AI Governance Checklist (EU AI Act)

Publisher: SimpleAct · https://simpleact.de
Version: 1.0
Contact: info@simpleact.de · support@simpleact.de
As of: March 2026 · Not legal advice

Legal notice

This checklist does not replace legal review. It structures typical governance questions in the EU AI Act context. Involve legal and compliance for binding decisions.

Keywords: AI governance, EU AI Act, compliance, RACI, audit, policy, risk management

---

Core problem and the SimpleAct framework

Core problem

Governance and **operational EU AI Act work** often run **in parallel instead of as one system**:

- Policies and RACI live in **decks**, while **real AI systems** sit in other tools.
- **Approvals** and ownership per system are **not standardized**.
- **Evidence** for boards and audits is missing a **consistent** format.
- **Shadow AI** undermines official control without a visible correction loop.

The SimpleAct framework

SimpleAct is the **AI Act compliance platform** built around a **shared five-phase reference model** across all materials:

Phase	Organizational focus	What SimpleAct brings together
1. Inventory	Transparency for systems, vendors, and data flows	A **central register** with consistent required fields
2. Risk & roles	Risk classes, deployer / provider, supply chain	**Guided classification** with documented decisions
3. Documentation	Annex IV, Art. 11, and related obligations	**Structured templates** instead of ad hoc files
4. Evidence & export	Defensible history; reports for legal, leadership, partners	**Unified exports** and traceable change records

5. Audit readiness	Updates when models, data, or products change	An **end-to-end chain** instead of folder and ticket silos

Note: This framework is the **same shared reference** in every SimpleAct document - guides, checklists, inventory, and documentation templates align to it.

---

1. Governance vs compliance

Aspect	Compliance	Governance
Focus	Meeting obligations	Steering, accountability
Artifacts	Evidence documents	Policies, approvals
Horizon	Deadlines, audits	Continuous control
Question	"Do we meet Art. X?"	"Who may approve what?"

Terms: governance framework, three lines of defense, policy lifecycle, risk appetite.

---

2. Roles and RACI (per AI system)

Activity	Responsible	Accountable	Consulted	Informed
Inventory	IT / AI owner	CISO / COO	Legal	Management
Risk class	AI owner	Legal/compliance	DPO	Audit
Go-live approval	Change board	Product	Legal	Support
Incident	SOC / ops	CISO	Legal	Regulator if needed

---

3. Policies and standards

- Acceptable use for **AI tools** (shadow AI rules)
- **Data classification** and purpose limitation
- **Vendor management** (DPA, subprocessors, GPAI considerations)
- **Retention** and deletion

---

4. Risk and approval workflow

1. Intake: new AI system or feature

2. Classification: EU risk + internal scoring
3. Approval: before production change
4. Review: quarterly + on model updates

Keywords: change management, model update, substantial modification.

---

5. Audit readiness

- Tamper-evident history (not "random PDFs")
- Exports for reviewers (reports, snapshots)
- Interview playbooks

---

6. Common mistakes

- Governance on paper only, no tooling
- No central inventory -> no prioritization
- Legal engaged only after launch

---

7. Glossary

Term	Meaning
RACI	Responsibility matrix
Shadow AI	Unapproved AI usage
Segregation of duties	Role separation

---

8. Compact checklist

- [ ] AI inventory complete
- [ ] Owner per system
- [ ] Risk class documented
- [ ] Pre-production approval
- [ ] Incident process defined
- [ ] Business training done

---

9. Three lines of defense (deep dive)

First line: business owns usage descriptions.
Second line: risk/compliance defines standards and samples.
Third line: internal audit / external audit receives **structured exports**.

---

10. Scenarios

A: Marketing uses external LLM without IT approval -> **shadow AI**; fix with inventory + allowlist.
B: Product ships new model -> trigger **change**, reassess risk, update documentation.
C: Auditor asks for risk-class evidence -> point to documented rationale + history.

---

11. SEO keyword clusters

AI governance checklist, EU AI Act organization, AI Act roles, compliance evidence, AI audit, AI policy, AI risk management.

---

12. How SimpleAct helps

SimpleAct combines **inventory**, **risk classes**, **documentation**, and **exportable reports** in an **AI Act Compliance Platform** - so governance decisions are backed by **data**, not spreadsheets.

Pricing: From €199/month (see website).

Appendix A: 45-minute workshop prompts

1. Which **AI systems** run today **without** formal approval?
2. Who is **accountable** for a high-risk HR use case?
3. What **evidence** exists for the last model change?
4. How is **shadow AI** detected (network, allowlists)?
5. Which **KPIs** does leadership track (systems count, open risks)?

Appendix B: Extended RACI detail

Task	R	A	C	I
DPIA / FRIA trigger	Legal	DPO	IT	Management

Vendor due diligence	Procurement	Legal	Security	Owner
AI API penetration test	Security	CISO	Vendor	Product

Appendix C: FAQ (deep dive)

Q: Must the executive team know every AI system?
A: At least **categories** and **top risks** - otherwise risk acceptance is not meaningful.

Q: Is an annual audit enough?
A: For **stable** systems, maybe; with **monthly** model updates, continuous review is more realistic.

Q: How does ISO 27001 relate to the AI Act?
A: ISMS provides controls; the AI Act adds **domain-specific** duties - map them in a **matrix**.

Appendix D: Extended keyword list

AI Act governance, EU AI regulation enterprise, AI policy template, AI risk committee, AI Act accountability, compliance evidence AI.

Appendix E: Governance maturity (staged rollout)

Level	Posture	Typical artifacts
1 - Ad hoc	Shadow tools, spreadsheets	Informal owner list
2 - Defined	Policy published	RACI, acceptable-use policy
3 - Managed	Quarterly reviews	Risk register, vendor attestations
4 - Optimized	Continuous monitoring	Automated inventory, audit dashboards

Keywords: AI governance maturity model, AI risk register enterprise, continuous compliance AI.

Appendix F: Sample escalation path (incident)

1. **Detect** (SOC / user report)
2. **Triage** (severity, PII, Annex III proximity)
3. **Contain** (disable feature flag, revoke keys)

4. **Notify** (legal, DPO, customer contract owners)
5. **Learn** (post-incident review, update controls)
