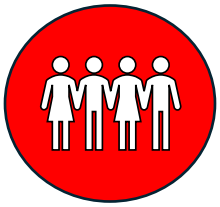
Shadow IT Governance Starter Kit

The Three Truths (from CIO/CISO interviews)

Shadow IT—technology adopted outside central IT oversight—creates both opportunity and risk in higher education. This starter kit provides campus leaders with a practical framework to gain visibility, classify tools by risk, and respond with proportionate governance strategies. Built from CIO and CISO insights, it translates research into actionable checklists, tiered responses, and a 90-day roadmap. Institutions can adapt these tools to their own policies and culture, using the kit as a foundation for more mature governance practices.



Risk management is relational.
Trust makes shadow IT visible; curiosity keeps partners

Governance is cultural.
Policies work only when norms, incentives, and language align.

Shadow IT is contextual.
Responses should be tiered by data sensitivity, purpose, and campus

---

Visibility Pipeline

Signals → Correlate → Act

- **Signals.** Procurement/ProCard, SaaS licensing, identity/endpoint logs, network/cloud telemetry.
- **Correlate.** Join signals to surface unmanaged tools; prioritize by data class and regulatory scope.
- **Act.** Route to a tiered response (allow & monitor; co-govern & harden; integrate or decommission).

Quick start: begin with Procurement + Identity *data; add* Endpoint/Network *as capacity allows.*

Tiered Response Matrix (Policy Starters)

Tier	When to use	Guardrails (examples)	Typical next step
Allow & monitor (Low)	No sensitive data; pilot/teaching tool; low blast radius	Notify central IT; basic security checklist; auto-renew review	Add to "declared tools" register; reassess in 90 days
Co-govern & harden (Medium)	Institutional or FERPA-adjacent data; moderate adoption	DPA/BAA; SSO/MFA; data classification tag; owner + steward named	Security review; onboarding playbook; unit MOU
Integrate or decommission (High)	Regulated or high-risk data (e.g., GLBA/PHI); broad reliance	Central logging; backups; IR plan; vendor risk assessment	Migration or integration plan with timeline

Prepared by: **Joel I. Larson, PhD** — Kalamazoo Valley Community College • Contact: joel@joelilarson.com • More resources: joelilarson.com

90-day roadmap

- **Weeks 1–2 — Discover.** Interview 8–12 stakeholders; pull 6–12 months of procurement/licensing; snapshot identity/endpoint logs; list declared tools.
- **Weeks 3–6 — Design.** Classify 15–30 tools by data class; draft tier matrix + decision paths; policy starters; pilot with two units.
- **Weeks 7–12 — Deliver.** Finalize playbooks/templates; publish declared-tools register; two trainings; agree on 90-day follow-ups.

Matrix Worksheets are available for download from joelilarson.com

Impact metrics (pick 3–5)

Declared tools ↑ · High-risk exceptions ↓ · Time-to-visibility ↓ · Time-to-onboard ↓ · Stakeholder satisfaction ↑

Visibility Checklist (pick 6–8 this month)

- Procurement/ProCard export (6–12 months)
- SaaS/licensing list vs. known inventory
- Identity/SSO apps vs. unmanaged logins
- Endpoint report (installed apps/high-risk binaries)
- DNS/firewall/CASB hits to unknown domains
- Help-desk tickets mentioning outside tools
- Contract addendum check (DPA/BAA)
- Backup/DR coverage for non-central systems

Discovery Prompts (use curiosity first)

1. What problem are you solving, and for whom?
2. Who needs to see or change the data?
3. What data leaves campus or the primary system?
4. What breaks if this is offline for a day? a week?
5. How is access granted today (SSO, shared logins)?
6. Where are backups, and who restores?
7. Which agreement or click-through governs this tool?

Risk-Tier Quick Test (fast triage)

Score 1 point per “yes.” 0–1 = Low · 2–3 = Medium · 4–5 = High

[ ] Regulated data (FERPA/GLBA/PHI/export-controlled)
[ ] Broad reliance (≥ 2 units or ≥ 50 users)
[ ] No SSO/MFA
[ ] No backups/DR plan
[ ] Vendor outside existing agreements