AI Vendor Assessment Template

A practical framework for evaluating AI vendors before granting access to enterprise systems, data, and business processes.

Assessment Framework

01 Security
How systems, data, and connections are protected.

02 Governance
Who is accountable and how the AI is overseen.

03 Compliance
Which regulations and standards are met.

04 Transparency
How explainable and documented the AI is.

05 Permissions
What access the AI requests and holds.

06 Data Handling
How data is stored, used, and retained.

07 Reliability
How consistently the service performs.

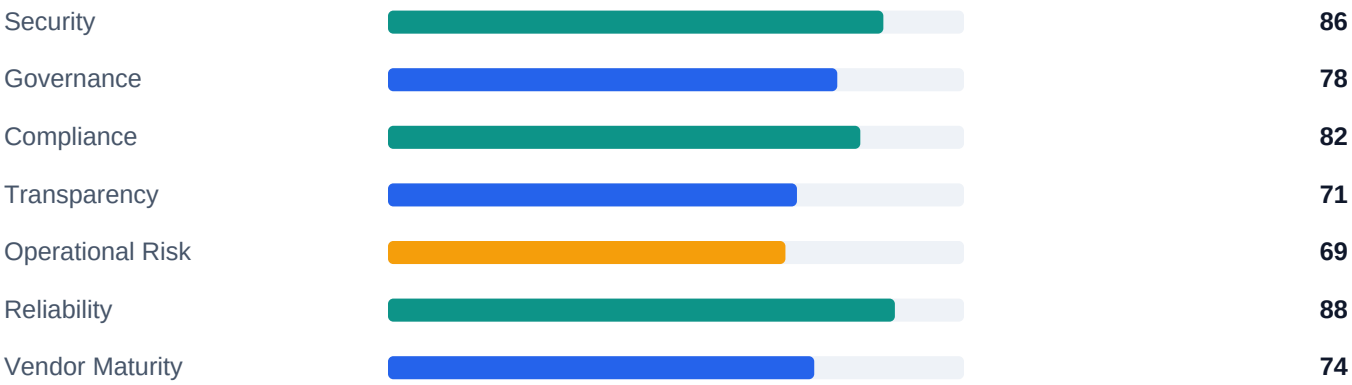
08 Operational Risk
The business impact if it fails.

09 Vendor Maturity
The vendor's track record and stability.

15 Questions to Ask Every AI Vendor

- [ ] 01 What data can your AI access?
- [ ] 02 How is customer data protected?
- [ ] 03 What permissions does the AI require?
- [ ] 04 Are AI actions logged and auditable?
- [ ] 05 Can permissions be revoked immediately?
- [ ] 06 How are integrations secured?
- [ ] 07 Does the AI connect through MCP servers or other tools?
- [ ] 08 What governance controls exist?
- [ ] 09 What compliance frameworks are supported?
- [ ] 10 Can outputs be reviewed by humans?
- [ ] 11 How are model updates managed?
- [ ] 12 What monitoring exists?
- [ ] 13 How are incidents handled?
- [ ] 14 What business continuity plans exist?
- [ ] 15 What independent assessments have been performed?

Vendor Scorecard (Sample)



Overall Trust Score: 78 **Risk Rating: Medium**

Common Red Flags

- ! Unknown data usage
- ! Excessive permissions
- ! No audit trail
- ! No governance controls
- ! No security documentation
- ! No incident response process
- ! No transparency