
Data Card	R	A	C	C	A	I
Model Card	R	A	C	C	C	I
Risk Assessment	C	A	R	C	C	I
ATLAS Assessment	C	A	C	R	I	I
Model Approval	R	A	C	C	C	A
Monitoring	R	A	C	R	I	I
Incident Response	R	A	C	R	C	I

R = Responsible
A = Accountable
C = Consulted
I = Informed

6. GOVERNANCE DOCUMENTATION REQUIREMENTS

The following templates are mandatory:

- Model Card
- Data Card
- AI Use Case Intake Form
- AI Decision Log
- AI Risk Assessment Form
- AI Model Approval Form
- AI Audit Log
- MITRE ATLAS Threat Assessment Template

7. POLICIES REQUIRED

The Following Policies are required:

- AI Governance Policy
- Data Governance Policy
- Fairness & Ethics Policy
- Explainability Policy
- AI Security Policy
- AI Monitoring & Incident Policy
- AI Third-Party Risk Policy

8. PERFORMANCE & RISK METRICS

8.1 Performance Metrics:

- Accuracy
- F1 Score
- Latency
- Throughput

8.2 Fairness Metrics:

- Group error rates
- Disparate impact
- Equal opportunity

8.3 Security Metrics:

- Prompt injection attempts
- Model extraction attempts
- Anomaly scores

8.4 Operational Metrics:

- Drift rate
- Uptime
- Incident count

9. GOVERNANCE CADENCE

- Monthly AI Monitoring Report
- Quarterly AI Governance Committee
- Quarterly AI Security Review
- Annual Recertification
- Annual Third-Party AI Risk Review