

SKILLNAVORA · AI PRODUCT MANAGEMENT & GENAI
LAUNCHPAD

AI Governance & Responsible AI

Ship AI responsibly: principles and risks, regulations (EU AI Act, India's DPDP Act and AI guidelines, sector rules), AI risk and impact assessments, policies and documentation, and operating governance.

Edition 2026 · skillnavora.in

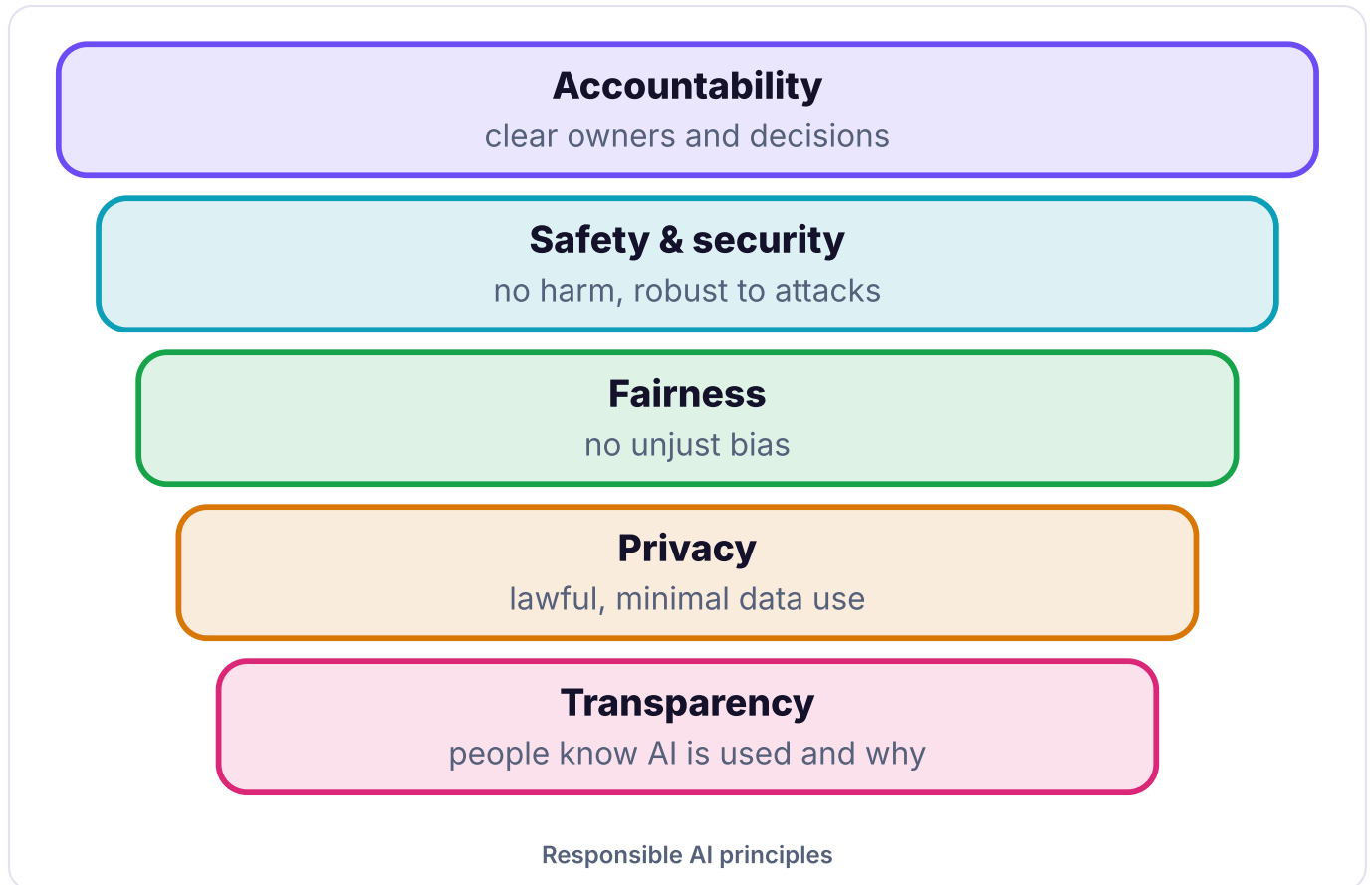
How to use this guide

Each class has goals, concepts with Indian examples, key takeaways and a practice exercise, from basic to advanced. Finish with the final project to build something you can show in interviews.

	Class	Level
Class 1	Principles and risks	Basic
Class 2	Regulations to know	Basic
Class 3	AI risk and impact assessment	Intermediate
Class 4	Policies and documentation	Intermediate
Class 5	Operating governance	Advanced
Class 6	Final project	Advanced
Toolkit: templates, cheat sheet, glossary, 5 interview questions, further reading		

Principles and risks

Know the main responsible-AI principles and risks.



Typical risks: harmful or wrong outputs, bias, privacy leaks, IP/copyright, security (prompt injection), over-reliance, and job or social impact.

Key takeaways

- Principles must turn into checks.
- List risks per feature.
- Name an accountable owner.

Practice exercise: List the top 5 risks of an AI hiring-screening feature.

Regulations to know

Understand the main laws and frameworks at a PM level.

Framework	What PMs should know
EU AI Act	Risk tiers: prohibited, high-risk (e.g. hiring, credit), limited-risk (transparency duties like disclosing chatbots), minimal; obligations phase in over several years
India: DPDP Act 2023	Consent, purpose limitation, data minimisation, rights of data principals; applies to personal data used in AI
India: government AI guidance	Advisories and governance guidelines on responsible AI, deepfakes and labelling; check current versions
Sector rules	RBI (lending, fraud), SEBI (investment advice), IRDAI (insurance), health regulators
Standards	NIST AI Risk Management Framework; ISO/IEC 42001 AI management systems

This is a learning summary, not legal advice; involve legal counsel for real decisions.

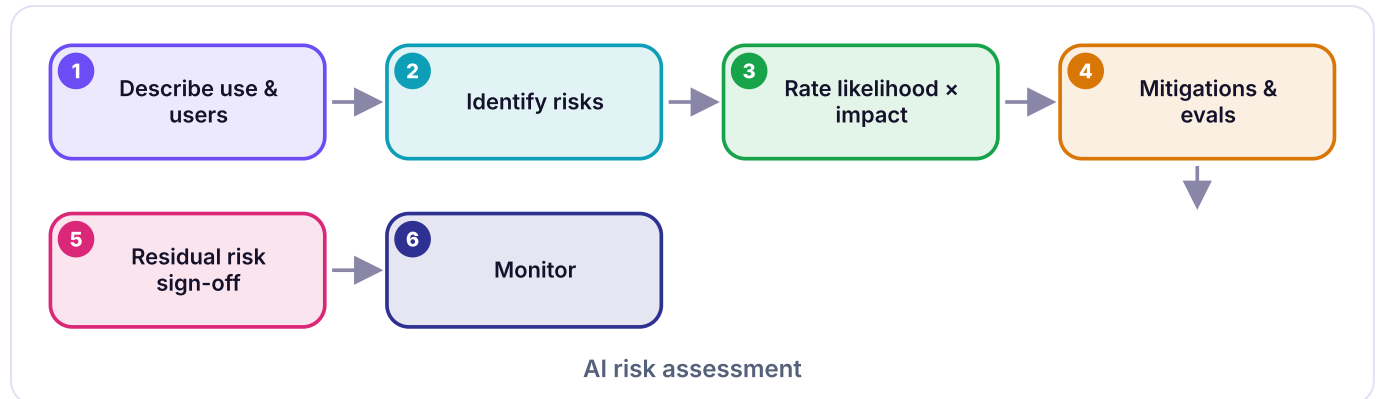
Key takeaways

- Know your feature's risk tier.
- Personal data → DPDP duties.
- Check sector regulators and current guidance.

Practice exercise: Classify 5 AI features by EU AI Act risk tier and explain.

AI risk and impact assessment

Assess a feature before launch.



Use evals and red-teaming results as evidence for each mitigation.

Key takeaways

- Assess before launch, not after incidents.
- Evidence = evals and red-team results.
- Sign off residual risk explicitly.

Practice exercise: Complete a risk assessment for an AI loan-eligibility assistant.

Policies and documentation

Write the documents governance needs.

- Company AI use policy (what tools, what data, approvals).
- Model/system cards: purpose, data, evaluation, limits, contacts.
- Data protection impact assessment for personal data.
- User-facing disclosures: "You're chatting with AI", AI-generated labels.
- Decision logs for high-impact choices.

Key takeaways

- Document purpose, data, evals and limits.
- Disclose AI to users.
- Keep decision logs.

Practice exercise: Draft a 1-page AI use policy for a 50-person startup.

Operating governance

Run governance without slowing teams down.

- Tiered review: light checklist for low-risk features, committee review for high-risk.
- Incident response: report, triage, rollback, communicate, learn.
- Audits: periodic eval and bias re-checks, access reviews.
- Vendor management: data terms, security, model changes.

Key takeaways

- Tier the process by risk.
- Have an incident playbook.
- Re-check periodically.

Practice exercise: Design a tiered AI review process for your company.

Final project

Govern a real AI feature.

For an AI feature, produce: risk tier, risk assessment table, mitigations with eval evidence, system card, user disclosure copy, DPDP checklist, incident playbook.

Key takeaways

- Governance is a product practice.
- Evidence over promises.
- Make it lightweight for low risk.

Practice exercise: Complete the governance pack.

Templates

AI risk register

```
risk | feature | likelihood (1-5) | impact (1-5) | mitigation | eval evidence | owner |  
status
```

Cheat sheet

Term / tool	Meaning / use
EU AI Act	EU law with risk-based AI obligations
DPDP Act	India's Digital Personal Data Protection Act, 2023
NIST AI RMF	US framework for AI risk management
ISO/IEC 42001	AI management system standard
System card	Document describing an AI system's purpose and limits

Glossary

Residual risk	Risk left after mitigations
Red-teaming	Trying to make the AI fail

5 interview questions with answers

Q1. What is responsible AI?

Building AI that is accountable, safe, fair, private and transparent, backed by processes and evidence.

Q2. How does the EU AI Act affect products?

Obligations depend on risk tier; high-risk uses like hiring or credit need risk management, data governance, documentation and human oversight.

Q3. What does DPDP mean for AI features?

Lawful consent/purpose, minimal data, user rights, security, and care with personal data in prompts and logs.

Q4. How do you run a risk assessment?

Describe use, identify risks, rate them, add mitigations with eval evidence, sign off residual risk, monitor.

Q5. How do you keep governance fast?

Tiered reviews, templates, automation of checks, clear owners.

Further reading and tools

- EU AI Act overview: <https://artificialintelligenceact.eu/>
- NIST AI Risk Management Framework: <https://www.nist.gov/itl/ai-risk-management-framework>
- ISO/IEC 42001: <https://www.iso.org/standard/81230.html>
- India DPDP Act (MeitY): <https://www.meity.gov.in/data-protection-framework>
- OECD AI principles: <https://oecd.ai/en/ai-principles>

© SkillNavora · skillnavora.in · Part of the AI Product Management and GenAI Launchpad programs. Practise with the free AI Tutor, AI PM Toolkit and Practice Lab on skillnavora.in.