Vendor AI Assessment Checklist

Vendor name: [Name] **Product / service:** [Name] **Assessed by:** [Name and role] **Date:** [Date]

Complete this checklist alongside the standard Use Case Registration Form for any vendor-procured AI system.

Transparency and Documentation

- ☐ Vendor provides a model card or equivalent documentation
- ☐ Vendor can explain how the model was trained, what data was used, and what its known limitations are
- ☐ Vendor publishes bias testing or fairness audit results
- ☐ Vendor is transparent about sub-processors and third-party model use

Notes:

Data Practices

- ☐ Data storage and processing locations are documented
- ☐ Customer data use for model training is clearly disclosed
- ☐ Organization can opt out of data use for model training
- ☐ Data retention and deletion policies are documented
- ☐ Vendor handles data subject rights (access, deletion, correction)
- ☐ Data flows between the vendor and third parties are mapped

Notes:

Security

- ☐ Vendor holds SOC 2, ISO 27001, or equivalent certification
- ☐ Vendor has performed adversarial testing (red-teaming, prompt injection testing for generative AI)
- ☐ Vulnerability disclosure and patching process is documented
- ☐ Vendor has a defined incident response process and notification timeline

Notes:

Contractual

- ☐ Contract provides audit rights
- ☐ Liability and indemnification terms address AI-specific harms (bias, hallucination, data leakage)
- ☐ Organization can exit the contract and retrieve or delete its data
- ☐ Service levels cover model performance and availability, not just uptime
- ☐ Contract addresses what happens when the vendor changes or discontinues the model

Notes:

Onboarding Checklist

- ☐ Deployed configuration matches what was assessed
- ☐ Customizations, fine-tuning, or prompt engineering is documented
- ☐ Guardrails, content filters, and access controls are enabled
- ☐ Affected users are informed about the AI, its purpose, and limitations
- ☐ Appropriate use guidance is published
- ☐ User feedback channel is established
- ☐ System is added to the AI Inventory with vendor-specific fields

Risk Tiering Note

Vendor cases should not receive a lower risk tier simply because the AI is third-party. Reduced visibility into model internals may warrant a higher tier than an equivalent in-house system.

Risk tier assigned: [ ] Tier 1 [ ] Tier 2 [ ] Tier 3 [ ] Tier 4

Overall Assessment

Recommendation: [ ] Proceed to onboarding [ ] Proceed with conditions [ ] Do not proceed [ ] Need more information

Conditions (if any):

Assessed by: [Signature / name] **Date:** [Date]