Evaluating an AI governance control

A practical checklist for security and procurement teams. The questions below separate a control that reports cleanly from one that holds up under a regulator, an auditor, or a court. **Ask every vendor the same questions, and watch where the answers turn into qualifiers.**

Coverage

- [ ] **Does it see unsanctioned tools, personal accounts, and new providers, or only what we configured it to watch?**
  If coverage depends on integration, shadow AI is invisible to it by design.
- [ ] **Does it work across every provider and tool that speaks HTTPS, without changes to those tools?**
  Per-tool or per-provider coverage leaves gaps that grow every time staff adopt something new.

The decision

- [ ] **Is the decision made before content leaves the device, or only observed after it has already gone?**
  After-the-fact detection cannot prevent the leak; it only documents it.
- [ ] **When a decision is uncertain, does it fail closed?**
  A control that defaults to allow under ambiguity is not a control in the cases that matter most.

Data and keys

- [ ] **Who holds the encryption keys, and can the vendor read our content?**
  If the vendor can read it, the vendor is now a custodian of your most sensitive data, and a new breach surface.

Evidence

- [ ] **Is the record signed at the source and tamper-evident, or is it an ordinary log the keeper could edit?**
  Only a signed, hash-chained record survives a challenge to its integrity.
- [ ] **Do we hold the evidence, and can we verify it without trusting the vendor?**
  Evidence you cannot independently verify is the vendor's word, not yours.

Deployment

- [ ] **Does it run on our infrastructure, including air-gapped environments?**
  Cloud-only controls cannot serve the most regulated environments, where the need is greatest.

Commercial

- [ ] **Is pricing predictable, and can we buy through cooperative purchasing vehicles?**
  Per-seat annual pricing and routes like GSA or NASPO shorten the path from decision to deployment.

The right control answers all of these without a qualifier. Most answer the first four and start hedging at evidence.