Leadership Preview

Google Workspace Risk Exposure Baseline for Multi-Campus Schools

Typical audit duration: 3–5 working days | Leadership time required: ~90 minutes total

LEAD ANALYST

Arttu Karppanen

Incident-informed Google Workspace security reviews

Web: Working-Draft.org

Telegram: t.me/AtPitou

Address First
3 areas typically create the fastest path to serious exposure.

Secondary Controls
2 areas often require tuning after the urgent issues are contained.

Existing Strengths
4 positives usually exist before remediation even starts.

RISK DOMAIN	LEADERSHIP SIGNAL
RED | ADDRESS THESE FIRST	
Offboarding And Identity Lifecycle Former or suspended staff can retain meaningful access beyond the expected employment boundary.	Quiet persistence after role change can become a confidentiality incident. It usually means offboarding, access review, and ownership transfer are not operating together.
Logging And Human Alert Routing Abuse is often discovered after deletion, exfiltration, or policy bypass has already happened.	Late discovery turns manageable drift into a reportable incident with operational impact. Strong controls still fail in practice when no human is accountable for the alert.
Shared Drive Governance Ownerless content and broad editor rights weaken accountability, recovery, and change control.	Integrity events become harder to reverse when no clear ownership model exists. The school loses clean lines of responsibility at the moment they matter most.
YELLOW | SECONDARY REMEDIATION LAYER	
OAuth Grants And Third-Party Apps Old app consents and shadow integrations can keep data access alive after the original need is gone.	Delegated access weakens governance even when the main account policy appears healthy. This is usually fixable once someone inventories what was actually approved.
External Sharing And Student Sessions Convenience settings can broaden exposure far beyond the intended audience for staff and student data.	Collaboration risk grows when open sharing is not paired with clear session boundaries. The issue is usually structural drift, not individual user carelessness.

Central Identity Plane

Your campuses already have one control surface for users, roles, and core policy. That means visible risk reduction can happen quickly.

Containment Levers Already Exist

Sharing, protocol, and session controls can usually be tightened without replatforming. That keeps cost and disruption lower.

Auditability Is Available

Useful administrative evidence already exists inside Workspace when someone is assigned to read it. That is the beginning of institutional memory.

Secure Passwords and MFA consistently enforced

Password best practices are in place with minimum mixed case characters with numerals and special character-requirements. MfA is consistently enforced at Admin account level, and a fair few staff members / teachers have voluntarily enrolled!

How Evidence Is Gathered

1. Admin Console policy review
2. Identity and offboarding control checks
3. Drive and external-sharing review
4. Log retention and alert-routing review

Leadership Output

- Traffic-light risk summary
- Control gaps by risk area
- Mitigation steps ranked by impact versus effort

Typical First 30-Day Outcomes

- Former staff access boundary enforced automatically
- Alert routing assigned to named roles
- Shared drive ownership model restored
- External sharing defaults tightened
- Legacy access paths removed

Assessment Basis

- Built from anonymized baseline assumptions typical of Phnom Penh schools.
- Framed by the control failures documented in IR-2025-1021 and IR-2026-0108, plus the ISO 27001-aligned resilience framework in the white paper.

This scorecard is intentionally made to be processed at a glance, and will be backed up by a full audit report.