Purpose. To examine how technology executives at U.S. public R1 universities apply risk management strategies to shadow IT while preserving innovation and academic autonomy.
Research question. *How do technology executives at public R1 HEIs in the U.S. apply risk management strategies in response to shadow IT?*

Method. Generic qualitative inquiry with purposive sampling of **11 leaders** (7 CIOs, 4 CISOs) from separate public R1 institutions. Semi-structured interviews (≈45–75 minutes) with transcript checks. Thematic coding in NVivo 15; interpretation informed by **Technology Threat Avoidance Theory (TTAT)**.

SIGNALS Procurement/ ProCard & SaaS licensing; identity/endpoint logs; network & cloud telemetry (e.g., DNS, firewall, CASB).

CORRELATE Join signals to surface unmanaged tools; prioritize by data class and regulatory scope.

ACT Tiered response: allow & monitor (low risk), co-govern & harden (medium), integrate or decommission (high)

"We stopped opening with policy and started with curiosity: *What problem were you solving?* That one change made people bring us their tools before they broke something."
— CIO, public R1

DOT POLL
Where do you find shadow IT first?
- ○ Network Telemetry
- ○ Procurement/ProCard
- ○ Help Desk
- ○ Audit/Compliance
- ○ Other:_____

Joel I. Larson, PhD - Director of IT Support & Network Services
Kalamazoo Valley Community College

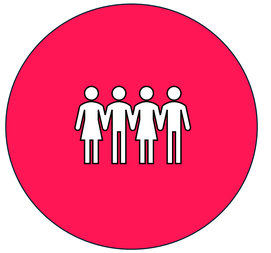
Beyond the Shadows: How IT Leaders in Higher Education Manage Shadow IT Risk

Is your "department of no" creating more risk than it prevents?

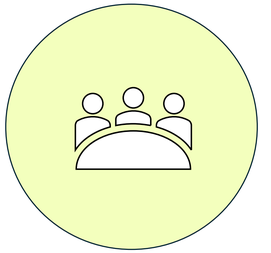
Turn your "department of no" into a "department of know."

Scan for links to Executive Summary, Full Dissertation, References, and More

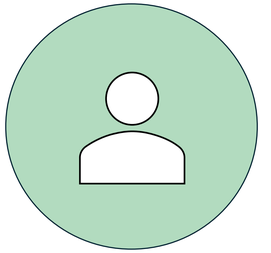
Findings



Risk Management is Relational
Trust makes shadow IT visible; curiosity keeps partners engaged.



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



Shadow IT is Contextual
Tier responses by data sensitivity, purpose, and politics.