Remediation Roadmap

Teton Risk Advisory Group · Cybersecurity & IT Risk Management

Prepared for District 101 | June 30, 2026

Client	District 101
Planning horizon	36-month phased program · 3 phases
Total remediation items	203

Critical: 34 | High: 79 | Medium: 90

EXECUTIVE SUMMARY

District 101's 36-month cybersecurity roadmap strengthens its defenses against evolving threats, ensuring the confidentiality, integrity, and availability of sensitive student data. This strategic plan builds a robust posture that balances security with educational needs, fostering trust among students, parents, and staff. By the end of this journey, District 101 will have established a mature cybersecurity program.

PROJECTED SECURITY POSTURE

Projected (+1 tier) **3.51**
Every control one tier up

With 2→3 lifts **3.64**
Lowest controls to level 3

Every control +1 tier Lowest lifted to level 3

Raising every control one tier lifts projected NIST CSF posture from 2.76 today to 3.51. Adding the 34 further 2→3 lifts to a floor of 3 reaches 3.64. The national K-12 average is 2.54.

Two projections are shown. The first raises every assessed control by one maturity tier. The second adds the further 2→3 lifts that bring the lowest-maturity controls up to a floor of level 3. The horizontal benchmark line is the national K-12 average from the CIS/MS-ISAC Nationwide Cybersecurity Review (NCSR) — originally a 1–7 scale, normalized to this 1–5 axis — and applies to the overall score only. This is a planning projection, not a guarantee.

P1 · FOUNDATIONS · 0–6 MONTHS · 25 ITEMS

Phase 1 lays the groundwork for a resilient cybersecurity posture by establishing foundational controls, including risk assessment, incident response, and compliance frameworks, providing a solid base for subsequent phases.

WS-01 · GOVERNANCE, RISK & POLICY · 3 ITEMS

Finding	Severity	Current Maturity	What earns each maturity step
Regulatory Compliance Policy Affected: All systems and data	Critical	1	**REACH LEVEL 2** Key regulations are known informally but no formal policy assigns ownership or defines compliance monitoring. **REACH LEVEL 3** Regulatory compliance policy exists but does not cover all applicable regulations, compliance status is not tracked, or no one is responsible for monitoring regulatory changes.
Risk Assessment Program Affected: All systems and data	Critical	1	**REACH LEVEL 2** Risk is discussed informally or only after incidents, with no methodology or schedule. **REACH LEVEL 3** A risk assessment program exists but assessments are not conducted on a defined schedule, or results are not tracked to treatment.
Termination & Offboarding Security Policy Affected: All systems and data	Critical	1	**REACH LEVEL 2** Informal offboarding checklist exists but is not consistently followed and access revocation is delayed. **REACH LEVEL 3** Offboarding policy exists but does not define revocation timelines for all system types, does not address cloud accounts, or does not include an exit security interview.

WS-02 · IDENTITY & ACCESS · 5 ITEMS

Finding	Severity	Current Maturity	What earns each maturity step
Account Deprovisioning and Leaver Process Affected: All systems and applications with user accounts	Critical	1	**REACH LEVEL 2** Accounts disabled within 1 business day of departure notification from HR; process documented; checked periodically. **REACH LEVEL 3** Automated account disablement triggered by HR system departure event; all system access reviewed at departure (not just primary account); process tested with spot checks.
Cloud User MFA and Conditional Access Affected: All cloud-based systems and applications	Critical	1	**REACH LEVEL 2** MFA enforced for all users on cloud platforms (M365, Google Workspace); legacy authentication blocked. **REACH LEVEL 3** Conditional access policies deployed — high-risk sign-ins (new device, unfamiliar location) require step-up authentication.
Electronic Access Control System Affected: All systems and data within the facility	Critical	1	**REACH LEVEL 2** Badge or PIN access on main entrances and all sensitive areas (server rooms, HR offices, finance areas); logs maintained 30+ days. **REACH LEVEL 3** Access logs reviewed regularly for anomalies; multi-factor physical access for highest-sensitivity areas; access rights recertified at least annually and upon departure.
Key and Badge Management Affected: Sensitive areas and equipment within the facility	Critical	1	**REACH LEVEL 2** Badge issuance logged; departing employees required to return badges on last day; lost badges reported and deactivated promptly. **REACH LEVEL 3** Badge inventory reconciled quarterly; master key inventory maintained with controlled issuance; badge deactivation tied to HR offboarding workflow.
Physical Security Perimeter Affected: All systems and data within the facility	Critical	1	**REACH LEVEL 2** Primary entry points controlled; restricted areas marked and locked; secondary exits alarmed. **REACH LEVEL 3** Physical security perimeter reviewed at least annually; all entry points inventoried and assessed;

Finding	Severity	Current Maturity	What earns each maturity step
			loading dock access controlled and logged.

WS-03 · DETECTION, LOGGING & IR · 6 ITEMS

Finding	Severity	Current Maturity	What earns each maturity step
Incident Classification and Declaration Affected: All systems and data	Critical	1	**REACH LEVEL 2** Incident definition and severity levels documented; escalation path clear; declaration authority assigned. **REACH LEVEL 3** Severity classification matrix (P1-P4 or equivalent) with response time SLAs per level; all staff know how to escalate a potential incident.
Incident Response Plan (IRP) Affected: All systems and data	Critical	1	**REACH LEVEL 2** Basic incident response procedures exist informally or in a single person's knowledge. **REACH LEVEL 3** A documented IRP exists but has never been tested, key contacts are outdated, or it is missing required phases (containment, eradication, recovery).
Insider Threat Response Playbook Affected: All systems and data	Critical	1	**REACH LEVEL 2** Insider threat is mentioned in the IRP but no specific investigation steps are defined. **REACH LEVEL 3** A basic insider threat playbook exists but does not address legal and HR coordination, evidence preservation, or the distinction between malicious and negligent insiders.
Post-Incident Review Process Affected: Incident Response Team, IT systems	Critical	1	**REACH LEVEL 2** PIR conducted after significant incidents; key findings documented; IRP updated based on findings. **REACH LEVEL 3** PIR conducted within 2 weeks of incident resolution; cross-functional review including IT, legal, and communications; root cause documented.
Simulation Results and Remediation Affected: Employee email and network access	Critical	1	**REACH LEVEL 2** Employees who click receive immediate training redirect; results reviewed by security team. **REACH LEVEL 3** Repeat offenders identified and receive mandatory remedial training; department-level results shared with managers.
Tabletop Exercise Program	Critical	1	**REACH LEVEL 2**

Finding	Severity	Current Maturity	What earns each maturity step
Affected: Incident Response Team, IT systems			Annual tabletop exercise conducted using a realistic scenario; key IRT members participate; findings documented. **REACH LEVEL 3** Scenario reflects current threat landscape (e.g., ransomware hitting during peak operations, data breach notifying a regulator); gaps identified and tracked to remediation.

WS-04 · ASSET & VULNERABILITY MGMT · 1 ITEM

Finding	Severity	Current Maturity	What earns each maturity step
Remediation SLAs by Severity Affected: All systems with identified vulnerabilities	Critical	1	**REACH LEVEL 2** SLAs defined: critical ≤14 days on internet-facing, high ≤30 days, medium ≤90 days. **REACH LEVEL 3** SLA compliance tracked and reported monthly; SLA breaches escalated to leadership; exceptions formally approved with compensating controls.

WS-05 · DATA PRIVACY & K-12 COMPLIANCE · 2 ITEMS

Finding	Severity	Current Maturity	What earns each maturity step
Privacy Policy & PII Handling Policy Affected: Systems containing PII	Critical	1	**REACH LEVEL 2** A public-facing privacy notice exists but no internal PII handling procedures are documented. **REACH LEVEL 3** PII handling policy exists internally but does not fully address data subject rights, cross-border transfers, or processing purpose limitation.
State Breach Notification Compliance Affected: Student data and systems	Critical	1	**REACH LEVEL 2** Staff are generally aware notification may be required, but no documented procedure, timelines, or template notices exist. **REACH LEVEL 3** A breach-notification procedure exists referencing the applicable state law, but notification timelines, recipient lists, and content requirements are incomplete or untested.

WS-06 · THIRD-PARTY / VENDOR RISK · 2 ITEMS

Finding	Severity	Current Maturity	What earns each maturity step
Data Processing Agreements Affected: All systems and data handled by third-party vendors	Critical	1	**REACH LEVEL 2** DPAs required for all vendors processing personal data; covers data types, purpose, retention, and deletion. **REACH LEVEL 3** DPAs reviewed annually or at contract renewal; FERPA school official designations or BAAs in place where required; sub-processor lists maintained.
Vendor Access Controls and Least Privilege Affected: All systems accessed by vendors	Critical	1	**REACH LEVEL 2** Vendor accounts are separate from employee accounts; access limited to systems required for the vendor's function; vendor access reviewed when scope changes. **REACH LEVEL 3** Vendor access provisioned through a defined process; MFA required for all vendor remote access; vendor session activity logged.

WS-07 · RESILIENCE & PHYSICAL · 6 ITEMS

Finding	Severity	Current Maturity	What earns each maturity step
Backup & Restore Policy Affected: All systems and data	Critical	1	**REACH LEVEL 2** Backups occur but no policy defines scope, frequency, retention, or testing requirements. **REACH LEVEL 3** Backup policy exists but restoration is never tested, backups are stored only onsite, or ransomware-resilient (immutable) backups are not maintained.
BCM Policy and Scope Affected: All organizational systems and data	Critical	1	**REACH LEVEL 2** Some continuity awareness exists but no policy, objectives, or scope. **REACH LEVEL 3** A BCM policy exists but objectives, roles, or scope are unclear or incomplete.
Business Continuity Policy Affected: All systems and data	Critical	1	**REACH LEVEL 2** Awareness that BC planning is needed but no formal policy or program exists. **REACH LEVEL 3** Business continuity policy exists but no BIA has been conducted, critical functions are undefined, or the program has no executive sponsorship.
Disaster Recovery Policy Affected: All systems and data	Critical	1	**REACH LEVEL 2** Basic backup procedures exist but no formal DR policy defines RTOs, RPOs, or alternate processing site requirements. **REACH LEVEL 3** DR policy exists but RTOs and RPOs are defined but not validated through testing, or backup restoration has never been tested.
Endpoint Security Policy Affected: All endpoints	Critical	1	**REACH LEVEL 2** Antivirus is deployed on most endpoints but no formal policy governs configuration, monitoring, or hardening standards. **REACH LEVEL 3** Endpoint security policy exists but EDR is not deployed, tamper protection is not enabled, or coverage gaps exist.
MDM Enrollment and Coverage	Critical	1	**REACH LEVEL 2** MDM deployed for organization-owned smartphones and tablets; MDM enrollment tracked against issued

Finding	Severity	Current Maturity	What earns each maturity step
Affected: All mobile devices, including company-owned and personal devices used for work purposes.			devices; remote wipe capability confirmed. **REACH LEVEL 3** MDM covers all organization-owned mobile devices; enrollment tracked and gaps remediated; MDM agent health monitored.

P2 · STANDARDIZE & EXPAND · 6–18 MONTHS · 75 ITEMS

Phase 2 standardizes and expands District 101's security program through policy development, awareness training, and access control enhancements, ensuring consistency and broad coverage across the organization.

WS-01 · GOVERNANCE, RISK & POLICY · 12 ITEMS

Finding	Severity	Current Maturity	What earns each maturity step
AI Governance Structure Affected: All systems and data utilizing AI tools	Critical	1	**REACH LEVEL 2** AI tool approval requires IT and legal sign-off; a designated person or team owns AI policy; AI incidents have an escalation path. **REACH LEVEL 3** Cross-functional AI governance group established (IT, legal, privacy, business units); meets at least quarterly; AI risk included in enterprise risk management.
AI-Accelerated Attack Response Readiness Affected: All systems and data	Critical	1	**REACH LEVEL 2** IR team aware that AI enables faster attacks; detection SLAs calibrated to hours-not-days response requirements. **REACH LEVEL 3** Automated detection and containment playbooks reduce time from detection to response; mean time to contain (MTTC) tracked as a security metric; IR plan tested with compressed timelines.
Acceptable Use Policy (AUP)	High	2	**REACH LEVEL 3** AUP exists and is signed at onboarding but is not re-acknowledged annually, does not address social media, or does not define monitoring notification.
Audit & Assessment Policy	High	2	**REACH LEVEL 3** Audit policy exists but findings are not tracked to remediation, assessors are not required to be independent, or penetration testing is not included.
Change Management Policy	High	2	**REACH LEVEL 3** Change management policy exists but emergency changes are not consistently documented or security impact analysis is not required.
Cloud Storage and Sharing Controls Affected: All cloud-based storage systems	High	2	**REACH LEVEL 3** Sharing permissions reviewed quarterly; "anyone with the link" sharing disabled for sensitive document libraries; DLP prevents sensitive data from being shared externally.
Email Security in Cloud Affected: All cloud-based email systems	High	2	**REACH LEVEL 3** DMARC at reject; advanced anti-phishing policies configured (impersonation protection, spoof

Finding	Severity	Current Maturity	What earns each maturity step
			intelligence); DLP rules for sensitive data in email.
Information Security Program Charter Affected: All systems and data	High	2	**REACH LEVEL 3** Charter exists and designates a security lead but is not formally approved by senior leadership.
Leadership Engagement and Tone from the Top Affected: Executive communications and employee email	High	2	**REACH LEVEL 3** Executive leadership publicly communicates security as a priority; CISO presents security updates to board or cabinet.
Personnel Security & Background Check Policy	High	2	**REACH LEVEL 3** Personnel security policy exists but background check scope is minimal, contractors are not consistently screened, or rescreening is not conducted.
Print and Fax Security Affected: Sensitive information transmitted via print or fax	High	2	**REACH LEVEL 3** Secure print (pull printing) deployed — jobs held until user authenticates at the printer; printer hard drive encryption enabled; print logs maintained for sensitive printers.
Training Coverage and Completion Affected: Employee training records and HR systems	High	2	**REACH LEVEL 3** Training completion reported to HR and leadership; non-completers escalated; training accessible in multiple formats.

WS-02 · IDENTITY & ACCESS · 6 ITEMS

Finding	Severity	Current Maturity	What earns each maturity step
Access Control Policy Affected: All systems and data	High	2	**REACH LEVEL 3** Access control policy exists but least privilege and access reviews are not consistently enforced.
Application Access Controls Affected: All applications and systems with sensitive data	High	2	**REACH LEVEL 3** Access controls exist but are inconsistently applied, not least-privilege, or not reviewed.
Cloud Admin Account Security Affected: All cloud-based systems and applications	High	2	**REACH LEVEL 3** Phishing-resistant MFA (FIDO2, hardware token) for all global admin accounts; emergency "break glass" account documented and secured.
Guest and External User Access Affected: All cloud-based systems and applications	High	2	**REACH LEVEL 3** Guest accounts reviewed quarterly; inactive guests removed; guest access policies communicated to staff.
MFA Coverage and Enforcement Affected: All systems and applications with user accounts	High	2	**REACH LEVEL 3** MFA enforced for all users on all systems (not just cloud/remote); phishing-resistant MFA (FIDO2, passkeys) for high-risk roles; MFA coverage audited quarterly.
Remote Access Policy Affected: All systems and data	High	2	**REACH LEVEL 3** Remote access policy exists but split tunneling is permitted, monitoring is limited, or personal devices are used without controls.

WS-03 · DETECTION, LOGGING & IR · 9 ITEMS

Finding	Severity	Current Maturity	What earns each maturity step
AI-Enhanced Phishing and Social Engineering Affected: All systems and data accessible via email	Critical	1	**REACH LEVEL 2** Security awareness training updated to cover AI-enhanced phishing; staff taught that grammar mistakes are no longer a reliable indicator of phishing. **REACH LEVEL 3** Phishing simulation templates include AI-quality spear phishing scenarios; awareness covers voice deepfakes (vishing) and video deepfakes; callback verification procedures established for urgent financial requests.
Shadow AI Detection and Control Affected: All systems and data utilizing AI tools	Critical	1	**REACH LEVEL 2** Acceptable use policy communicates restrictions; IT aware of most-used unsanctioned tools; high-risk consumer AI sites (ChatGPT, Claude.ai, etc.) monitored or restricted on corporate networks. **REACH LEVEL 3** Web proxy or CASB provides visibility into AI tool usage; high-risk tools blocked on managed networks; shadow AI usage data reviewed monthly.
Cloud Security Posture Reporting Affected: All cloud-based systems and applications	High	2	**REACH LEVEL 3** Cloud security posture reported to CISO with trend analysis; top misconfigurations tracked to remediation.
Cloud Threat Detection and Alerting Affected: All cloud-based systems and applications	High	2	**REACH LEVEL 3** Alerts integrated into SIEM or MDR platform; alert triage SLA defined; threat detection coverage reviewed quarterly.
Data Breach Response & Notification Playbook Affected: All systems and data	High	2	**REACH LEVEL 3** Breach playbook exists but regulatory timelines are not mapped, notification templates are not pre-drafted, or legal counsel involvement is not defined.
Incident Response Plan Existence and Quality Affected: All systems and data	High	2	**REACH LEVEL 3** IRP covers specific scenarios (ransomware, data breach, BEC/wire fraud, account compromise); reviewed and updated after significant changes; accessible offline.

Finding	Severity	Current Maturity	What earns each maturity step
Incident Response Team Structure and Roles Affected: Incident Response Team	High	2	**REACH LEVEL 3** Role-specific responsibilities documented in IRP; team aware of their roles without looking them up; after-hours contact information current.
Phishing Simulation Program Affected: Phishing simulation software and employee email	High	2	**REACH LEVEL 3** Simulations conducted quarterly; results broken down by department; click rate tracked as a program metric.
Report Triage and Response Affected: Security incident reporting system and employee email	High	2	**REACH LEVEL 3** Triage SLA defined and met; confirmed phishing campaigns trigger email gateway rules; playbook for common report types.

WS-04 · ASSET & VULNERABILITY MGMT · 8 ITEMS

Finding	Severity	Current Maturity	What earns each maturity step
AI Use Case Inventory and Risk Assessment Affected: All systems and data utilizing AI tools	High	2	**REACH LEVEL 3** Risk assessment conducted for each AI use case: data sensitivity, model opacity, vendor data handling, accuracy risks; high-risk AI use cases reviewed by legal and privacy.
Application Risk Classification Affected: All web-based applications handling sensitive data	High	2	**REACH LEVEL 3** A classification framework exists but is inconsistently applied or not tied to control requirements.
Attack Surface Inventory Affected: All systems	High	2	**REACH LEVEL 3** External attack surface mapped and reviewed quarterly; unauthorized exposures identified and remediated.
Cloud and SaaS Vulnerability Coverage Affected: Cloud-based systems and SaaS applications	High	2	**REACH LEVEL 3** Cloud Security Posture Management (CSPM) or equivalent tool identifies cloud misconfigurations; container images scanned before deployment.
Cloud Configuration Baseline Affected: All district cloud resources, including AWS, Azure, and Google Cloud	High	2	**REACH LEVEL 3** Cloud Security Posture Management (CSPM) tool scans for configuration drift; high-risk findings alerted and remediated.
End-of-Life System Management Affected: Outdated systems	High	2	**REACH LEVEL 3** EOL systems network-isolated from sensitive systems; vendor-extended support purchased where available; replacement tracked quarterly.
SaaS Application Governance Affected: All district systems accessing SaaS applications	High	2	**REACH LEVEL 3** Shadow IT discovery tool or CASB provides visibility into unsanctioned cloud application use; unauthorized tools identified and actioned.
Software and Application Inventory Affected: All district systems, including endpoints, servers, and network devices	High	2	**REACH LEVEL 3** Software inventory auto-populated from endpoint management tool; covers all managed devices; reviewed quarterly.

WS-05 · DATA PRIVACY & K-12 COMPLIANCE · 15 ITEMS

Finding	Severity	Current Maturity	What earns each maturity step
Sensitive Data Leakage via AI Tools Affected: All systems and data containing sensitive information	Critical	1	**REACH LEVEL 2** Policy prohibits sensitive data entry into unauthorized AI tools; staff trained on the risk; major sensitive data categories defined in policy. **REACH LEVEL 3** DLP rules detect and alert when classified data is submitted to unsanctioned AI endpoints; approved enterprise AI tools configured to not use organizational data for model training.
Annual FERPA Notification Affected: Student data and systems	High	2	**REACH LEVEL 3** An annual notice is issued but is incomplete (missing directory-information opt-out, rights to inspect/amend, or complaint procedures) or distribution is not tracked.
Data Access Controls and DLP Affected: All systems and devices storing or processing sensitive data	High	2	**REACH LEVEL 3** Some controls exist but coverage is partial (e.g., email only), alert-only, or not classification-driven.
Data Classification Coverage Affected: All district systems storing or processing sensitive data	High	2	**REACH LEVEL 3** Classification enforced through labeling tools (e.g., Microsoft Purview, Google Workspace labels); DLP rules aligned to classification levels.
Data Classification Policy Affected: Systems containing sensitive data	High	2	**REACH LEVEL 3** Classification policy exists with defined tiers but labeling is not applied consistently and handling requirements are not enforced technically.
Data Loss Prevention (DLP) Policy	High	2	**REACH LEVEL 3** DLP policy exists and some controls are deployed but coverage is incomplete (e.g., covers email but not cloud or USB) or alert-only mode with no blocking.
Information Security & Privacy Policy Framework Affected: All systems and data	High	2	**REACH LEVEL 3** A policy framework exists but coverage is incomplete, ownership is unclear, or review cycles are not defined.
Legitimate Educational Interest & Access Controls	High	2	**REACH LEVEL 3** Legitimate-educational-interest criteria are documented, but role-based access to student records

Finding	Severity	Current Maturity	What earns each maturity step
Affected: Student data and systems			is incompletely implemented or not reviewed.
Opt-Out and Data Deletion Handling Affected: Systems storing personal data	High	2	**REACH LEVEL 3** Deletion propagated to third parties and sub-processors within reasonable timeframe; opt-out honored across all channels (email, SMS, targeted advertising); deletion confirmed and documented.
Parental Consent Mechanisms Affected: Student data and systems	High	2	**REACH LEVEL 3** A consent process exists but coverage is incomplete (e.g., not all EdTech tools), records are not centralized, or revocation is not handled.
Personal Data Mapping and Processing Records Affected: All systems handling personal data	High	2	**REACH LEVEL 3** ROPA or equivalent maintained covering all processing activities; legal basis documented for each activity (where required); third-party data sharing documented.
Regulatory Breach Notification Obligations Affected: Customer data, regulatory compliance	High	2	**REACH LEVEL 3** Decision tree for notification triggers documented in IRP; templates prepared for regulatory and individual notifications; legal counsel pre-briefed.
Security & Privacy Awareness Training Affected: Employee systems and data	High	2	**REACH LEVEL 3** Training exists but is not role-relevant, not annual, or completion is not tracked.
Security & Privacy Program Leadership Affected: Security team and stakeholders	High	2	**REACH LEVEL 3** A leadership role exists but authority, reporting line, or resourcing is unclear or part-time without mandate.
Security and Privacy Contract Requirements Affected: All systems and data handled by third-party vendors	High	2	**REACH LEVEL 3** Requirements are specific and measurable: encryption standards, access control requirements, audit rights, sub-processor disclosure, incident response cooperation; reviewed by legal before execution.

WS-06 · THIRD-PARTY / VENDOR RISK · 12 ITEMS

Finding	Severity	Current Maturity	What earns each maturity step
AI Model and Output Risk Affected: All systems utilizing AI models	Critical	1	**REACH LEVEL 2** Staff using AI tools trained on hallucination risk and the need for human review; high-stakes decisions require human verification of AI output. **REACH LEVEL 3** AI output accuracy risk assessed per use case; human-in-the-loop required for AI decisions affecting individuals; error monitoring in place for production AI systems.
Alternate Facility and Supply Chain Strategy Affected: Supply chain management systems, facility management databases	High	2	**REACH LEVEL 3** A strategy exists but alternate sites/suppliers are not identified or contracted.
Pre-Onboarding Security Assessment Affected: Systems and data managed by new vendors	High	2	**REACH LEVEL 3** A pre-onboarding assessment exists but is inconsistently applied or not risk-tiered.
Security and Privacy Contract Requirements Affected: Systems and data managed by third-party vendors with access to sensitive information	High	2	**REACH LEVEL 3** Standard terms exist but are not applied to all vendors or lack key clauses (breach, audit, data use).
Supply Chain Risk Program Governance Affected: All systems and data handled by third-party vendors	High	2	**REACH LEVEL 3** Vendor risk program includes inventory, assessment, contracting, monitoring, and offboarding procedures; cross-functional governance (IT, legal, procurement, business units).
Technology Asset & Software Inventory Affected: All systems and data	High	2	**REACH LEVEL 3** An inventory exists but is not automated, misses endpoints/servers/cloud, or is not reconciled.
TPRM Policy and Framework Affected: All systems and data managed by third-party vendors	High	2	**REACH LEVEL 3** A TPRM policy exists but tiering, assessment cadence, or offboarding are undefined.

Finding	Severity	Current Maturity	What earns each maturity step
Vendor Access Controls in Contracts Affected: Systems and data managed by third-party vendors with access to sensitive information	High	2	**REACH LEVEL 3** Contracts mention access but lack specific authentication, least-privilege, or accounting requirements.
Vendor Criticality and Concentration Risk Affected: Systems and data managed by critical vendors	High	2	**REACH LEVEL 3** A criticality method exists but concentration risk is not analyzed or mitigated.
Vendor Performance and SLA Management Affected: Systems and data managed by third-party vendors with service level agreements (SLAs)	High	2	**REACH LEVEL 3** Some monitoring exists but is inconsistent and not tied to remediation.
Vendor Risk Classification Affected: All systems and data handled by third-party vendors	High	2	**REACH LEVEL 3** Formal tiering criteria documented (data classification, access type, service criticality, subprocessor use); all vendors classified; classification drives assessment frequency and contractual requirements.
Vendor Risk Management Policy	High	2	**REACH LEVEL 3** Vendor risk management policy exists but risk tiering is not used, re-assessments are not conducted, or vendor offboarding (credential revocation, data return) is undefined.

Finding	Severity	Current Maturity	What earns each maturity step
Clean Desk and Screen Lock Policy Affected: Sensitive information and equipment within the facility	Critical	1	**REACH LEVEL 2** Clean desk policy documented; automatic screen lock configured at 15 minutes or less; policy communicated to all staff. **REACH LEVEL 3** Screen lock enforced at 10 minutes or less via Group Policy; random clean desk compliance checks conducted; policy included in security awareness training; locking storage provided for sensitive materials.
Mobile Application Management Affected: All mobile devices with access to company resources and data.	Critical	1	**REACH LEVEL 2** Corporate email configured through managed mail client; copy/paste between corporate and personal apps restricted. **REACH LEVEL 3** Mobile Application Management (MAM) deployed; corporate data restricted to approved managed apps; data cannot be transferred to unmanaged personal applications.
BYOD Policy and Scope Affected: All personal devices used for work purposes.	High	2	**REACH LEVEL 3** BYOD policy specifies permitted access types, required device configuration (screen lock, encryption, OS currency), and prohibited data types on personal devices.
Crisis Management and Communication Plans Affected: Crisis management systems, communication platforms	High	2	**REACH LEVEL 3** A plan exists but roles, escalation, or stakeholder communication templates are incomplete.
Critical Function Identification Affected: Business process management systems, stakeholder engagement platforms	High	2	**REACH LEVEL 3** A business impact analysis exists but is incomplete or stale.

Finding	Severity	Current Maturity	What earns each maturity step
Legal, Regulatory, and Contractual Continuity Requirements Affected: Contract management systems, regulatory compliance databases	High	2	**REACH LEVEL 3** Obligations are partially documented but not mapped to continuity plans.
MDM Policy Configuration and Enforcement Affected: All mobile devices enrolled in the MDM solution.	High	2	**REACH LEVEL 3** Comprehensive policy set: screen lock timeout, encryption, app allowlist/blocklist, jailbreak/root detection, OS version compliance; non-compliant devices quarantined from email and applications.
Network Security Policy	High	2	**REACH LEVEL 3** Network security policy exists but segmentation is incomplete, firewall rules are undocumented, or network monitoring is minimal.
Network Segmentation and Micro-Segmentation Affected: All network-connected systems and devices	High	2	**REACH LEVEL 3** Segmentation exists but is incomplete (e.g., guest/IoT/student/staff not separated) or rules are undocumented.
Operational Recovery Procedures Affected: Business process management systems, operational recovery databases	High	2	**REACH LEVEL 3** Procedures exist but are incomplete, untested, or not maintained.
Physical Security Policy	High	2	**REACH LEVEL 3** Physical security policy exists but access lists are not reviewed regularly, visitor logs are informal, or server rooms lack dedicated access controls.
Ransomware Recovery Testing Affected: All systems with sensitive data	High	2	**REACH LEVEL 3** Technical ransomware recovery drill conducted: production systems isolated, recovery from pre-infection backup attempted, restoration time recorded.
Recovery Strategy Selection and Validation Affected: Disaster recovery systems, cloud infrastructure	High	2	**REACH LEVEL 3** Strategies exist but are not validated through testing or aligned to recovery objectives.

P3 · OPTIMIZE · 18–36 MONTHS · 103 ITEMS

Phase 3 optimizes District 101's cybersecurity capabilities by implementing advanced controls, such as data minimization, vendor risk management, and incident response refinement, positioning the district for long-term success in managing cyber threats.

WS-01 · GOVERNANCE, RISK & POLICY · 13 ITEMS

Finding	Severity	Current Maturity	What earns each maturity step
AI Acceptable Use Policy Affected: All systems and data utilizing AI tools	Critical	1	**REACH LEVEL 2** AI acceptable use policy published; approved and prohibited tools listed; data entry restrictions defined (e.g., no sensitive data in public LLMs); communicated to all staff. **REACH LEVEL 3** Policy distinguishes between approved tools (enterprise-grade with data processing agreements) and consumer tools (public LLMs with no data protection); updated at least annually as the AI landscape evolves.
Program Metrics and KPIs Affected: Security awareness program metrics and analytics tools	High	2	**REACH LEVEL 3** Metrics trended over time; click rate, report rate, and repeat offender rate all tracked; reported to CISO quarterly.
AI Tool Security Awareness Affected: All systems and data utilizing AI tools	Medium	3	**REACH LEVEL 4** Quarterly AI risk awareness communications; AI-specific phishing and social engineering scenarios included in simulation program.
Cloud Application and OAuth Consent Controls Affected: All cloud-based applications	Medium	3	**REACH LEVEL 4** Automated detection of risky third-party app connections; CASB or app governance tool monitors OAuth grants.
Data Visibility and Classification Affected: All systems and devices storing or processing sensitive data	Medium	3	**REACH LEVEL 4** Data is classified and discovered using tools/processes, with handling rules per classification.
Information Security Policy (Master)	Medium	3	**REACH LEVEL 4** Policy approved by executive leadership, communicated to all staff, and reviewed within the past 2 years.
Records Management & Legal Hold Policy	Medium	3	**REACH LEVEL 4** Policy is approved, retention schedules are defined per record type, technical enforcement is in place, and legal hold procedures are documented.
Risk Management Policy	Medium	3	**REACH LEVEL 4**

Finding	Severity	Current Maturity	What earns each maturity step
			Policy defines risk tolerance, risk assessment frequency, treatment options, and risk acceptance authority; annual risk assessments are conducted.
Role-Based Security Training Affected: Employee training records and HR systems	**Medium**	**3**	**REACH LEVEL 4** Training effectiveness tracked per role; high-risk roles complete training more frequently (quarterly vs. annual).
Security Awareness & Training Policy Affected: All systems	**Medium**	**3**	**REACH LEVEL 4** Policy requires annual security awareness training for all employees with completion tracked, quarterly phishing simulations, role-based training for IT and security staff, and defined consequences for non-completion.
Security Champion and Developer Training Programs Affected: All development teams	**Medium**	**3**	**REACH LEVEL 4** Developers receive recurring secure-coding training and a security champion program is established.
Security Metrics & Reporting Policy Affected: All systems	**Medium**	**3**	**REACH LEVEL 4** Policy defines KRIs and KPIs covering patch compliance, phishing click rate, mean time to detect/respond, vulnerability age, and training completion; requires monthly reporting to IT leadership and quarterly reporting to executive leadership.
Security Requirements Definition Affected: All applications developed and maintained by District 101	**Medium**	**3**	**REACH LEVEL 4** Security requirements are defined at project initiation, integrated into the SDLC, and verified before release.

WS-02 · IDENTITY & ACCESS · 10 ITEMS

Finding	Severity	Current Maturity	What earns each maturity step
Identity Threat Detection Affected: All systems and applications with user accounts	High	2	**REACH LEVEL 3** Identity threat alerts integrated into SIEM; impossible travel, anomalous access pattern, and bulk data access alerts reviewed within defined SLA.
Service Account and Non-Human Identity Management Affected: All systems and applications with service accounts	High	2	**REACH LEVEL 3** Service account passwords stored in vault and rotated automatically; API keys have expiry dates and are scanned for in code repositories; service accounts monitored for anomalous behavior.
Cloud Account and Resource Inventory Affected: All district cloud resources, including AWS, Azure, and Google Cloud	Medium	3	**REACH LEVEL 4** Continuous cloud resource discovery; shadow cloud accounts detected; resource inventory integrated with billing and security tools.
Identity as the Control Plane Affected: All systems and applications with identity-based access controls	Medium	3	**REACH LEVEL 4** Identity governs access centrally with lifecycle management, role-based access, and conditional access policies.
Legacy Authentication and Protocol Blocking Affected: All systems and applications with legacy authentication protocols	Medium	3	**REACH LEVEL 4** NTLM authentication restricted on internal network; NTLMv1 disabled; legacy auth block verified through testing.
Non-Human Identity Governance Affected: All systems and applications with non-human identities	Medium	3	**REACH LEVEL 4** Non-human identities are inventoried, owned, least-privilege, and credentials are rotated and monitored.
Password & Authenticator Policy	Medium	3	**REACH LEVEL 4** Policy mandates MFA for privileged and remote access; passwords meet minimum length (12+ characters); breached password detection is in place.
Privileged Access Management Policy	Medium	3	**REACH LEVEL 4** Policy requires separate privileged accounts, prohibits shared admin credentials, mandates MFA, and requires privileged session logging.

Finding	Severity	Current Maturity	What earns each maturity step
Privileged Account Inventory and Separation Affected: All systems and applications with privileged accounts	Medium	3	**REACH LEVEL 4** Privileged account count minimized; unnecessary admin accounts removed; service account passwords in vault and rotated; admin account usage anomalies alerted.
Single Sign-On Coverage Affected: All critical systems and applications	Medium	3	**REACH LEVEL 4** All new applications required to support SSO before adoption; legacy standalone accounts managed through PAM; SSO coverage approaching 95%+.

WS-03 · DETECTION, LOGGING & IR · 11 ITEMS

Finding	Severity	Current Maturity	What earns each maturity step
Deepfake and Synthetic Media Risk Affected: All systems and data accessible via media	High	2	**REACH LEVEL 3** Code words or out-of-band verification established for executives and finance staff; deepfake scenarios included in tabletop exercises; fraud controls address synthetic identity risk.
Cloud Audit Logging Affected: All cloud-based systems and applications	Medium	3	**REACH LEVEL 4** 12-month log retention; log integrity protected (immutable storage); log coverage audited for completeness.
Data Breach Detection and Notification Readiness Affected: All systems handling personal data	Medium	3	**REACH LEVEL 4** Breach notification process tested; templates reviewed by legal; regulatory contact information current; breach notification decision flow tested within required timelines.
Distributed Denial of Service (DDoS) Response Playbook	Medium	3	**REACH LEVEL 4** Playbook defines detection thresholds, ISP and CDN/scrubbing provider contact procedures, internal escalation path, business communication template, and recovery validation steps.
External and Public Communications Affected: Customers, stakeholders	Medium	3	**REACH LEVEL 4** PR firm pre-engaged with crisis experience; social media monitoring during incidents; regulatory communications coordinated with external communications.
External Incident Response Support Affected: Incident Response Team, IT systems	Medium	3	**REACH LEVEL 4** IR retainer firm has conducted a pre-engagement scoping call and has baseline documentation of the environment; MDR provider integrated into IR workflow.
Internal and Executive Communications Affected: Executive team, employees	Medium	3	**REACH LEVEL 4** Communications reviewed and pre-approved in tabletop exercises; backup communications channels identified for when email is compromised.
Log Management & SIEM Policy Affected: All systems	Medium	3	**REACH LEVEL 4** Policy defines required log sources (endpoints, servers, network devices, applications, cloud), minimum retention period (1 year minimum, 90 days

Finding	Severity	Current Maturity	What earns each maturity step
			hot), mandates SIEM integration, and requires regular log review with alerting.
Ransomware Response Playbook	**Medium**	**3**	**REACH LEVEL 4** Playbook covers detection indicators, immediate isolation steps, offline communication method, backup restoration procedure, ransom decision authority, and law enforcement notification.
Suspicious Activity Reporting Mechanism Affected: Security incident reporting system and employee email	**Medium**	**3**	**REACH LEVEL 4** 24/7 reporting with after-hours response for urgent reports; anonymous reporting option available; metrics on reports received tracked.
Unauthorized Device Detection Affected: All district systems, including endpoints, servers, and network devices	**Medium**	**3**	**REACH LEVEL 4** Certificate-based network authentication prevents unauthorized device connections before they occur.

WS-04 · ASSET & VULNERABILITY MGMT · 7 ITEMS

Finding	Severity	Current Maturity	What earns each maturity step
Application Security Policy and Strategy Affected: All applications developed and maintained by District 101	Medium	3	**REACH LEVEL 4** The policy defines secure development, testing requirements, and app vetting, aligned to recognized practices.
Cloud Tenant Security Baseline Affected: All cloud-based systems and applications	Medium	3	**REACH LEVEL 4** Continuous configuration monitoring; policy-as-code enforces baseline; drift from baseline triggers automated alert.
Patch Deployment Process Affected: All systems with identified vulnerabilities	Medium	3	**REACH LEVEL 4** Patch compliance dashboard; failed patches automatically retried; application patches included alongside OS patches.
Penetration Testing Affected: All systems	Medium	3	**REACH LEVEL 4** Scope expanded to include cloud, social engineering, and physical; red team exercises conducted biannually; pen test findings drive policy and control improvements.
Risk Acceptance Process Affected: All systems with identified vulnerabilities	Medium	3	**REACH LEVEL 4** Risk acceptance register reviewed quarterly; expired acceptances escalated; compensating controls validated.
Vulnerability Management Policy Affected: All systems	Medium	3	**REACH LEVEL 4** Policy requires authenticated scanning of all assets at defined frequency (monthly for internet-facing, quarterly minimum for internal), risk-based prioritization, and tracked remediation with defined SLAs.
Vulnerability Scan Coverage Affected: Unscanned systems	Medium	3	**REACH LEVEL 4** Continuous or weekly scanning on internet-facing; monthly on all internal; scan coverage verified against asset inventory.

WS-05 · DATA PRIVACY & K-12 COMPLIANCE · 16 ITEMS

Finding	Severity	Current Maturity	What earns each maturity step
Data Minimization & Retention for Student Data Affected: Student data and systems	High	2	**REACH LEVEL 3** A retention schedule for student data exists but is not consistently applied or technically enforced, and minimization is not assessed at collection.
Student Data Transparency & Public Reporting Affected: Student data and systems	High	2	**REACH LEVEL 3** A data-sharing or vendor list is published but is incomplete, outdated, or not aligned to state transparency requirements.
Acceptable Use Policy — Students & Staff Affected: Employee systems and data	Medium	3	**REACH LEVEL 4** The AUP covers district and personal use, online conduct, monitoring notice, and consequences, and is acknowledged by students and staff.
Children's Data Protection Affected: Systems handling children's personal data	Medium	3	**REACH LEVEL 4** Data minimization enforced for children's data; children's privacy notice in age-appropriate language; staff trained on children's data obligations.
Cloud Data Encryption Affected: All cloud-based storage systems	Medium	3	**REACH LEVEL 4** Customer-managed encryption keys for highest-sensitivity data; key rotation automated; encryption coverage audited.
Data Subject Access Request Fulfillment Affected: Systems storing personal data	Medium	3	**REACH LEVEL 4** Data discovery tools support access request fulfillment; response time consistently within legal deadline; portability format (machine-readable) available where required.
EdTech App Inventory & COPPA Applicability Assessment Affected: Student data and systems	Medium	3	**REACH LEVEL 4** A maintained inventory captures each tool's data collection and COPPA applicability, and new tools are assessed before adoption.
Encryption & Cryptography Policy Affected: Systems containing sensitive data	Medium	3	**REACH LEVEL 4** Policy prohibits deprecated algorithms, defines minimum standards (AES-256, RSA-2048+, TLS 1.2+), mandates encryption of sensitive data at rest and in transit, and defines key management requirements.

Finding	Severity	Current Maturity	What earns each maturity step
FERPA Breach & Unauthorized Disclosure Procedures Affected: Student data and systems	Medium	3	**REACH LEVEL 4** The procedure defines containment, the FERPA disclosure record, parent/eligible-student notification, and remediation, with a named owner.
Incident Response & Breach Notification Affected: All systems and data	Medium	3	**REACH LEVEL 4** The procedure defines breach criteria, notification obligations and timelines, responsible roles, and communication templates, and is integrated with the overall IRP.
Internet Safety Policy Affected: Employee systems and data	Medium	3	**REACH LEVEL 4** The policy addresses content filtering, monitoring, education, and acceptable use across district and personal devices, and is reviewed periodically.
Privacy Regulatory Inventory Affected: All systems handling personal data	Medium	3	**REACH LEVEL 4** Regulatory obligations mapped to specific controls and data processing activities; compliance calendar maintained for reporting deadlines; legal counsel engaged for regulatory interpretation.
Sensitive Data Discovery and Location Affected: All district systems storing or processing sensitive data	Medium	3	**REACH LEVEL 4** Continuous or quarterly data discovery scanning; sensitive data outside approved locations triggers remediation.
Sensitive Data Handling and Minimization Affected: Systems storing sensitive personal data	Medium	3	**REACH LEVEL 4** Automated enforcement of data minimization through DLP; sensitive data processing requires documented justification; sensitive data inventory reviewed quarterly.
State Privacy Law Inventory & Applicability Assessment Affected: All systems and data	Medium	3	**REACH LEVEL 4** A maintained inventory maps each applicable state law to obligations, data flows, and owners.
Technology Protection Measures & Content Filtering Affected: All systems and data	Medium	3	**REACH LEVEL 4** Filtering covers district and 1:1 devices on and off network, categories and exceptions are managed, and CIPA requirements are met.

WS-06 · THIRD-PARTY / VENDOR RISK · 23 ITEMS

Finding	Severity	Current Maturity	What earns each maturity step
AI in Security Tools Affected: All systems utilizing AI in security tools	High	2	**REACH LEVEL 3** AI security tool performance reviewed quarterly; false positive and false negative rates tracked; AI recommendations reviewed by security staff before automated action.
AI Vendor and Tool Due Diligence Affected: All systems and data utilizing AI tools	High	2	**REACH LEVEL 3** AI tools subject to the standard vendor risk assessment process with AI-specific additions: model training data use, data retention, output accuracy risks, and model transparency.
Fourth-Party and Supply Chain Risk Affected: Systems and data managed by third-party vendors with access to sensitive information	High	2	**REACH LEVEL 3** Some fourth-party awareness exists but assessment is inconsistent and not contractual.
TPRM Metrics and Program Performance Affected: All systems and data managed by third-party vendors	High	2	**REACH LEVEL 3** Some metrics exist but are not consistently captured or reported.
TPRM Program Continuous Improvement Affected: All systems and data managed by third-party vendors	High	2	**REACH LEVEL 3** Reviews occur but are irregular and findings are not tracked.
Assessment Finding Management Affected: Systems and data managed by third-party vendors with identified security risks	Medium	3	**REACH LEVEL 4** Findings are tracked to remediation with owners, timelines, and verification.
Continuous Security Posture Monitoring Affected: Systems and data managed by third-party vendors with service level agreements (SLAs)	Medium	3	**REACH LEVEL 4** Vendor posture and SLA adherence are monitored on a cadence with defined response to changes.
Data Processing Agreements Affected: Systems and data managed by third-party vendors	Medium	3	**REACH LEVEL 4** A standard DPA with security, use-limitation, subprocessor, and breach terms is executed for applicable vendors.

Finding	Severity	Current Maturity	What earns each maturity step
with access to sensitive information			
Data Processing Agreements & Student Data Contracts Affected: Vendor systems and data	**Medium**	**3**	**REACH LEVEL 4** A standard DPA with required security, use-limitation, and breach terms is executed for all student-data vendors and tracked centrally.
EdTech Procurement & Review Process Affected: Vendor systems and data	**Medium**	**3**	**REACH LEVEL 4** New EdTech is reviewed for security and privacy (including COPPA/DPA) before adoption through a defined gate.
Incident Notification and Cooperation Requirements Affected: Systems and data managed by third-party vendors with access to sensitive information	**Medium**	**3**	**REACH LEVEL 4** Contracts define breach-notification timelines, scope, and cooperation/forensics obligations for applicable vendors.
Periodic Vendor Re-Assessment Affected: All systems and data handled by third-party vendors	**Medium**	**3**	**REACH LEVEL 4** Third-party security ratings provide continuous posture signals between formal re-assessments; rating drops trigger accelerated review.
Third-Party Access Policy Affected: All systems and data	**Medium**	**3**	**REACH LEVEL 4** Policy requires separate accounts for all third parties, mandates MFA, limits access to defined systems and time windows, requires session monitoring for privileged access, and defines deprovisioning within 24 hours of engagement end.
Third-Party Disclosure Controls & School Official Agreements Affected: Student data and systems	**Medium**	**3**	**REACH LEVEL 4** School-official agreements and disclosure controls govern third-party access to student data, with records maintained.
TPRM Program Governance and Reporting Affected: All systems and data managed by third-party vendors	**Medium**	**3**	**REACH LEVEL 4** Defined governance and regular reporting track KPIs and provide stakeholder updates.

Finding	Severity	Current Maturity	What earns each maturity step
Vendor & Third-Party Risk Management Affected: Vendor systems and data	Medium	3	**REACH LEVEL 4** Vendors are vetted and risk-managed by tier with assessments, contractual terms, and monitoring.
Vendor Contact and Relationship Management Affected: Systems and data managed by third-party vendors with access to sensitive information	Medium	3	**REACH LEVEL 4** Vendor contacts, owners, and relationships are centrally tracked and current.
Vendor Incident and Breach Notification Tracking Affected: All systems and data handled by third-party vendors	Medium	3	**REACH LEVEL 4** Vendor incident response integrated with organizational IR plan; tabletop exercises include vendor breach scenario; sub-processor incidents tracked.
Vendor Inventory Completeness and Currency Affected: Systems and data managed by third-party vendors	Medium	3	**REACH LEVEL 4** A maintained inventory captures all vendors with risk tiers and key attributes, reconciled periodically.
Vendor Offboarding and Access Termination Affected: All systems accessed by vendors	Medium	3	**REACH LEVEL 4** Offboarding automated where possible; deletion certificate required for high-risk vendors; sub-processor offboarding verified; 24-hour access revocation for terminated high-risk vendors.
Vendor Offboarding and Access Termination Affected: Systems and data managed by third-party vendors with access to sensitive information	Medium	3	**REACH LEVEL 4** Offboarding revokes access, recovers/destroys data, and deprovisions credentials on a defined timeline.
Vendor Onboarding Process Affected: Systems and data managed by third-party vendors with access to sensitive information	Medium	3	**REACH LEVEL 4** Onboarding includes risk assessment, contractual terms, least-privilege access provisioning, and documentation.
Vendor Security Assessment Methodology Affected: Systems and data managed by new vendors	Medium	3	**REACH LEVEL 4** A defined methodology assesses vendors by risk tier using questionnaires and evidence.

Finding	Severity	Current Maturity	What earns each maturity step
BCM Programme Review and Continuous Improvement Affected: BCM programme management systems, continuous improvement databases	High	2	**REACH LEVEL 3** Reviews occur but are irregular and findings are not tracked to closure.
Backup Frequency and Retention Affected: All systems with sensitive data	Medium	3	**REACH LEVEL 4** Hourly or continuous backup for highest-criticality systems; 1-year retention for ransomware resilience; retention verified through recovery testing.
Backup Monitoring and Alerting Affected: All systems with sensitive data	Medium	3	**REACH LEVEL 4** Backup health integrated into overall monitoring dashboard; 24/7 backup monitoring; repeated failures escalated to management.
BCM Awareness and Training Affected: Training management systems, employee engagement platforms	Medium	3	**REACH LEVEL 4** Role-based continuity training is delivered on a schedule and tracked.
BCM Integration with Organizational Risk Management Affected: Risk management systems, BCM programme databases	Medium	3	**REACH LEVEL 4** Continuity risks are identified, assessed, and treated within the risk-management process.
Business Continuity During Recovery Affected: All systems with sensitive data	Medium	3	**REACH LEVEL 4** BCP tested alongside DR testing; recovery priority validated with business owners; maximum tolerable downtime defined per function.
Business Continuity Plans Affected: Business process management systems, continuity planning databases	Medium	3	**REACH LEVEL 4** Documented BC plans cover critical functions with roles, procedures, and recovery steps.

Finding	Severity	Current Maturity	What earns each maturity step
BYOD Security Controls Affected: All personal devices used for work purposes.	Medium	3	**REACH LEVEL 4** Conditional access verifies device health (non-jailbroken, OS currency, screen lock) before granting access; access denied for non-compliant personal devices.
Cabling and Network Port Security Affected: Sensitive networks and systems within the facility	Medium	3	**REACH LEVEL 4** All network closets on access control with logging; rogue device detection on wired network; cable management documented.
CCTV and Physical Surveillance Affected: All systems and data within the facility	Medium	3	**REACH LEVEL 4** No critical blind spots at access control points; license plate recognition for vehicle access; real-time monitoring during after-hours periods; integrated with access control for event correlation.
Clean Desk & Screen Lock Policy Affected: All systems	Medium	3	**REACH LEVEL 4** Policy mandates automatic screen lock after defined inactivity period (maximum 10 minutes), requires secure storage of sensitive documents when unattended, and prohibits visible display of passwords.
Dependency Mapping and Single Points of Failure Affected: Business process management systems, stakeholder engagement platforms	Medium	3	**REACH LEVEL 4** Dependencies and SPOFs are mapped for critical functions and mitigation is planned.
Encrypted Traffic and Protocol Controls Affected: All network-connected systems and devices	Medium	3	**REACH LEVEL 4** Encryption (TLS/IPsec/SSH) is required for sensitive traffic, legacy protocols are restricted, and configuration is standardized.
Executive Leadership and BCM Governance Affected: Executive leadership systems, governance databases	Medium	3	**REACH LEVEL 4** Leadership actively sponsors BCM and it is integrated into governance and decisions.
Exercise Programme Affected: Exercise management systems, crisis management databases	Medium	3	**REACH LEVEL 4** A defined exercise program tests plans on a schedule with documented results.

Finding	Severity	Current Maturity	What earns each maturity step
Financial Impact and Cost of Downtime Affected: Financial management systems, business process databases	Medium	3	**REACH LEVEL 4** Downtime impact is analyzed per critical function and informs recovery priorities and investment.
Immutable and Air-Gapped Backups Affected: All systems with sensitive data	Medium	3	**REACH LEVEL 4** Air-gapped backup (physically disconnected, not accessible from network) in addition to immutable cloud copy; immutability tested.
Physical Device Security and Tamper Prevention Affected: Sensitive equipment within the facility	Medium	3	**REACH LEVEL 4** Full-disk encryption on all portable devices; remote wipe capability for laptops and mobile devices; hardware tamper detection on critical servers.
Removable Media & USB Policy Affected: Systems containing sensitive data	Medium	3	**REACH LEVEL 4** Policy restricts USB to authorized devices only, requires encryption on all removable media containing sensitive data, and technical controls (endpoint DLP, USB blocking) enforce the policy.
Server Room and Data Center Physical Security Affected: Server room and data center equipment and data	Medium	3	**REACH LEVEL 4** Server room access limited to named IT personnel only; access reviewed quarterly; cage or rack-level locking for highest-sensitivity equipment; out-of-band management available.
Visitor Management Process Affected: All systems and data within the facility	Medium	3	**REACH LEVEL 4** Visitor access controlled at area level — visitors badged for specific zones only; access log retained 90+ days; background checks for contractors with recurring unescorted access.
Wireless Network Security Policy Affected: Wireless networks	Medium	3	**REACH LEVEL 4** Policy requires WPA3 or WPA2-Enterprise with 802.1X, separates corporate, guest, and IoT networks, mandates rogue AP detection, and prohibits personal hotspots on corporate networks.
Workforce Continuity and Alternate Work Arrangements Affected: Human resources systems, workforce management databases	Medium	3	**REACH LEVEL 4** Workforce continuity plans define alternate work arrangements, role coverage, and support.

NOTES

Phase timeframes (0–6 / 6–18 / 18–36 months) are planning estimates and assume timely Client cooperation and resource allocation. Phasing and target maturity are set by each control's foundational tier and current maturity, not by severity alone. Target maturity levels and effort are advisory guidance, not fixed quotes. This roadmap is advisory; the Client is responsible for implementation, prioritization, and outcomes. New or changed work should be confirmed in writing.