Template: AI System Inventory (AI Asset Register)

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 template does not replace legal review. It helps register and classify AI systems; binding classification requires legal and compliance on a case-by-case basis.

Keywords: AI inventory, AI register, shadow AI, risk classification, EU AI Act

---

Core problem and the SimpleAct framework

Core problem

Without a defensible **inventory**, you cannot ground **risk** and **evidence**:

- **Shadow AI** and vendor APIs stay **partly invisible**.
- **Spreadsheets** and ad hoc lists are **neither** revision-safe **nor** audit-ready.
- **Mapping** from asset to **risk class** is often missing.
- There is **no single source of truth** for owners, versions, and data flows.

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. Purpose

An **AI inventory** is the foundation for **risk classification**, **prioritization**, and **evidence** for internal and external reviews.

---

2. Master data (required fields)

Field	Description
System ID	Unique ID
Name	Product/model name
Vendor	Supplier
Version	Release/model version
Owner	Business owner
Department	Using org unit
Purpose	Business use case
Data types	Personal data? sensitive?
Interfaces	API, SaaS, on-prem

---

3. Risk & EU AI Act

Field	Notes
EU risk class	minimal / limited / high / unacceptable
Rationale	Short, auditable
Annex III	Any listed use case applies?
GPAI link	Base model / fine-tuned?

Terms: deployer, provider, high-risk AI, conformity.

---

4. Technology & operations

Field	Description
Hosting region	EU / non-EU
Model type	LLM, vision, tabular
Training	In-house / vendor / API-only
Monitoring	Drift, quality
Backup / availability	if relevant

---

5. Compliance & contracts

- DPA in place?
- Subprocessors known?
- Retention defined?
- RBAC enforced?

---

6. Shadow AI

Shadow AI: tools without IT approval. Mitigations: allowlists, monitoring, training, reporting channel.

---

7. Review cadence

Frequency	Action
Quarterly	Sample inventory quality
On release	Register new systems
On incident	Update record

---

8. Example row (anonymized)

System ID	Name	Vendor	Purpose	Risk

AI-014	HR assist	Vendor X	Pre-screening	High (Annex III)

---

9. Checklist

- [ ] All known AI systems captured
- [ ] Owner assigned
- [ ] Risk rationale documented
- [ ] Contracts linked
- [ ] Next review date set

---

10. Glossary

Term	Meaning
Asset register	Catalog of digital assets
Data lineage	Traceability of data flows

---

11. Deep dive: textual data-flow

1. **Source** -> raw data
2. **Processing** -> features / prompts
3. **Model** -> output
4. **Use** -> decision / UI
5. **Storage** -> logs, retention

---

12. SEO keyword clusters

AI inventory template, AI system register, EU AI Act inventory, high-risk AI inventory, shadow AI enterprise.

---

13. How SimpleAct helps

SimpleAct provides a **structured inventory** with **risk classes** and **exports** as part of an **AI Act Compliance Platform**.

Pricing: From €199/month.

Appendix A: Extended optional fields

Field	Why
Business criticality	Prioritization under constraints
PII exposure	Privacy focus
Model provider region	Third-country / Schrems II
Cost center	Chargeback

Appendix B: Sample matrix "department x risk"

Department	Systems count	High-risk (estimate)
HR		
Sales		
Engineering		

Appendix C: FAQ

Q: How often to refresh?
A: Quarterly + on every new tool onboarding.

Q: What about "shadow GPT"?
A: Treat as **incident**, register, tighten policy.

Appendix D: Extended keywords

AI asset register, EU AI Act inventory fields, enterprise AI catalog, third-country transfer AI, vendor risk AI.

Appendix E: Data quality rules

- Avoid duplicate records for the same API instance
- Normalize vendor strings (e.g., "OpenAI" vs. "api.openai.com")
- Link to CMDB / ITSM IDs

Appendix F: IAM, access, and logging

Aspect	Inventory field / note
Authentication	SSO, API keys, service accounts - who may call the model?
Authorization	RBAC/ABAC, least privilege
Logs	Retention, tamper resistance, access limited to authorized roles
Key rotation	Cadence and owners

Without a clear **access chain**, evidence for **monitorability** and **incident response** is often missing - capture these for every production AI system.
