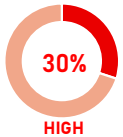
POLICY COMPLIANCE GAP ANALYSIS

RISK LEVEL OVERVIEW



Control Domain	Current State	Framework Requirement	Gap Identified	Risk Level	Owner	Remediation Plan	Target Date	Status	Evidence / Notes
Password Policy	Only length enforced	SOC 2 / ISO 27001 require complexity & rotation	Missing complexity & expiration rules	Medium	IT Security	Update policy & enforce system settings for complexity & reset	Q4 2025	In progress	AD password policy screenshot
Data Backup	Daily backups, not tested	SOC 2 requires tested recovery	No restoration test done	High	IT Ops	Schedule quarterly recovery drill	Q3 2025	In progress	Backup logs
Access Control	Broad user permissions	ISO 27001 requires least privilege / RBAC	No role-based access structure	Low	IT Manager	Implement RBAC & quarterly reviews	Q4 2025	Open	Access control list
Incident Response	Plan exists, never tested	SOC 2 requires tested IR plans	No exercises done	Medium	SecOps	Conduct tabletop drill & document lessons learned	Q3 2025	Closed	IR plan document
Vendor Risk Management	No vendor reviews done	SOC 2 requires vendor due diligence	No vendor assessments	Medium	Compliance	Create vendor risk questionnaire & review process	Q4 2025	In progress	Vendor contracts
Data Encryption	Encrypted in transit only	SOC 2 & ISO require at-rest + transit	No encryption at rest	High	IT Security	Enable DB & storage encryption	Q4 2025	Open	DB config evidence
Change Management	Ad hoc IT changes	ISO 27001 requires formal approval process	No documented change controls	Low	IT Ops	Establish change approval workflow	Q1 2026	Open	Change request logs
Security Awareness	Training at onboarding only	SOC 2 requires annual refreshers	No recurring training	Medium	HR / Compliance	Launch yearly training & phishing tests	Q4 2025	In Progress	Training records
Physical Security	Locked doors only	ISO 27001 requires facility monitoring	No visitor logs / CCTV	Medium	Admin	Implement visitor log + surveillance cameras	Q2 2026	Open	Visitor log book
Data Retention	Data kept indefinitely	ISO 27001 requires retention schedules	No purge process	High	Compliance	Create retention policy & automate purging	Q4 2025	In Progress	Policy draft