Cybersecurity Posture Report

Combined — 18 Assessments

Technical Detail Report

CLIENT

District 101

Assessments Combined: 18

Total Findings: 203

Generated: 2026-06-30

COMBINED POSTURE SCORE

2.76 / 5.0

MEDIUM

TABLE OF CONTENTS

ASSESSMENTS SUMMARY

ASSESSMENT	SCORE	RISK	FINDINGS
AI & Emerging Technology Risk Discovery	1.50	CRITICAL	12
Mobile & Endpoint Security Discovery	2.17	HIGH	5
Physical Security Discovery	2.27	HIGH	10
Cloud Security Posture Discovery	2.42	HIGH	11
Incident Response Readiness Discovery	2.50	HIGH	9
IT Policy Library Review	2.58	MEDIUM	38
Education Policy & Compliance Review	2.58	MEDIUM	22
Business Continuity Management	2.75	MEDIUM	16
Secure SDLC and Application Security	2.75	MEDIUM	4
Third-Party Risk Management Program	2.83	MEDIUM	19
Vendor & Third-Party Risk Discovery	2.83	MEDIUM	8
Security Awareness & Phishing Discovery	3.00	MEDIUM	8
Vulnerability Management Discovery	3.08	MEDIUM	8
Identity & Access Management Discovery	3.17	MEDIUM	7
Zero Trust Maturity Assessment	3.25	MEDIUM	7
Asset & Data Inventory Discovery	3.25	MEDIUM	7
Data Privacy Baseline Discovery	3.33	MEDIUM	7
Backup & Disaster Recovery Discovery	3.67	LOW	5

AGGREGATE RISK POSTURE

34	79	90	0
CRITICAL	HIGH	MEDIUM	LOW

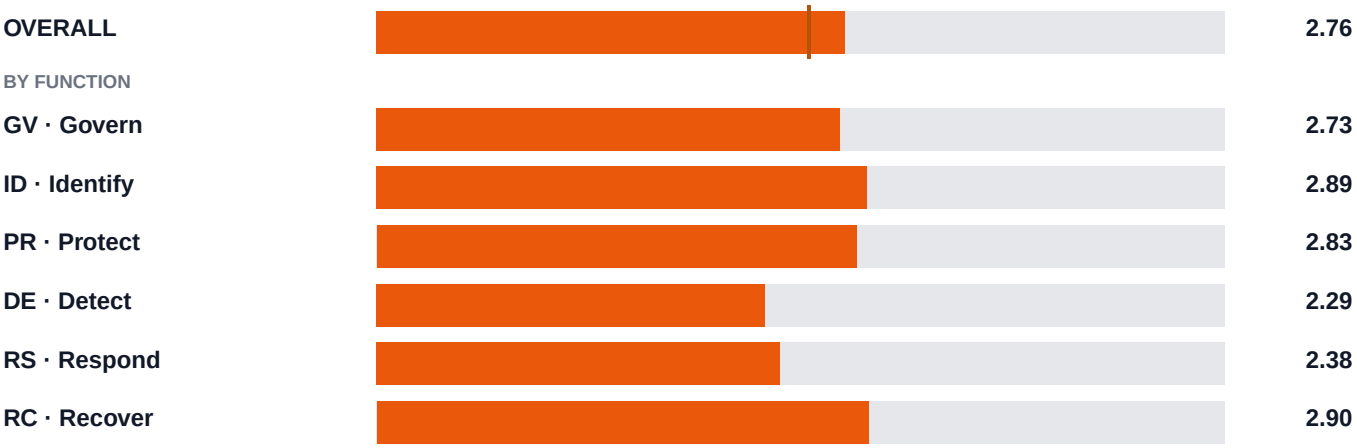
NIST CSF POSTURE

K12 SIX ESSENTIALS
2.80 / 5.0
Crosswalked from Discovery · no national benchmark

NIST CSF (OVERALL)
2.76 / 5.0
National K-12 average: 2.54 (NCSR)

K12 SIX — BY DOMAIN

Per-domain benchmark appears once 3+ districts are assessed on K12 SIX (currently 0).



Amber line = national K-12 average (CIS/MS-ISAC Nationwide Cybersecurity Review (NCSR) — national K-12 average). Benchmark is overall only; function bars show your distribution without a national line.

ASSESSMENT BREAKDOWN

AI & Emerging Technology Risk Discovery

AI & Emerging Technology Risk Discovery v1.0 — District 101 2026 · 1.50/5 · CRITICAL · 12 findings

AI-GOV — AI Governance & Policy 1.3 / 5

AI-LEAK — Shadow AI & Data Leakage 1.7 / 5

AI-VEN — AI Vendor Risk 1.7 / 5

AI-TACT — AI-Enabled Threats 1.3 / 5

AI-GOV — AI Governance & Policy

AI-1.1 AI Acceptable Use Policy	1 / 5
AI-1.2 AI Use Case Inventory and Risk Assessment	2 / 5
AI-1.3 AI Governance Structure	1 / 5

AI-LEAK — Shadow AI & Data Leakage

AI-2.1 Shadow AI Detection and Control	1 / 5
AI-2.2 Sensitive Data Leakage via AI Tools	1 / 5
AI-2.3 AI Tool Security Awareness	3 / 5

AI-VEN — AI Vendor Risk

AI-3.1 AI Vendor and Tool Due Diligence	2 / 5
AI-3.2 AI Model and Output Risk	1 / 5
AI-3.3 AI in Security Tools	2 / 5

AI-TACT — AI-Enabled Threats

AI-4.1 AI-Enhanced Phishing and Social Engineering	1 / 5
AI-4.2 Deepfake and Synthetic Media Risk	2 / 5

AI-4.3 AI-Accelerated Attack Response Readiness	1 / 5

Mobile & Endpoint Security Discovery

Mobile & Endpoint Security Discovery v1.0 — District 101 2026 · 2.17/5 · HIGH · 5 findings

ME-MDM — Mobile Device Management

1.3 / 5

ME-BYOD — BYOD Policy & Controls

3.0 / 5

ME-EP — Endpoint Protection

0.0 / 5

ME-MDM — Mobile Device Management

ME-1.1 MDM Enrollment and Coverage	1 / 5
ME-1.2 MDM Policy Configuration and Enforcement	2 / 5
ME-1.3 Mobile Application Management	1 / 5

ME-BYOD — BYOD Policy & Controls

ME-2.1 BYOD Policy and Scope	2 / 5
ME-2.2 BYOD Security Controls	3 / 5
ME-2.3 BYOD Data Separation and Wipe Capability	4 / 5

ME-EP — Endpoint Protection

ME-3.1 Endpoint Protection Coverage	0 / 5
ME-3.2 Endpoint Configuration and Hardening	0 / 5
ME-3.3 Endpoint Patching and Software Currency	0 / 5

Physical Security Discovery

Physical Security Discovery v1.0 — District 101 2026 · 2.27/5 · HIGH · 10 findings

PS-FAC — Facility Access Control

1.0 / 5

PS-SRV — Server Room & Equipment

3.0 / 5

PS-MED — Media & Document Security

1.5 / 5

PS-VIS — Visitor & Social Engineering

3.3 / 5

PS-FAC — Facility Access Control

PS-1.1 Electronic Access Control System	1 / 5
PS-1.2 Key and Badge Management	1 / 5
PS-1.3 Physical Security Perimeter	1 / 5

PS-SRV — Server Room & Equipment

PS-2.1 Server Room and Data Center Physical Security	3 / 5
PS-2.2 Physical Device Security and Tamper Prevention	3 / 5
PS-2.3 Cabling and Network Port Security	3 / 5

PS-MED — Media & Document Security

PS-3.1 Media Sanitization and Disposal	0 / 5
PS-3.2 Clean Desk and Screen Lock Policy	1 / 5
PS-3.3 Print and Fax Security	2 / 5

PS-VIS — Visitor & Social Engineering

PS-4.1 Visitor Management Process	3 / 5
PS-4.2 Social Engineering and Tailgating Prevention	4 / 5
PS-4.3 CCTV and Physical Surveillance	3 / 5

Cloud Security Posture Discovery

Cloud Security Posture Discovery v1.0 — District 101 2026 · 2.42/5 · HIGH · 11 findings

CSP-IAM — Identity & Access in Cloud

1.7 / 5

CSP-CFG — Configuration & Hardening

2.7 / 5

CSP-DATA — Data Protection in Cloud

3.0 / 5

CSP-LOG — Monitoring & Logging

2.3 / 5

CSP-IAM — Identity & Access in Cloud

CSP-1.1 Cloud Admin Account Security	2 / 5
CSP-1.2 Cloud User MFA and Conditional Access	1 / 5
CSP-1.3 Guest and External User Access	2 / 5

CSP-CFG — Configuration & Hardening

CSP-2.1 Cloud Tenant Security Baseline	3 / 5
CSP-2.2 Cloud Storage and Sharing Controls	2 / 5
CSP-2.3 Cloud Application and OAuth Consent Controls	3 / 5

CSP-DATA — Data Protection in Cloud

CSP-3.1 Cloud Data Encryption	3 / 5
CSP-3.2 Email Security in Cloud	2 / 5
CSP-3.3 Cloud DLP and Information Protection	4 / 5

CSP-LOG — Monitoring & Logging

CSP-4.1 Cloud Audit Logging	3 / 5

CSP-4.2 Cloud Threat Detection and Alerting	2 / 5
CSP-4.3 Cloud Security Posture Reporting	2 / 5

Incident Response Readiness Discovery

Incident Response Readiness Discovery v1.0 — District 101 2026 · 2.50/5 · HIGH · 9 findings

IR-PLAN — IR Plan & Policy

2.3 / 5

IR-TEAM — Team & Contacts

3.0 / 5

IR-TEST — Testing & Exercises

2.0 / 5

IR-NOTIF — Notification & Communication

2.7 / 5

IR-PLAN — IR Plan & Policy

IR-1.1 Incident Response Plan Existence and Quality	2 / 5
IR-1.2 Incident Classification and Declaration	1 / 5
IR-1.3 Legal Hold and Evidence Preservation	4 / 5

IR-TEAM — Team & Contacts

IR-2.1 Incident Response Team Structure and Roles	2 / 5
IR-2.2 24/7 Contact List and Communication Plan	4 / 5
IR-2.3 External Incident Response Support	3 / 5

IR-TEST — Testing & Exercises

IR-3.1 Tabletop Exercise Program	1 / 5
IR-3.2 Post-Incident Review Process	1 / 5
IR-3.3 Recovery Capability Testing	4 / 5

IR-NOTIF — Notification & Communication

IR-4.1 Regulatory Breach Notification Obligations	2 / 5
IR-4.2 Internal and Executive Communications	3 / 5
IR-4.3 External and Public Communications	3 / 5

IT Policy Library Review

IT Policy Library Review v1.0 — District 101 2026 · 2.58/5 · MEDIUM · 38 findings

GOV — Governance & Program Policies

3.0 / 5

ACC — Access Control & Identity Policies

2.8 / 5

INC — Incident Response & Playbooks

2.6 / 5

DAT — Data Management & Classification Policies

2.4 / 5

NET — Network & Infrastructure Security Policies

2.8 / 5

END — Endpoint & Device Security Policies

2.8 / 5

VND — Vendor & Third-Party Risk Policies

3.0 / 5

PHY — Physical & Environmental Security Policies

3.7 / 5

HRU — Human Resources & Acceptable Use Policies

2.0 / 5

BC — Business Continuity & Disaster Recovery Policies

1.0 / 5

COM — Compliance & Audit Policies

2.3 / 5

GOV — Governance & Program Policies

GOV-1 Information Security Policy (Master)	3 / 5
GOV-2 Information Security Program Charter	2 / 5
GOV-3 Risk Management Policy	3 / 5
GOV-4 Policy Management & Exception Policy	4 / 5
GOV-5 Records Management & Legal Hold Policy	3 / 5

ACC — Access Control & Identity Policies

ACC-1 Access Control Policy	2 / 5
ACC-2 Password & Authenticator Policy	3 / 5
ACC-3 Identity Lifecycle & Account Management Policy	4 / 5
ACC-4 Privileged Access Management Policy	3 / 5
ACC-5 Remote Access Policy	2 / 5

INC — Incident Response & Playbooks

INC-1 Incident Response Plan (IRP)	1 / 5
INC-2 Ransomware Response Playbook	3 / 5
INC-3 Data Breach Response & Notification Playbook	2 / 5
INC-4 Business Email Compromise (BEC) / Phishing Response Playbook	4 / 5
INC-5 Insider Threat Response Playbook	1 / 5
INC-6 Third-Party / Supply Chain Breach Playbook	4 / 5
INC-7 Distributed Denial of Service (DDoS) Response Playbook	3 / 5

DAT — Data Management & Classification Policies

DAT-1 Data Classification Policy	2 / 5
DAT-2 Data Retention & Disposal Policy	4 / 5
DAT-3 Privacy Policy & PII Handling Policy	1 / 5
DAT-4 Encryption & Cryptography Policy	3 / 5
DAT-5 Data Loss Prevention (DLP) Policy	2 / 5

NET — Network & Infrastructure Security Policies

NET-1 Network Security Policy	2 / 5
NET-2 Patch Management Policy	4 / 5
NET-3 Vulnerability Management Policy	3 / 5
NET-4 Change Management Policy	2 / 5
NET-5 Wireless Network Security Policy	3 / 5

END — Endpoint & Device Security Policies

END-1 Endpoint Security Policy	1 / 5
END-2 Mobile Device Management (MDM) & BYOD Policy	4 / 5
END-3 Removable Media & USB Policy	3 / 5
END-4 Clean Desk & Screen Lock Policy	3 / 5

VND — Vendor & Third-Party Risk Policies

VND-1 Vendor Risk Management Policy	2 / 5
VND-2 Vendor Contract Security Requirements Policy	4 / 5
VND-3 Third-Party Access Policy	3 / 5

PHY — Physical & Environmental Security Policies

PHY-1 Physical Security Policy	2 / 5
PHY-2 Asset Management Policy	5 / 5
PHY-3 Business Travel & Security Policy	4 / 5

HRU — Human Resources & Acceptable Use Policies

HRU-1 Acceptable Use Policy (AUP)	2 / 5
HRU-2 Security Awareness & Training Policy	3 / 5
HRU-3 Personnel Security & Background Check Policy	2 / 5
HRU-4 Termination & Offboarding Security Policy	1 / 5

BC — Business Continuity & Disaster Recovery Policies

BC-1 Business Continuity Policy	1 / 5
BC-2 Disaster Recovery Policy	1 / 5
BC-3 Backup & Restore Policy	1 / 5

COM — Compliance & Audit Policies

COM-1 Regulatory Compliance Policy	1 / 5
COM-2 Audit & Assessment Policy	2 / 5
COM-3 Log Management & SIEM Policy	3 / 5
COM-4 Security Metrics & Reporting Policy	3 / 5

Education Policy & Compliance Review

Education Policy & Compliance Review v1.0 — District 101 2026 · 2.58/5 · MEDIUM · 22 findings

GOV — Governance & Policy Program
2.2 / 5

FERPA — FERPA — Student Records Privacy
2.8 / 5

COPPA — COPPA — Children's Online Privacy (K-12)
2.3 / 5

CIPA — CIPA & Acceptable Use (K-12)
3.0 / 5

EDTECH — EdTech & Third-Party App Governance
3.3 / 5

STATE — State Student Privacy Laws
2.0 / 5

GOV — Governance & Policy Program

GOV.PP Information Security & Privacy Policy Framework	2 / 5
GOV.PROG Security & Privacy Program Leadership	2 / 5
GOV.RISK Risk Assessment Program	1 / 5
GOV.TRAIN Security & Privacy Awareness Training	2 / 5
GOV.IR Incident Response & Breach Notification	3 / 5
GOV.VENDOR Vendor & Third-Party Risk Management	3 / 5

FERPA — FERPA — Student Records Privacy

FERPA.ANN Annual FERPA Notification	2 / 5
FERPA.DIR Directory Information Policy	4 / 5
FERPA.ACCESS Legitimate Educational Interest & Access Controls	2 / 5
FERPA.3RD Third-Party Disclosure Controls & School Official Agreements	3 / 5
FERPA.BREACH FERPA Breach & Unauthorized Disclosure Procedures	3 / 5

COPPA — COPPA — Children's Online Privacy (K-12)

COPPA.INV EdTech App Inventory & COPPA Applicability Assessment	3 / 5
COPPA.CONSENT Parental Consent Mechanisms	2 / 5
COPPA.DATA Data Minimization & Retention for Student Data	2 / 5

CIPA — CIPA & Acceptable Use (K-12)

CIPA.ISP Internet Safety Policy	3 / 5
CIPA.FILTER Technology Protection Measures & Content Filtering	3 / 5
CIPA.AUP Acceptable Use Policy — Students & Staff	3 / 5

EDTECH — EdTech & Third-Party App Governance

EDT.PROC EdTech Procurement & Review Process	3 / 5
EDT.DPA Data Processing Agreements & Student Data Contracts	3 / 5
EDT.INVENT Technology Asset & Software Inventory	2 / 5
EDT.OFFBOARD Vendor Offboarding & Data Return/Deletion	5 / 5

STATE — State Student Privacy Laws

STATE.INV State Privacy Law Inventory & Applicability Assessment	3 / 5
STATE.BREACH State Breach Notification Compliance	1 / 5
STATE.TRANS Student Data Transparency & Public Reporting	2 / 5

Business Continuity Management

Business Continuity Management v1.0 — District 101 2026 · 2.75/5 · MEDIUM · 16 findings

BCM-GOV — BCM Governance & Policy 2.3 / 5

BCM-BIA — Business Impact Analysis 3.0 / 5

BCM-STR — Recovery Strategy 2.8 / 5

BCM-PLN — Plans and Procedures 2.8 / 5

BCM-EX — Exercises and Improvement 3.0 / 5

BCM-GOV — BCM Governance & Policy

BCM-G1 BCM Policy and Scope	1 / 5
BCM-G2 Executive Leadership and BCM Governance	3 / 5
BCM-G3 Legal, Regulatory, and Contractual Continuity Requirements	2 / 5
BCM-G4 BCM Integration with Organizational Risk Management	3 / 5

BCM-BIA — Business Impact Analysis

BCM-B1 Critical Function Identification	2 / 5
BCM-B2 Dependency Mapping and Single Points of Failure	3 / 5
BCM-B3 Recovery Time and Recovery Point Objectives	4 / 5
BCM-B4 Financial Impact and Cost of Downtime	3 / 5

BCM-STR — Recovery Strategy

BCM-S1 Recovery Strategy Selection and Validation	2 / 5
BCM-S2 IT Disaster Recovery Architecture	4 / 5
BCM-S3 Workforce Continuity and Alternate Work Arrangements	3 / 5
BCM-S4 Alternate Facility and Supply Chain Strategy	2 / 5

BCM-PLN — Plans and Procedures

BCM-P1 Business Continuity Plans	3 / 5
BCM-P2 IT Disaster Recovery Plans	4 / 5
BCM-P3 Crisis Management and Communication Plans	2 / 5
BCM-P4 Operational Recovery Procedures	2 / 5

BCM-EX — Exercises and Improvement

BCM-E1 Exercise Programme	3 / 5
BCM-E2 Exercise Evaluation and Findings Management	4 / 5
BCM-E3 BCM Awareness and Training	3 / 5
BCM-E4 BCM Programme Review and Continuous Improvement	2 / 5

Secure SDLC and Application Security

Secure SDLC and Application Security v1.0 — District 101 2026 · 2.75/5 · MEDIUM · 4 findings

SDLC-GOV — Governance & Security Requirements

2.8 / 5

SDLC-GOV — Governance & Security Requirements

SDLC-G1 Application Security Policy and Strategy	3 / 5
SDLC-G2 Security Requirements Definition	3 / 5
SDLC-G3 Application Risk Classification	2 / 5
SDLC-G4 Security Champion and Developer Training Programs	3 / 5

Third-Party Risk Management Program

Third-Party Risk Management Program v1.0 — District 101 2026 · 2.83/5 · MEDIUM · 19 findings

TPRM-GOV — Program Governance

2.8 / 5

TPRM-INV — Vendor Inventory

3.0 / 5

TPRM-DD — Due Diligence

3.0 / 5

TPRM-CONT — Contract Management

2.5 / 5

TPRM-MON — Ongoing Monitoring

2.8 / 5

TPRM-LCL — Vendor Lifecycle

3.0 / 5

TPRM-GOV — Program Governance

TPRM-G1 TPRM Policy and Framework	2 / 5
TPRM-G2 TPRM Program Governance and Reporting	3 / 5
TPRM-G3 Fourth-Party and Supply Chain Risk	2 / 5
TPRM-G4 TPRM Integration with Procurement	4 / 5

TPRM-INV — Vendor Inventory

TPRM-I1 Vendor Inventory Completeness and Currency	3 / 5
TPRM-I2 Vendor Risk Tiering and Classification	4 / 5
TPRM-I3 Vendor Criticality and Concentration Risk	2 / 5
TPRM-I4 Vendor Contact and Relationship Management	3 / 5

TPRM-DD — Due Diligence

TPRM-D1 Pre-Onboarding Security Assessment	2 / 5
TPRM-D2 Vendor Security Assessment Methodology	3 / 5
TPRM-D3 Periodic Re-Assessment	4 / 5
TPRM-D4 Assessment Finding Management	3 / 5

TPRM-CONT — Contract Management

TPRM-C1 Security and Privacy Contract Requirements	2 / 5
TPRM-C2 Data Processing Agreements	3 / 5
TPRM-C3 Vendor Access Controls in Contracts	2 / 5
TPRM-C4 Incident Notification and Cooperation Requirements	3 / 5

TPRM-MON — Ongoing Monitoring

TPRM-M1 Continuous Security Posture Monitoring	3 / 5
TPRM-M2 Vendor Incident and Breach Tracking	4 / 5
TPRM-M3 Vendor Performance and SLA Management	2 / 5
TPRM-M4 TPRM Metrics and Program Performance	2 / 5

TPRM-LCL — Vendor Lifecycle

TPRM-L1 Vendor Onboarding Process	3 / 5
TPRM-L2 Vendor Offboarding and Access Termination	3 / 5
TPRM-L3 Vendor Relationship Change Management	4 / 5
TPRM-L4 TPRM Program Continuous Improvement	2 / 5

Vendor & Third-Party Risk Discovery

Vendor & Third-Party Risk Discovery v1.0 — District 101 2026 · 2.83/5 · MEDIUM · 8 findings

VR-INV — Vendor Inventory

VR-ASMT — Vendor Assessment

VR-CONT — Contract Controls

VR-MON — Monitoring & Offboarding

VR-INV — Vendor Inventory

VR-1.1 Vendor Inventory Completeness	4 / 5
VR-1.2 Vendor Risk Classification	2 / 5
VR-1.3 Critical Vendor Single-Point-of-Failure Analysis	4 / 5

VR-ASMT — Vendor Assessment

VR-2.1 Pre-Onboarding Security Assessment	4 / 5
VR-2.2 Periodic Vendor Re-Assessment	3 / 5
VR-2.3 Vendor Incident and Breach Notification Tracking	3 / 5

VR-CONT — Contract Controls

VR-3.1 Security and Privacy Contract Requirements	2 / 5
VR-3.2 Data Processing Agreements	1 / 5
VR-3.3 Vendor Access Controls and Least Privilege	1 / 5

VR-MON — Monitoring & Offboarding

VR-4.1 Ongoing Vendor Security Monitoring	5 / 5
VR-4.2 Vendor Offboarding and Access Termination	3 / 5
VR-4.3 Supply Chain Risk Program Governance	2 / 5

Security Awareness & Phishing Discovery

Security Awareness & Phishing Discovery v1.0 — District 101 2026 · 3.00/5 · MEDIUM · 8 findings

SA-PROG — Training Program

SA-PHISH — Phishing Simulation

SA-CULT — Reporting Culture

SA-MEAS — Measurement & Improvement

SA-PROG — Training Program

SA-1.1 Training Coverage and Completion	2 / 5
SA-1.2 Training Content Quality and Currency	4 / 5

SA-1.3 Role-Based Security Training	3 / 5

SA-PHISH — Phishing Simulation

SA-2.1 Phishing Simulation Program	2 / 5
SA-2.2 Simulation Template Realism and Variety	5 / 5
SA-2.3 Simulation Results and Remediation	1 / 5

SA-CULT — Reporting Culture

SA-3.1 Suspicious Activity Reporting Mechanism	3 / 5
SA-3.2 Report Triage and Response	2 / 5
SA-3.3 Security Culture and Psychological Safety	5 / 5

SA-MEAS — Measurement & Improvement

SA-4.1 Program Metrics and KPIs	2 / 5
SA-4.2 Leadership Engagement and Tone from the Top	2 / 5
SA-4.3 Program Continuous Improvement	5 / 5

Vulnerability Management Discovery

Vulnerability Management Discovery v1.0 — District 101 2026 · 3.08/5 · MEDIUM · 8 findings

VM-SCAN — Scanning & Discovery

3.0 / 5

VM-RISK — Prioritization & Risk

3.0 / 5

VM-REM — Remediation & Patching

3.3 / 5

VM-VIS — Visibility & Reporting

3.0 / 5

VM-SCAN — Scanning & Discovery

VM-1.1 Vulnerability Scan Coverage	3 / 5
VM-1.2 Authenticated Scanning	4 / 5
VM-1.3 Cloud and SaaS Vulnerability Coverage	2 / 5

VM-RISK — Prioritization & Risk

VM-2.1 CVSS and Risk-Based Prioritization	5 / 5
VM-2.2 Remediation SLAs by Severity	1 / 5
VM-2.3 Risk Acceptance Process	3 / 5

VM-REM — Remediation & Patching

VM-3.1 Patch Deployment Process	3 / 5
VM-3.2 End-of-Life System Management	2 / 5
VM-3.3 Remediation Verification	5 / 5

VM-VIS — Visibility & Reporting

VM-4.1 Attack Surface Inventory	2 / 5
VM-4.2 Vulnerability Metrics and Reporting	4 / 5
VM-4.3 Penetration Testing	3 / 5

Identity & Access Management Discovery

Identity & Access Management Discovery v1.0 — District 101 2026 · 3.17/5 · MEDIUM · 7 findings

IAM-AUTH — Authentication & MFA

3.0 / 5

IAM-LIFE — Account Lifecycle

3.3 / 5

IAM-PRIV — Privileged Access

3.0 / 5

IAM-GOV — Access Governance

3.3 / 5

IAM-AUTH — Authentication & MFA

IAM-1.1 MFA Coverage and Enforcement	2 / 5
IAM-1.2 Password Policy and Credential Hygiene	4 / 5
IAM-1.3 Legacy Authentication and Protocol Blocking	3 / 5

IAM-LIFE — Account Lifecycle

IAM-2.1 Account Provisioning and Joiner Process	5 / 5
IAM-2.2 Account Deprovisioning and Leaver Process	1 / 5
IAM-2.3 Orphaned and Dormant Account Management	4 / 5

IAM-PRIV — Privileged Access

IAM-3.1 Privileged Account Inventory and Separation	3 / 5
IAM-3.2 Privileged Session Monitoring and Control	4 / 5
IAM-3.3 Service Account and Non-Human Identity Management	2 / 5

IAM-GOV — Access Governance

IAM-4.1 Access Reviews and Recertification	5 / 5
IAM-4.2 Single Sign-On Coverage	3 / 5
IAM-4.3 Identity Threat Detection	2 / 5

Zero Trust Maturity Assessment

Zero Trust Maturity Assessment v1.0 — District 101 2026 · 3.25/5 · MEDIUM · 7 findings

ZT-ID — Identity

3.5 / 5

ZT-DEV — Devices

4.0 / 5

ZT-NET — Networks

2.5 / 5

ZT-APP — Applications & Workloads

3.5 / 5

ZT-DATA — Data

2.5 / 5

ZT-ID — Identity

ZT-ID.1 Identity as the Control Plane	3 / 5
ZT-ID.2 Privileged Identity Controls	4 / 5
ZT-ID.3 Non-Human Identity Governance	3 / 5
ZT-ID.4 Identity Federation and SSO	4 / 5

ZT-DEV — Devices

ZT-DEV.1 Device Inventory and Trust Assessment	4 / 5
ZT-DEV.2 Endpoint Security Configuration	4 / 5

ZT-NET — Networks

ZT-NET.1 Network Segmentation and Micro-Segmentation	2 / 5
ZT-NET.2 Encrypted Traffic and Protocol Controls	3 / 5

ZT-APP — Applications & Workloads

ZT-APP.1 Application Access Controls	2 / 5
ZT-APP.2 Workload Security	5 / 5

ZT-DATA — Data

ZT-DATA.1 Data Visibility and Classification	3 / 5
ZT-DATA.2 Data Access Controls and DLP	2 / 5

Asset & Data Inventory Discovery

Asset & Data Inventory Discovery v1.0 — District 101 2026 · 3.25/5 · MEDIUM · 7 findings

INV-HW — Hardware Asset Management

4.0 / 5

INV-SW — Software & SaaS Management

2.7 / 5

INV-DATA — Data Asset Management

3.3 / 5

INV-CLOD — Cloud Asset Visibility

3.0 / 5

INV-HW — Hardware Asset Management

INV-1.1 Hardware Inventory Completeness	4 / 5
INV-1.2 Asset Lifecycle Management	5 / 5

INV-1.3 Unauthorized Device Detection	3 / 5

INV-SW — Software & SaaS Management

INV-2.1 Software and Application Inventory	2 / 5
INV-2.2 SaaS Application Governance	2 / 5
INV-2.3 License Compliance and EOL Tracking	4 / 5

INV-DATA — Data Asset Management

INV-3.1 Sensitive Data Discovery and Location	3 / 5
INV-3.2 Data Classification Coverage	2 / 5
INV-3.3 Data Retention and Disposal Tracking	5 / 5

INV-CLOD — Cloud Asset Visibility

INV-4.1 Cloud Account and Resource Inventory	3 / 5
INV-4.2 Cloud Configuration Baseline	2 / 5
INV-4.3 Cloud Access and Identity Inventory	4 / 5

Data Privacy Baseline Discovery

Data Privacy Baseline Discovery v1.0 — District 101 2026 · 3.33/5 · MEDIUM · 7 findings

DPB-REG — Regulatory Awareness

3.0 / 5

DPB-NOT — Privacy Notices & Consent

4.0 / 5

DPB-RTS — Individual Rights

3.0 / 5

DPB-HAND — Data Handling & Breach

3.3 / 5

DPB-REG — Regulatory Awareness

DPB-1.1 Privacy Regulatory Inventory	3 / 5
DPB-1.2 Personal Data Mapping and Processing Records	2 / 5
DPB-1.3 Privacy Impact Assessment Process	4 / 5

DPB-NOT — Privacy Notices & Consent

DPB-2.1 Privacy Notice Accuracy and Accessibility	5 / 5
DPB-2.2 Consent Mechanisms	4 / 5
DPB-2.3 Children's Data Protection	3 / 5

DPB-RTS — Individual Rights

DPB-3.1 Individual Rights Request Process	4 / 5
DPB-3.2 Data Subject Access Request Fulfillment	3 / 5
DPB-3.3 Opt-Out and Data Deletion Handling	2 / 5

DPB-HAND — Data Handling & Breach

DPB-4.1 Sensitive Data Handling and Minimization	3 / 5
DPB-4.2 Data Breach Detection and Notification Readiness	3 / 5
DPB-4.3 Privacy by Design and Default	4 / 5

Backup & Disaster Recovery Discovery

Backup & Disaster Recovery Discovery v1.0 — District 101 2026 · 3.67/5 · LOW · 5 findings

BDR-COV — Backup Coverage & Strategy

3.7 / 5

BDR-SEC — Backup Security

3.7 / 5

BDR-TEST — Recovery Testing

3.3 / 5

BDR-PLAN — DR Planning & RTO/RPO

4.0 / 5

BDR-COV — Backup Coverage & Strategy

BDR-1.1 Backup Coverage	4 / 5
BDR-1.2 Backup Frequency and Retention	3 / 5
BDR-1.3 Offsite and Cloud Backup Storage	4 / 5

BDR-SEC — Backup Security

BDR-2.1 Immutable and Air-Gapped Backups	3 / 5
BDR-2.2 Backup Access Controls	5 / 5
BDR-2.3 Backup Monitoring and Alerting	3 / 5

BDR-TEST — Recovery Testing

BDR-3.1 Regular Restoration Testing	4 / 5
BDR-3.2 Ransomware Recovery Testing	2 / 5
BDR-3.3 Recovery Integrity Verification	4 / 5

BDR-PLAN — DR Planning & RTO/RPO

BDR-4.1 Recovery Time and Point Objectives	4 / 5
BDR-4.2 Disaster Recovery Plan	5 / 5
BDR-4.3 Business Continuity During Recovery	3 / 5

ALL FINDINGS

CRITICAL · EFFORT TO FIX: HIGH — IDENTITY & ACCESS MANAGEMENT DISCOVERY · ACCOUNT LIFECYCLE

Account Deprovisioning and Leaver Process

QUESTION ASKED

Accounts and access are promptly revoked when employees, contractors, or vendors leave the organization — with automated or procedural controls ensuring no orphaned accounts remain active.

District 101 Response - 1

RISK & IMPACT

The lack of an automated account deprovisioning process poses a significant risk to District 101, as former employees may retain access to sensitive systems and data. This gap can lead to unauthorized access, data breaches, and compliance issues.

Affected: All systems and applications with user accounts

RECOMMENDATION

Implement an automated account deprovisioning process that integrates with HR systems to ensure timely removal of access for former employees.

CRITICAL · EFFORT TO FIX: HIGH — MOBILE & ENDPOINT SECURITY DISCOVERY · MOBILE DEVICE MANAGEMENT

MDM Enrollment and Coverage

QUESTION ASKED

All organization-owned mobile devices — smartphones, tablets, and laptops — are enrolled in a Mobile Device Management (MDM) platform that provides visibility, configuration enforcement, and remote management capability.

District 101 Response - 1

RISK & IMPACT

The lack of a comprehensive MDM enrollment process leaves devices unmanaged and vulnerable to security threats. This gap allows unauthorized access to company resources and data.

Affected: All mobile devices, including company-owned and personal devices used for work purposes.

RECOMMENDATION

Implement an automated MDM enrollment process, ensuring all devices are properly configured and secured upon onboarding.

CRITICAL · EFFORT TO FIX: HIGH — MOBILE & ENDPOINT SECURITY DISCOVERY · MOBILE DEVICE MANAGEMENT

Mobile Application Management

QUESTION ASKED

Corporate applications and data on managed mobile devices are containerized or managed — preventing corporate data from being copied to personal apps, cloud storage, or other unauthorized locations.

District 101 Response - 1

RISK & IMPACT

The absence of a mobile application management policy enables unregulated app installations, introducing potential security risks and data breaches.

Affected: All mobile devices with access to company resources and data.

RECOMMENDATION

Develop and enforce a mobile application management policy, regulating app installations and usage on company-owned and personal devices.

CRITICAL · EFFORT TO FIX: HIGH

BUSINESS CONTINUITY MANAGEMENT · BCM GOVERNANCE & POLICY

BCM Policy and Scope

QUESTION ASKED

A formal BCM policy documents the organization's commitment to business continuity, defines the scope of the program, and establishes the framework for BCM governance.

District 101 Response - 1

RISK & IMPACT

District 101 lacks a comprehensive BCM policy and scope, which hinders the organization's ability to effectively manage continuity risks.

Affected: All organizational systems and data

RECOMMENDATION

Develop a BCM policy that outlines the organization's continuity objectives, roles, and responsibilities, as well as its approach to managing continuity risks.

CRITICAL · EFFORT TO FIX: HIGH

IT POLICY LIBRARY REVIEW · INCIDENT RESPONSE & PLAYBOOKS

Incident Response Plan (IRP)

QUESTION ASKED

A formal documented plan providing the organization with a roadmap for detecting, responding to, and recovering from information security incidents, covering all six NIST phases.

District 101 Response - 1

RISK & IMPACT

The lack of a comprehensive Incident Response Plan (IRP) leaves District 101 vulnerable to security incidents. An IRP is essential for timely response and mitigation of security breaches.

Affected: All systems and data

RECOMMENDATION

Develop an IRP that outlines incident response procedures, assigns roles and responsibilities, and establishes communication protocols.

CRITICAL · EFFORT TO FIX: HIGH

IT POLICY LIBRARY REVIEW · INCIDENT RESPONSE & PLAYBOOKS

Insider Threat Response Playbook

QUESTION ASKED

A playbook providing guidance for detecting, investigating, and responding to potential insider threats, including malicious insiders, negligent employees, and compromised credentials.

District 101 Response - 1

RISK & IMPACT

The absence of an Insider Threat Response Playbook increases the risk of insider threats going undetected. An effective playbook is necessary for identifying and responding to insider threats.

Affected: All systems and data

RECOMMENDATION

Develop an Insider Threat Response Playbook that outlines procedures for detecting, reporting, and responding to insider threats.

CRITICAL · EFFORT TO FIX: HIGH

IT POLICY LIBRARY REVIEW · DATA MANAGEMENT & CLASSIFICATION POLICIES

Privacy Policy & PII Handling Policy

QUESTION ASKED

A policy governing the collection, processing, storage, sharing, and disposal of personally identifiable information (PII) in compliance with applicable privacy laws and regulations.

District 101 Response - 1

RISK & IMPACT

The lack of a Privacy Policy & PII Handling Policy puts sensitive personal identifiable information (PII) at risk. A policy is necessary for protecting PII and ensuring compliance with regulations.

Affected: Systems containing PII

RECOMMENDATION

Develop a Privacy Policy & PII Handling Policy that outlines procedures for collecting, storing, and handling PII.

CRITICAL · EFFORT TO FIX: HIGH

IT POLICY LIBRARY REVIEW · ENDPOINT & DEVICE SECURITY POLICIES

Endpoint Security Policy

QUESTION ASKED

A policy governing the security configuration, protection software, and monitoring requirements for all endpoints including desktops, laptops, servers, and virtual machines.

District 101 Response - 1

RISK & IMPACT

The absence of an Endpoint Security Policy leaves endpoints vulnerable to security threats. An effective policy is necessary for securing endpoints and preventing the spread of malware.

Affected: All endpoints

RECOMMENDATION

Develop an Endpoint Security Policy that outlines procedures for endpoint security, including antivirus software, firewall configuration, and patch management.

CRITICAL · EFFORT TO FIX: HIGH

IT POLICY LIBRARY REVIEW · HUMAN RESOURCES & ACCEPTABLE USE POLICIES

Termination & Offboarding Security Policy

QUESTION ASKED

A policy governing the security steps required when an employee or contractor leaves the organization, including immediate access revocation, device return, data handling, and exit interview requirements.

District 101 Response - 1

RISK & IMPACT

The lack of a Termination & Offboarding Security Policy increases the risk of former employees accessing sensitive systems and data. A policy is necessary for ensuring secure offboarding procedures.

Affected: All systems and data

RECOMMENDATION

Develop a Termination & Offboarding Security Policy that outlines procedures for revoking access to systems and data upon employee termination.

CRITICAL · EFFORT TO FIX: HIGH — IT POLICY LIBRARY REVIEW · BUSINESS CONTINUITY & DISASTER RECOVERY POLICIES

Business Continuity Policy

QUESTION ASKED

A top-level policy establishing the organization's commitment to maintaining critical business functions during and after a disruptive event, and governing the business continuity program.

District 101 Response - 1

RISK & IMPACT

The absence of a Business Continuity Policy puts District 101 at risk of significant disruption during disasters or outages. A policy is necessary for ensuring minimal disruption to operations.

Affected: All systems and data

RECOMMENDATION

Develop a Business Continuity Policy that outlines procedures for maintaining business operations during disasters or outages.

CRITICAL · EFFORT TO FIX: HIGH — IT POLICY LIBRARY REVIEW · BUSINESS CONTINUITY & DISASTER RECOVERY POLICIES

Disaster Recovery Policy

QUESTION ASKED

A policy governing the technical recovery of IT systems and infrastructure following a disaster, including recovery objectives, backup requirements, alternate site provisions, and testing requirements.

District 101 Response - 1

RISK & IMPACT

The lack of a Disaster Recovery Policy increases the risk of significant data loss during disasters. A policy is necessary for ensuring timely recovery of critical systems and data.

Affected: All systems and data

RECOMMENDATION

Develop a Disaster Recovery Policy that outlines procedures for recovering critical systems and data during disasters.

CRITICAL · EFFORT TO FIX: HIGH — IT POLICY LIBRARY REVIEW · BUSINESS CONTINUITY & DISASTER RECOVERY POLICIES

Backup & Restore Policy

QUESTION ASKED

A policy governing the backup of organizational data and systems, including frequency, retention, storage location, encryption, and regular restoration testing.

District 101 Response - 1

RISK & IMPACT

The absence of a Backup & Restore Policy puts District 101 at risk of significant data loss. A policy is necessary for ensuring regular backups and timely restoration of critical systems and data.

Affected: All systems and data

RECOMMENDATION

Develop a Backup & Restore Policy that outlines procedures for backing up and restoring critical systems and data.

CRITICAL · EFFORT TO FIX: HIGH

IT POLICY LIBRARY REVIEW · COMPLIANCE & AUDIT POLICIES

Regulatory Compliance Policy

QUESTION ASKED

A policy identifying all applicable legal, regulatory, and contractual obligations affecting the organization and establishing responsibilities for maintaining and demonstrating compliance.

District 101 Response - 1

RISK & IMPACT

The lack of a Regulatory Compliance Policy increases the risk of non-compliance with regulations. A policy is necessary for ensuring compliance with relevant laws and regulations.

Affected: All systems and data

RECOMMENDATION

Develop a Regulatory Compliance Policy that outlines procedures for complying with relevant laws and regulations.

CRITICAL · EFFORT TO FIX: HIGH

EDUCATION POLICY & COMPLIANCE REVIEW · GOVERNANCE & POLICY PROGRAM

Risk Assessment Program

QUESTION ASKED

A formal risk assessment process is conducted at least annually covering all systems that store, process, or transmit student or sensitive institutional data.

District 101 Response - 1

RISK & IMPACT

District 101 lacks a formal risk assessment program, which leaves the district vulnerable to unidentified security threats.

Affected: All systems and data

RECOMMENDATION

Conduct a comprehensive risk assessment to identify and prioritize potential security threats.

CRITICAL · EFFORT TO FIX: HIGH

EDUCATION POLICY & COMPLIANCE REVIEW · STATE STUDENT PRIVACY LAWS

State Breach Notification Compliance

QUESTION ASKED

The institution has breach notification procedures that comply with applicable state breach notification laws, including required timelines, notification content, and regulatory reporting obligations.

District 101 Response - 1

RISK & IMPACT

District 101 does not have a state breach notification compliance program in place, which could result in non-compliance with state regulations.

Affected: Student data and systems

RECOMMENDATION

Establish a state breach notification compliance program to ensure timely notification in the event of a breach.

CRITICAL · EFFORT TO FIX: HIGH

VULNERABILITY MANAGEMENT DISCOVERY · PRIORITIZATION & RISK

Remediation SLAs by Severity

QUESTION ASKED

Remediation Service Level Agreements (SLAs) define maximum time-to-remediate for each vulnerability severity level, and compliance against those SLAs is tracked.

District 101 Response - 1

RISK & IMPACT

District 101 lacks remediation SLAs by severity, which can lead to delayed or ineffective vulnerability management. This gap increases the risk of exploitation and potential security breaches.

Affected: All systems with identified vulnerabilities

RECOMMENDATION

Establish clear remediation SLAs based on vulnerability severity, ensuring that high-risk vulnerabilities are addressed promptly.

CRITICAL · EFFORT TO FIX: HIGH

SECURITY AWARENESS & PHISHING DISCOVERY · PHISHING SIMULATION

Simulation Results and Remediation

QUESTION ASKED

Phishing simulation results drive targeted action — not just measurement. Employees who fail receive immediate feedback, additional training, and follow-up assessment.

District 101 Response - 1

RISK & IMPACT

The current phishing simulation results and remediation process is inadequate, leaving employees who fall victim to simulations without targeted support or guidance.

Affected: Employee email and network access

RECOMMENDATION

Implement a comprehensive remediation plan that includes personalized training and awareness activities for employees who fail phishing simulations.

CRITICAL · EFFORT TO FIX: HIGH

INCIDENT RESPONSE READINESS DISCOVERY · IR PLAN & POLICY

Incident Classification and Declaration

QUESTION ASKED

Clear criteria define what constitutes a security incident, how severity levels are classified, and who has authority to declare an incident and activate the response plan.

District 101 Response - 1

RISK & IMPACT

The lack of an Incident Classification and Declaration process hinders timely and effective incident response, increasing the risk of prolonged downtime and data breaches.

Affected: All systems and data

RECOMMENDATION

Develop and implement a clear incident classification framework, defining criteria for declaring incidents and triggering response procedures.

CRITICAL · EFFORT TO FIX: HIGH — INCIDENT RESPONSE READINESS DISCOVERY · TESTING & EXERCISES

Tabletop Exercise Program

QUESTION ASKED

Tabletop exercises test the IR plan and the team's decision-making under simulated incident conditions — at least annually, using realistic scenarios.

District 101 Response - 1

RISK & IMPACT

The absence of a Tabletop Exercise Program leaves the organization unprepared to respond to incidents, increasing the risk of ineffective response and prolonged recovery.

Affected: Incident Response Team, IT systems

RECOMMENDATION

Establish a regular tabletop exercise program, incorporating scenario-based training and incident response plan testing.

CRITICAL · EFFORT TO FIX: HIGH — INCIDENT RESPONSE READINESS DISCOVERY · TESTING & EXERCISES

Post-Incident Review Process

QUESTION ASKED

After every significant security incident or exercise, a structured post-incident review (PIR) or "lessons learned" session is conducted and findings are used to improve the IRP and controls.

District 101 Response - 1

RISK & IMPACT

The lack of a Post-Incident Review Process prevents the organization from identifying areas for improvement, optimizing incident response, and reducing the risk of future incidents.

Affected: Incident Response Team, IT systems

RECOMMENDATION

Develop and implement a post-incident review process, incorporating root cause analysis and lessons learned to inform incident response plan updates.

CRITICAL · EFFORT TO FIX: HIGH — CLOUD SECURITY POSTURE DISCOVERY · IDENTITY & ACCESS IN CLOUD

Cloud User MFA and Conditional Access

QUESTION ASKED

MFA is enforced for all cloud platform users — not just admins — with conditional access policies that add friction for high-risk sign-ins such as new devices, unknown locations, or legacy protocols.

District 101 Response - 1

RISK & IMPACT

Cloud User MFA and Conditional Access is not implemented, leaving users vulnerable to unauthorized access.

Affected: All cloud-based systems and applications

RECOMMENDATION

Implement multi-factor authentication (MFA) for all cloud users and configure conditional access policies to restrict access based on user location, device, and other factors.

CRITICAL · EFFORT TO FIX: HIGH

VENDOR & THIRD-PARTY RISK DISCOVERY · CONTRACT CONTROLS

Data Processing Agreements

QUESTION ASKED

Formal Data Processing Agreements (DPAs) or equivalent privacy agreements are in place with all vendors that process personal data — defining purpose, data types, retention, and obligations.

District 101 Response - 1

RISK & IMPACT

District 101 lacks comprehensive Data Processing Agreements, which exposes sensitive data to potential breaches and non-compliance with regulations.

Affected: All systems and data handled by third-party vendors

RECOMMENDATION

Develop and implement standardized Data Processing Agreements that outline specific security controls, data protection requirements, and incident response procedures for all vendors handling sensitive data.

CRITICAL · EFFORT TO FIX: HIGH

VENDOR & THIRD-PARTY RISK DISCOVERY · CONTRACT CONTROLS

Vendor Access Controls and Least Privilege

QUESTION ASKED

Vendor access to organizational systems, data, and facilities is governed by least privilege — vendors receive only the access needed for their contracted function, with access logged and revocable.

District 101 Response - 1

RISK & IMPACT

Insufficient Vendor Access Controls and Least Privilege principles increase the attack surface and potential for lateral movement in case of a breach.

Affected: All systems accessed by vendors

RECOMMENDATION

Implement robust access controls, including multi-factor authentication, role-based access control, and least privilege principles to minimize vendor access to sensitive systems and data.

CRITICAL · EFFORT TO FIX: HIGH

PHYSICAL SECURITY DISCOVERY · FACILITY ACCESS CONTROL

Electronic Access Control System

QUESTION ASKED

Facilities are protected by electronic access control — badge, PIN, biometric, or combination — that restricts entry to authorized personnel and creates an auditable access log.

District 101 Response - 1

RISK & IMPACT

The lack of an electronic access control system poses a significant risk, allowing unauthorized individuals to access the facility without detection or tracking.

Affected: All systems and data within the facility

RECOMMENDATION

Implement an electronic access control system that includes features such as card readers, biometric authentication, and real-time monitoring.

CRITICAL · EFFORT TO FIX: HIGH

PHYSICAL SECURITY DISCOVERY · FACILITY ACCESS CONTROL

Key and Badge Management

QUESTION ASKED

Physical keys and access badges are inventoried, issued through a controlled process, and promptly deactivated or collected when employees or contractors depart.

District 101 Response - 1

RISK & IMPACT

Inadequate key and badge management increases the risk of unauthorized access to sensitive areas and equipment.

Affected: Sensitive areas and equipment within the facility

RECOMMENDATION

Develop and enforce a comprehensive key and badge management policy that includes procedures for issuance, revocation, and tracking.

CRITICAL · EFFORT TO FIX: HIGH

PHYSICAL SECURITY DISCOVERY · FACILITY ACCESS CONTROL

Physical Security Perimeter

QUESTION ASKED

The physical perimeter of facilities is secured — with controlled entry points, clear demarcation of restricted areas, and no unmonitored access paths that bypass access controls.

District 101 Response - 1

RISK & IMPACT

The physical security perimeter is vulnerable to unauthorized access, allowing individuals to bypass security controls and gain entry to the facility.

Affected: All systems and data within the facility

RECOMMENDATION

Conduct a thorough assessment of the physical security perimeter and implement necessary controls such as fencing, gates, and surveillance cameras.

CRITICAL · EFFORT TO FIX: HIGH

PHYSICAL SECURITY DISCOVERY · MEDIA & DOCUMENT SECURITY

Clean Desk and Screen Lock Policy

QUESTION ASKED

Sensitive documents and information are secured when workspaces are unattended, and screens are locked automatically after a short idle period — preventing casual observation or opportunistic access.

District 101 Response - 1

RISK & IMPACT

The lack of a clean desk and screen lock policy increases the risk of sensitive information being compromised through visual hacking or unauthorized access.

Affected: Sensitive information and equipment within the facility

RECOMMENDATION

Establish a comprehensive clean desk and screen lock policy that includes procedures for securing sensitive information and equipment.

CRITICAL · EFFORT TO FIX: HIGH

AI & EMERGING TECHNOLOGY RISK DISCOVERY · AI GOVERNANCE & POLICY

AI Acceptable Use Policy

QUESTION ASKED

A policy exists defining which AI tools are approved for organizational use, what data may be entered into them, and what uses are prohibited — communicated to all staff.

District 101 Response - 1

RISK & IMPACT

The lack of an AI Acceptable Use Policy poses a significant risk to the organization, as it may lead to unauthorized or malicious use of AI tools.

Affected: All systems and data utilizing AI tools

RECOMMENDATION

Develop and implement a comprehensive AI Acceptable Use Policy that outlines acceptable uses of AI tools, consequences for non-compliance, and procedures for reporting incidents.

CRITICAL · EFFORT TO FIX: HIGH

AI & EMERGING TECHNOLOGY RISK DISCOVERY · AI GOVERNANCE & POLICY

AI Governance Structure

QUESTION ASKED

Clear ownership and governance structures exist for AI risk management — including who approves new AI tools, who monitors AI risk, and who escalates AI-related incidents.

District 101 Response - 1

RISK & IMPACT

The absence of an AI Governance Structure hinders the organization's ability to oversee AI-related activities, leading to potential security risks and non-compliance with regulations.

Affected: All systems and data utilizing AI tools

RECOMMENDATION

Establish a comprehensive AI Governance Structure that includes clear roles and responsibilities, risk management processes, and audit mechanisms.

CRITICAL · EFFORT TO FIX: HIGH

AI & EMERGING TECHNOLOGY RISK DISCOVERY · SHADOW AI & DATA LEAKAGE

Shadow AI Detection and Control

QUESTION ASKED

The organization has visibility into unauthorized AI tool usage by employees — including browser-based LLMs, AI-powered productivity tools, and AI features within sanctioned software — and takes action to reduce unsanctioned data exposure.

District 101 Response - 1

RISK & IMPACT

The lack of Shadow AI Detection and Control measures increases the risk of unauthorized AI usage, which may lead to security breaches or data leakage.

Affected: All systems and data utilizing AI tools

RECOMMENDATION

Implement a Shadow AI Detection and Control solution that can identify and prevent unauthorized AI usage, and provide regular monitoring and reporting capabilities.

CRITICAL · EFFORT TO FIX: HIGH

AI & EMERGING TECHNOLOGY RISK DISCOVERY · SHADOW AI & DATA LEAKAGE

Sensitive Data Leakage via AI Tools

QUESTION ASKED

Controls are in place to prevent employees from inadvertently — or deliberately — entering sensitive organizational data into AI tools that do not provide adequate data protection.

District 101 Response - 1

RISK & IMPACT

Sensitive Data Leakage via AI Tools poses a significant risk to the organization, as it may lead to unauthorized disclosure of sensitive information.

Affected: All systems and data containing sensitive information

RECOMMENDATION

Implement robust access controls and encryption mechanisms for sensitive data, and conduct regular risk assessments of AI tools to identify potential security risks.

CRITICAL · EFFORT TO FIX: HIGH

AI & EMERGING TECHNOLOGY RISK DISCOVERY · AI VENDOR RISK

AI Model and Output Risk

QUESTION ASKED

The organization understands and manages risks arising from AI model outputs — including hallucinations, bias, and errors — particularly where AI outputs influence decisions affecting individuals or operations.

District 101 Response - 1

RISK & IMPACT

The lack of adequate AI Model and Output Risk management increases the risk of biased or inaccurate AI outputs, which may lead to security breaches or reputational damage.

Affected: All systems utilizing AI models

RECOMMENDATION

Develop and implement a comprehensive AI Model and Output Risk management framework that includes regular testing, validation, and monitoring of AI models and outputs.

CRITICAL · EFFORT TO FIX: HIGH

AI & EMERGING TECHNOLOGY RISK DISCOVERY · AI-ENABLED THREATS

AI-Enhanced Phishing and Social Engineering

QUESTION ASKED

The organization's defenses and awareness program account for the dramatic improvement in phishing quality enabled by AI — including perfectly-written spear phishing emails, AI-generated audio deepfakes of executives, and AI-powered pretexting.

District 101 Response - 1

RISK & IMPACT

AI-Enhanced Phishing and Social Engineering attacks pose a significant risk to the organization, as they may lead to security breaches or data leakage.

Affected: All systems and data accessible via email

RECOMMENDATION

Provide regular training on AI-Enhanced Phishing and Social Engineering attacks to employees, and implement robust email filtering and monitoring mechanisms.

CRITICAL · EFFORT TO FIX: HIGH

AI & EMERGING TECHNOLOGY RISK DISCOVERY · AI-ENABLED THREATS

AI-Accelerated Attack Response Readiness

QUESTION ASKED

The organization's incident response capability accounts for AI-accelerated attack timelines — where attackers now move from initial access to data exfiltration or ransomware deployment in hours rather than days or weeks.

District 101 Response - 1

RISK & IMPACT

The lack of adequate AI-Accelerated Attack Response Readiness increases the risk of security breaches or reputational damage, as the organization may not be able to respond effectively to AI-accelerated attacks.

Affected: All systems and data

RECOMMENDATION

Develop and implement an incident response plan that includes procedures for responding to AI-accelerated attacks, and conduct regular training and exercises to ensure readiness.

HIGH · EFFORT TO FIX: MEDIUM

IDENTITY & ACCESS MANAGEMENT DISCOVERY · AUTHENTICATION & MFA

MFA Coverage and Enforcement

QUESTION ASKED

Multi-factor authentication is enforced for all users across all systems — not just selected systems or users — with phishing-resistant options deployed for high-risk roles.

District 101 Response - 2

RISK & IMPACT

Insufficient MFA coverage leaves District 101 vulnerable to phishing attacks, password spraying, and other authentication-based threats. This gap can lead to unauthorized access, data breaches, and compliance issues.

Affected: All systems and applications with user accounts

RECOMMENDATION

Conduct a thorough risk assessment to identify high-risk users and systems, and implement MFA coverage accordingly. Consider implementing adaptive MFA policies based on user behavior and risk profiles.

HIGH · EFFORT TO FIX: MEDIUM

IDENTITY & ACCESS MANAGEMENT DISCOVERY · PRIVILEGED ACCESS

Service Account and Non-Human Identity Management

QUESTION ASKED

Service accounts, API keys, certificates, and other non-human identities are inventoried, least-privileged, regularly rotated, and monitored — preventing them from becoming persistent, unmonitored attack vectors.

District 101 Response - 2

RISK & IMPACT

Inadequate service account management poses a significant risk to District 101, as these accounts often have elevated privileges and can be used by attackers to move laterally within the network. This gap can lead to unauthorized access, data breaches, and compliance issues.

Affected: All systems and applications with service accounts

RECOMMENDATION

Develop and implement a comprehensive privileged access management program that includes service account management. Ensure that all service accounts are properly inventoried, monitored, and controlled.

HIGH · EFFORT TO FIX: MEDIUM

IDENTITY & ACCESS MANAGEMENT DISCOVERY · ACCESS GOVERNANCE

Identity Threat Detection

QUESTION ASKED

Anomalous identity activity — such as impossible travel, unfamiliar device logins, bulk data downloads, and unusual off-hours access — is detected, alerted, and investigated.

District 101 Response - 2

RISK & IMPACT

The lack of effective identity threat detection capabilities leaves District 101 vulnerable to advanced threats, such as insider attacks and credential-based attacks. This gap can lead to unauthorized access, data breaches, and compliance issues.

Affected: All systems and applications with user accounts

RECOMMENDATION

Enhance identity threat detection capabilities through the implementation of advanced monitoring tools and techniques, such as user behavior analytics and machine learning-based anomaly detection.

HIGH · EFFORT TO FIX: MEDIUM

MOBILE & ENDPOINT SECURITY DISCOVERY · MOBILE DEVICE MANAGEMENT

MDM Policy Configuration and Enforcement

QUESTION ASKED

MDM policies enforce security configuration baselines on managed devices — including screen lock, encryption, app management, and compliance requirements — with non-compliant devices quarantined.

District 101 Response - 2

RISK & IMPACT

Inadequate MDM policy configuration and enforcement compromise the security of managed devices. This gap allows unauthorized changes to device settings and configurations.

Affected: All mobile devices enrolled in the MDM solution.

RECOMMENDATION

Review and refine MDM policies, ensuring strict access controls and enforcing compliance with organizational security standards.

HIGH · EFFORT TO FIX: MEDIUM

MOBILE & ENDPOINT SECURITY DISCOVERY · BYOD POLICY & CONTROLS

BYOD Policy and Scope

QUESTION ASKED

A clear, communicated BYOD policy defines which personal devices may access organizational resources, what organizational controls apply, and what organizational data may reside on personal devices.

District 101 Response - 2

RISK & IMPACT

The BYOD policy lacks clear scope and definition, leading to confusion among employees and potential security risks. This gap enables unauthorized access to company resources and data.

Affected: All personal devices used for work purposes.

RECOMMENDATION

Review and refine the BYOD policy, clearly defining scope, security controls, and employee responsibilities.

HIGH · EFFORT TO FIX: MEDIUM

DATA PRIVACY BASELINE DISCOVERY · REGULATORY AWARENESS

Personal Data Mapping and Processing Records

QUESTION ASKED

The organization knows what personal data it collects, where it comes from, how it is used, who it is shared with, and how long it is retained — documented in a Record of Processing Activities (ROPA) or equivalent.

District 101 Response - 2

RISK & IMPACT

District 101 lacks a comprehensive Personal Data Mapping and Processing Records system, making it challenging to track data flows and ensure regulatory compliance.

Affected: All systems handling personal data

RECOMMENDATION

Develop a centralized data mapping tool to catalog personal data processing activities, including data sources, storage locations, and transmission protocols.

HIGH · EFFORT TO FIX: MEDIUM

DATA PRIVACY BASELINE DISCOVERY · INDIVIDUAL RIGHTS

Opt-Out and Data Deletion Handling

QUESTION ASKED

Opt-out requests (marketing, sale of data, profiling) and deletion requests are honored completely and promptly — including propagation to third parties and sub-processors — not just suppressed in the primary marketing list.

District 101 Response - 2

RISK & IMPACT

District 101's Opt-Out and Data Deletion Handling process is inadequate, potentially leading to non-compliance with individual rights requests.

Affected: Systems storing personal data

RECOMMENDATION

Establish a clear process for handling opt-out and data deletion requests, including automated workflows and employee training.

HIGH · EFFORT TO FIX: MEDIUM

ZERO TRUST MATURITY ASSESSMENT · NETWORKS

Network Segmentation and Micro-Segmentation

QUESTION ASKED

Networks are segmented based on sensitivity and function — with implicit trust from network location eliminated and traffic between segments explicitly inspected and authorized.

District 101 Response - 2

RISK & IMPACT

District 101's network segmentation and micro-segmentation controls are inadequate, leaving the organization vulnerable to lateral movement in the event of a breach. This gap allows attackers to easily move between systems and exploit sensitive data.

Affected: All network-connected systems and devices

RECOMMENDATION

Implement a more comprehensive network segmentation strategy, utilizing techniques such as VLANs, subnets, and access control lists (ACLs) to restrict traffic flow and limit the attack surface.

HIGH · EFFORT TO FIX: MEDIUM

ZERO TRUST MATURITY ASSESSMENT · APPLICATIONS & WORKLOADS

Application Access Controls

QUESTION ASKED

Access to applications is granted per-user, per-session, and based on verified identity and device posture — not on network location — with sensitive application access requiring additional verification.

District 101 Response - 2

RISK & IMPACT

District 101's application access controls are insufficient, allowing users to access applications and data without proper authorization. This gap increases the risk of unauthorized data access and malicious activity.

Affected: All applications and systems with sensitive data

RECOMMENDATION

Develop and enforce robust application access controls, utilizing techniques such as role-based access control (RBAC), attribute-based access control (ABAC), and multi-factor authentication (MFA).

HIGH · EFFORT TO FIX: MEDIUM

ZERO TRUST MATURITY ASSESSMENT · DATA

Data Access Controls and DLP

QUESTION ASKED

Access to sensitive data is controlled based on identity, device posture, and data classification — with DLP enforcing that data cannot leave authorized contexts regardless of user action.

District 101 Response - 2

RISK & IMPACT

District 101's data access controls and DLP measures are inadequate, leaving sensitive information vulnerable to unauthorized access and exfiltration. This gap increases the risk of data breaches and reputational damage.

Affected: All systems and devices storing or processing sensitive data

RECOMMENDATION

Implement a comprehensive data access control strategy, including data classification, encryption, and monitoring for suspicious activity. Utilize DLP tools to detect and prevent data exfiltration attempts.

HIGH · EFFORT TO FIX: MEDIUM

THIRD-PARTY RISK MANAGEMENT PROGRAM · PROGRAM GOVERNANCE

TPRM Policy and Framework

QUESTION ASKED

A formal TPRM policy documents the organization's approach to third-party risk, defining scope, risk tolerance, roles, and the processes that constitute the program.

District 101 Response - 2

RISK & IMPACT

The lack of a comprehensive TPRM policy and framework hinders the program's ability to effectively govern and manage third-party risks

Affected: All systems and data managed by third-party vendors

RECOMMENDATION

Develop and implement a TPRM policy and framework that outlines the program's objectives, roles and responsibilities, and risk management processes

HIGH · EFFORT TO FIX: MEDIUM

THIRD-PARTY RISK MANAGEMENT PROGRAM · PROGRAM GOVERNANCE

Fourth-Party and Supply Chain Risk

QUESTION ASKED

The organization understands and manages risks from fourth parties — vendors' vendors — and supply chain dependencies that could compromise organizational security through indirect pathways.

District 101 Response - 2

RISK & IMPACT

The absence of a process for identifying and assessing fourth-party risks exposes District 101 to potential supply chain vulnerabilities

Affected: Systems and data managed by third-party vendors with access to sensitive information

RECOMMENDATION

Establish a process for identifying and assessing fourth-party risks, including conducting regular risk assessments and implementing mitigation strategies as needed

HIGH · EFFORT TO FIX: MEDIUM

THIRD-PARTY RISK MANAGEMENT PROGRAM · VENDOR INVENTORY

Vendor Criticality and Concentration Risk

QUESTION ASKED

The organization identifies vendors whose disruption or compromise would have catastrophic impact — including single points of failure and concentration risk — and manages resilience accordingly.

District 101 Response - 2

RISK & IMPACT

The lack of a clear understanding of vendor criticality and concentration risk hinders the program's ability to effectively prioritize and manage vendor risks

Affected: Systems and data managed by critical vendors

RECOMMENDATION

Develop and implement a methodology for assessing vendor criticality and concentration risk, including identifying key vendors and implementing mitigation strategies as needed

HIGH · EFFORT TO FIX: MEDIUM

THIRD-PARTY RISK MANAGEMENT PROGRAM · DUE DILIGENCE

Pre-Onboarding Security Assessment

QUESTION ASKED

New vendors that will access sensitive data or critical systems are assessed for security posture before being granted access — with assessment scope proportionate to vendor risk tier.

District 101 Response - 2

RISK & IMPACT

The absence of pre-onboarding security assessments increases the risk of onboarding vendors with inadequate security controls

Affected: Systems and data managed by new vendors

RECOMMENDATION

Implement a process for conducting pre-onboarding security assessments, including reviewing vendor security questionnaires and conducting site visits as needed

HIGH · EFFORT TO FIX: MEDIUM

THIRD-PARTY RISK MANAGEMENT PROGRAM · CONTRACT MANAGEMENT

Security and Privacy Contract Requirements

QUESTION ASKED

All contracts with in-scope vendors include specific, enforceable security and privacy requirements — proportionate to the vendor's risk tier and the sensitivity of data or access involved.

District 101 Response - 2

RISK & IMPACT

The lack of robust security and privacy requirements in contracts increases the risk of vendors mishandling sensitive information

Affected: Systems and data managed by third-party vendors with access to sensitive information

RECOMMENDATION

Review and update contract templates to include clear security and privacy requirements, including data protection and incident response obligations

HIGH · EFFORT TO FIX: MEDIUM

THIRD-PARTY RISK MANAGEMENT PROGRAM · CONTRACT MANAGEMENT

Vendor Access Controls in Contracts

QUESTION ASKED

Contractual terms governing vendor access to organizational systems and data — including MFA, least privilege, session monitoring, and access termination — are defined and enforceable.

District 101 Response - 2

RISK & IMPACT

The absence of vendor access controls in contracts increases the risk of unauthorized access to sensitive systems and data

Affected: Systems and data managed by third-party vendors with access to sensitive information

RECOMMENDATION

Review and update contract templates to include clear requirements for vendor access controls, including authentication, authorization, and accounting (AAA) protocols

HIGH · EFFORT TO FIX: MEDIUM

THIRD-PARTY RISK MANAGEMENT PROGRAM · ONGOING MONITORING

Vendor Performance and SLA Management

QUESTION ASKED

Security SLAs and performance commitments in vendor contracts are monitored, measured, and enforced — with underperforming vendors subject to remediation plans or relationship consequences.

District 101 Response - 2

RISK & IMPACT

The lack of a process for tracking vendor performance and SLA adherence increases the risk of vendors failing to meet contractual obligations

Affected: Systems and data managed by third-party vendors with service level agreements (SLAs)

RECOMMENDATION

Implement a continuous monitoring program to track vendor performance and SLA adherence, including regular reporting and remediation as needed

HIGH · EFFORT TO FIX: MEDIUM

THIRD-PARTY RISK MANAGEMENT PROGRAM · ONGOING MONITORING

TPRM Metrics and Program Performance

QUESTION ASKED

The TPRM program tracks metrics that demonstrate its effectiveness — vendor risk coverage, assessment completion rates, finding remediation rates, and incident reduction — and uses them to continuously improve.

District 101 Response - 2

RISK & IMPACT

The absence of key performance indicators (KPIs) to measure the effectiveness of the TPRM program hinders the ability to evaluate program success

Affected: All systems and data managed by third-party vendors

RECOMMENDATION

Develop and track KPIs to measure the effectiveness of the TPRM program, including metrics for vendor risk management, contract compliance, and incident response

HIGH · EFFORT TO FIX: MEDIUM

THIRD-PARTY RISK MANAGEMENT PROGRAM · VENDOR LIFECYCLE

TPRM Program Continuous Improvement

QUESTION ASKED

The TPRM program learns from incidents, assessments, and external developments — continuously improving processes, controls, and capabilities to stay ahead of evolving third-party risk.

District 101 Response - 2

RISK & IMPACT

The lack of a process for continuous improvement hinders the ability to identify and address program weaknesses

Affected: All systems and data managed by third-party vendors

RECOMMENDATION

Establish a process for continuous improvement, including regular reviews of program effectiveness and implementation of remediation strategies as needed

HIGH · EFFORT TO FIX: MEDIUM

BUSINESS CONTINUITY MANAGEMENT · BCM GOVERNANCE & POLICY

Legal, Regulatory, and Contractual Continuity Requirements

QUESTION ASKED

BCM plans and capabilities account for legal, regulatory, and contractual obligations that apply during disruptions — including notification requirements, service level obligations, and regulatory reporting.

District 101 Response - 2

RISK & IMPACT

District 101 has not thoroughly reviewed legal, regulatory, and contractual requirements, which may lead to non-compliance and reputational damage.

Affected: Contract management systems, regulatory compliance databases

RECOMMENDATION

Conduct a comprehensive review of relevant laws, regulations, and contracts to identify continuity requirements and ensure compliance.

HIGH · EFFORT TO FIX: MEDIUM

BUSINESS CONTINUITY MANAGEMENT · BUSINESS IMPACT ANALYSIS

Critical Function Identification

QUESTION ASKED

All functions critical to organizational viability — and their maximum tolerable period of disruption (MTPD) — are identified and agreed by business owners and senior leadership.

District 101 Response - 2

RISK & IMPACT

District 101's critical function identification process is incomplete, which may lead to inadequate business impact analysis and ineffective recovery strategies.

Affected: Business process management systems, stakeholder engagement platforms

RECOMMENDATION

Enhance the critical function identification process by engaging with stakeholders and conducting a thorough review of organizational processes.

HIGH · EFFORT TO FIX: MEDIUM

BUSINESS CONTINUITY MANAGEMENT · RECOVERY STRATEGY

Recovery Strategy Selection and Validation

QUESTION ASKED

Recovery strategies are developed for each critical function — with strategies selected based on RTO/RPO requirements, cost, and feasibility — and validated before being incorporated into plans.

District 101 Response - 2

RISK & IMPACT

District 101's recovery strategy selection and validation process is inadequate, which may lead to ineffective recovery strategies and prolonged downtime.

Affected: Disaster recovery systems, cloud infrastructure

RECOMMENDATION

Validate recovery strategies through regular exercises and reviews, and consider alternative approaches such as cloud-based disaster recovery.

HIGH · EFFORT TO FIX: MEDIUM

BUSINESS CONTINUITY MANAGEMENT · RECOVERY STRATEGY

Alternate Facility and Supply Chain Strategy

QUESTION ASKED

Strategies are in place for scenarios where primary facilities are unavailable and critical suppliers are disrupted — including alternate locations, emergency procurement, and supply chain redundancy.

District 101 Response - 2

RISK & IMPACT

District 101 lacks a comprehensive alternate facility and supply chain strategy, which may lead to disruptions in critical operations.

Affected: Supply chain management systems, facility management databases

RECOMMENDATION

Develop an alternate facility and supply chain strategy that includes identification of alternative facilities, suppliers, and logistics providers.

HIGH · EFFORT TO FIX: MEDIUM

BUSINESS CONTINUITY MANAGEMENT · PLANS AND PROCEDURES

Crisis Management and Communication Plans

QUESTION ASKED

Crisis management plans define how the organization makes decisions, communicates with stakeholders, and manages organizational response during a significant disruption.

District 101 Response - 2

RISK & IMPACT

District 101's crisis management and communication plans are inadequate, which may lead to ineffective response to crises and reputational damage.

Affected: Crisis management systems, communication platforms

RECOMMENDATION

Establish clear crisis management and communication plans that include roles, responsibilities, and procedures for responding to crises.

HIGH · EFFORT TO FIX: MEDIUM

BUSINESS CONTINUITY MANAGEMENT · PLANS AND PROCEDURES

Operational Recovery Procedures

QUESTION ASKED

Detailed procedures for the manual workarounds, interim processes, and temporary measures needed to maintain essential operations during a disruption are documented and accessible.

District 101 Response - 2

RISK & IMPACT

District 101's operational recovery procedures are incomplete, which may lead to ineffective recovery of critical operations.

Affected: Business process management systems, operational recovery databases

RECOMMENDATION

Develop comprehensive operational recovery procedures that include steps for recovering critical operations and restoring normal business functions.

HIGH · EFFORT TO FIX: MEDIUM

BUSINESS CONTINUITY MANAGEMENT · EXERCISES AND IMPROVEMENT

BCM Programme Review and Continuous Improvement

QUESTION ASKED

The BCM programme is formally reviewed at least annually — using exercise findings, incident learnings, and changing organizational context to continuously improve BCM capability.

District 101 Response - 2

RISK & IMPACT

District 101's BCM programme review and continuous improvement process is inadequate, which may lead to stagnation of the organization's continuity capabilities.

Affected: BCM programme management systems, continuous improvement databases

RECOMMENDATION

Establish a regular review and continuous improvement process for the BCM programme that includes identification of areas for improvement and implementation of changes.

HIGH · EFFORT TO FIX: MEDIUM

SECURE SDLC AND APPLICATION SECURITY · GOVERNANCE & SECURITY REQUIREMENTS

Application Risk Classification

QUESTION ASKED

Applications are classified by security risk level based on data sensitivity, user base, exposure, and business criticality — with security controls, testing requirements, and review depth calibrated accordingly.

District 101 Response - 2

RISK & IMPACT

District 101's application risk classification process is inadequate, leading to potential misclassification of high-risk applications. This gap may result in insufficient security controls being applied, increasing the likelihood of a security breach.

Affected: All web-based applications handling sensitive data

RECOMMENDATION

Develop and implement a comprehensive application risk classification framework that considers factors such as data sensitivity, user base, and system criticality.

HIGH · EFFORT TO FIX: MEDIUM

IT POLICY LIBRARY REVIEW · GOVERNANCE & PROGRAM POLICIES

Information Security Program Charter

QUESTION ASKED

A charter formally establishing the information security program, designating the CISO or security lead, and defining the authority, responsibilities, and resources of the security function.

District 101 Response - 2

RISK & IMPACT

The Information Security Program Charter is not well-defined, which may lead to confusion about roles and responsibilities. A clear charter is necessary for effective information security governance.

Affected: All systems and data

RECOMMENDATION

Review and update the Information Security Program Charter to align with industry standards and best practices.

HIGH · EFFORT TO FIX: MEDIUM

IT POLICY LIBRARY REVIEW · ACCESS CONTROL & IDENTITY POLICIES

Access Control Policy

QUESTION ASKED

A policy establishing principles of least privilege, need-to-know, and role-based access control governing logical access to all systems and data.

District 101 Response - 2

RISK & IMPACT

The Access Control Policy is not comprehensive, which may lead to unauthorized access to sensitive systems and data. A clear policy is necessary for ensuring secure access controls.

Affected: All systems and data

RECOMMENDATION

Develop an Access Control Policy that outlines procedures for granting, revoking, and monitoring access to sensitive systems and data.

HIGH · EFFORT TO FIX: MEDIUM

IT POLICY LIBRARY REVIEW · ACCESS CONTROL & IDENTITY POLICIES

Remote Access Policy

QUESTION ASKED

A policy governing all forms of remote access to organizational systems including VPN, remote desktop, and cloud access, specifying security requirements and acceptable use.

District 101 Response - 2

RISK & IMPACT

The Remote Access Policy is not well-defined, which may lead to unauthorized remote access to sensitive systems and data. A clear policy is necessary for ensuring secure remote access.

Affected: All systems and data

RECOMMENDATION

Develop a Remote Access Policy that outlines procedures for granting, revoking, and monitoring remote access to sensitive systems and data.

HIGH · EFFORT TO FIX: MEDIUM

IT POLICY LIBRARY REVIEW · INCIDENT RESPONSE & PLAYBOOKS

Data Breach Response & Notification Playbook

QUESTION ASKED

A playbook providing step-by-step guidance for responding to a data breach involving personal information, including forensic preservation, regulatory notification timelines, and individual notification procedures.

District 101 Response - 2

RISK & IMPACT

The Data Breach Response & Notification Playbook is not comprehensive, which may lead to delayed or inadequate response to data breaches. A clear playbook is necessary for ensuring timely and effective response.

Affected: All systems and data

RECOMMENDATION

Develop a Data Breach Response & Notification Playbook that outlines procedures for responding to and notifying stakeholders of data breaches.

HIGH · EFFORT TO FIX: MEDIUM

IT POLICY LIBRARY REVIEW · DATA MANAGEMENT & CLASSIFICATION POLICIES

Data Classification Policy

QUESTION ASKED

A policy defining data classification tiers (e.g., Public, Internal, Confidential, Restricted), handling requirements for each tier, and the process for classifying data assets.

District 101 Response - 2

RISK & IMPACT

The Data Classification Policy is not well-defined, which may lead to inadequate protection of sensitive data. A clear policy is necessary for ensuring proper classification and protection of sensitive data.

Affected: Systems containing sensitive data

RECOMMENDATION

Develop a Data Classification Policy that outlines procedures for classifying and protecting sensitive data.

HIGH · EFFORT TO FIX: MEDIUM

IT POLICY LIBRARY REVIEW · DATA MANAGEMENT & CLASSIFICATION POLICIES

Data Loss Prevention (DLP) Policy

QUESTION ASKED

A policy defining how the organization detects and prevents the unauthorized transmission, sharing, or exfiltration of sensitive data across all channels including email, web, cloud, and removable media.

District 101 Response - 2

RISK & IMPACT

Data Loss Prevention (DLP) Policy scored 2/5 (Partial / Developing). A policy defining how the organization detects and prevents the unauthorized transmission, sharing, or exfiltration of sensitive data across all channels including email, web, cloud, and removable media.

RECOMMENDATION

Scoring: 1=No DLP policy or controls; sensitive data can be transmitted or copied without detection. 2=Basic DLP awareness exists but no policy or technical controls are in place. 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. 4=DLP policy defines sensitive data types, prohibited transmission channels, alert and block thresholds, incident response for DLP alerts, and covers email, web, cloud upload, and removable media. 5=DLP controls are fully deployed across all channels, blocking is enforced for high-risk transfers, false positive review process is in place, and DLP effectiveness metrics are reported quarterly. Key elements to verify: Defined sensitive data types and identifiers (PII, PCI, PHI, source code, financial data); prohibited transmission channels; alert vs. block thresholds by data type; DLP alert triage and incident response process; removable media controls; cloud upload monitoring. Evidence: DLP policy, DLP rule set, coverage report, sample DLP alert triage records.

HIGH · EFFORT TO FIX: MEDIUM

IT POLICY LIBRARY REVIEW · NETWORK & INFRASTRUCTURE SECURITY POLICIES

Network Security Policy

QUESTION ASKED

A policy governing network architecture, segmentation, perimeter protection, traffic monitoring, and acceptable use of network resources.

District 101 Response - 2

RISK & IMPACT

Network Security Policy scored 2/5 (Partial / Developing). A policy governing network architecture, segmentation, perimeter protection, traffic monitoring, and acceptable use of network resources.

RECOMMENDATION

Scoring: 1=No network security policy; the network is flat with no segmentation and no formal access controls. 2=Basic firewall exists but no formal policy governs network architecture or traffic rules. 3=Network security policy exists but segmentation is incomplete, firewall rules are undocumented, or network monitoring is minimal. 4=Policy requires network segmentation, defines firewall rule review frequency, mandates network traffic monitoring, and restricts lateral movement. 5=Policy enforces micro-segmentation or zero trust network access, all firewall rules are documented and reviewed annually, east-west traffic monitoring is in place, and network baseline anomaly detection is operational. Key elements to verify: Network segmentation requirements (production, development, PCI, management, guest); firewall rule review frequency and process; prohibited protocols and services; DMZ requirements; network monitoring and logging requirements; wireless network security standards. Evidence: Network security policy, network architecture diagram, firewall rule set with review date, network monitoring configuration.

HIGH · EFFORT TO FIX: MEDIUM

IT POLICY LIBRARY REVIEW · NETWORK & INFRASTRUCTURE SECURITY POLICIES

Change Management Policy

QUESTION ASKED

A policy governing the process for requesting, reviewing, approving, implementing, and documenting changes to IT systems, infrastructure, and applications to minimize risk and maintain stability.

District 101 Response - 2

RISK & IMPACT

Change Management Policy scored 2/5 (Partial / Developing). A policy governing the process for requesting, reviewing, approving, implementing, and documenting changes to IT systems, infrastructure, and applications to minimize risk and maintain stability.

RECOMMENDATION

Scoring: 1=No change management policy; changes are made without review or documentation. 2=Informal change communication exists but no formal approval process, testing requirement, or rollback procedure. 3=Change management policy exists but emergency changes are not consistently documented or security impact analysis is not required. 4=Policy requires security impact analysis for all changes, defines change categories (standard, normal, emergency), requires testing in non-production, and mandates rollback plans. 5=Policy is enforced through a CMDB and ticketing system, all changes are documented with security review evidence, emergency changes are retrospectively reviewed within 24 hours, and change metrics are reported monthly. Key elements to verify: Change categories and approval thresholds; security impact analysis requirement; CAB (Change Advisory Board) composition and meeting cadence; test environment requirement; rollback procedure; emergency change process and retrospective review; documentation requirements. Evidence: Change management policy, sample change request records with security review, emergency change log.

HIGH · EFFORT TO FIX: MEDIUM

IT POLICY LIBRARY REVIEW · VENDOR & THIRD-PARTY RISK POLICIES

Vendor Risk Management Policy

QUESTION ASKED

A policy governing the process for assessing, onboarding, monitoring, and offboarding third-party vendors and service providers with access to organizational data or systems.

District 101 Response - 2

RISK & IMPACT

Vendor Risk Management Policy scored 2/5 (Partial / Developing). A policy governing the process for assessing, onboarding, monitoring, and offboarding third-party vendors and service providers with access to organizational data or systems.

RECOMMENDATION

Scoring: 1=No vendor risk management policy; vendors are onboarded without security review and have no contractual security obligations. 2=Some high-profile vendors are reviewed informally but no formal policy, tiering, or process exists. 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. 4=Policy defines vendor risk tiers based on data access and criticality, requires security questionnaire or assessment for Tier 1 and Tier 2 vendors, mandates contractual security requirements, and defines annual re-assessment for high-risk vendors. 5=Policy includes continuous monitoring through third-party risk ratings, all Tier 1 vendors have signed DPAs and NDA, offboarding procedures are enforced and documented, and vendor risk is reported quarterly to leadership. Key elements to verify: Vendor risk tiering methodology; security assessment requirements by tier; contractual security requirements (security addendum, DPA, right to audit); re-assessment frequency by tier; vendor offboarding procedure (access revocation, data return/destruction, credential deprovisioning); fourth-party risk awareness. Evidence: Vendor risk management policy, vendor inventory with risk tier, sample vendor assessment, most recent vendor re-assessment records.

HIGH · EFFORT TO FIX: MEDIUM

IT POLICY LIBRARY REVIEW · PHYSICAL & ENVIRONMENTAL SECURITY POLICIES

Physical Security Policy

QUESTION ASKED

A policy governing physical access controls, visitor management, security monitoring, and the protection of facilities, equipment, and sensitive areas containing IT infrastructure.

District 101 Response - 2

RISK & IMPACT

Physical Security Policy scored 2/5 (Partial / Developing). A policy governing physical access controls, visitor management, security monitoring, and the protection of facilities, equipment, and sensitive areas containing IT infrastructure.

RECOMMENDATION

Scoring: 1=No physical security policy; server rooms and network equipment are accessible to anyone. 2=Basic door locks exist but no formal policy governs access authorization, visitor management, or monitoring. 3=Physical security policy exists but access lists are not reviewed regularly, visitor logs are informal, or server rooms lack dedicated access controls. 4=Policy requires electronic access control for all sensitive areas, formal visitor management process, physical access list review at least quarterly, CCTV monitoring of server rooms, and secure disposal of sensitive documents. 5=Policy enforces multi-factor physical access (badge + PIN) for the most sensitive areas, CCTV is monitored and recorded with defined retention, access logs are reviewed weekly, and a physical security audit is conducted annually. Key elements to verify: Physical access authorization process; sensitive area definition (server rooms, data centers, network closets); visitor escort and log requirements; CCTV coverage and retention period; physical access list review frequency; secure document disposal; tailgating prevention measures. Evidence: Physical security policy, access control system logs, visitor log, CCTV configuration and retention settings, quarterly access review records.

HIGH · EFFORT TO FIX: MEDIUM

IT POLICY LIBRARY REVIEW · HUMAN RESOURCES & ACCEPTABLE USE POLICIES

Acceptable Use Policy (AUP)

QUESTION ASKED

A policy defining the acceptable and prohibited use of organizational IT resources including computers, networks, internet, email, cloud services, and mobile devices.

District 101 Response - 2

RISK & IMPACT

Acceptable Use Policy (AUP) scored 2/5 (Partial / Developing). A policy defining the acceptable and prohibited use of organizational IT resources including computers, networks, internet, email, cloud services, and mobile devices.

RECOMMENDATION

Scoring: 1=No acceptable use policy; employees are unaware of what is permitted or prohibited on corporate systems. 2=Basic AUP exists but is outdated, not signed by all employees, or does not address cloud services and personal use. 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. 4=AUP covers all IT resources including cloud and personal use, is signed at onboarding and annually re-acknowledged, explicitly informs employees of monitoring, and defines consequences for violations. 5=AUP is reviewed annually, includes social media, GenAI tool usage, and remote work provisions, is integrated into security awareness training, and acknowledgment is tracked with automated reminders. Key elements to verify: Covered resources (corporate systems, email, internet, cloud, mobile, personal use); prohibited activities (illegal activity, unauthorized software, data exfiltration); monitoring notification (employees have no expectation of privacy); social media guidance; GenAI tool usage guidelines; violation consequences; annual re-acknowledgment. Evidence: Acceptable use policy, signed acknowledgment records, annual re-acknowledgment tracking.

HIGH · EFFORT TO FIX: MEDIUM

IT POLICY LIBRARY REVIEW · HUMAN RESOURCES & ACCEPTABLE USE POLICIES

Personnel Security & Background Check Policy

QUESTION ASKED

A policy governing pre-employment screening, background checks, and ongoing personnel security requirements based on position risk designation and access to sensitive systems or data.

District 101 Response - 2

RISK & IMPACT

Personnel Security & Background Check Policy scored 2/5 (Partial / Developing). A policy governing pre-employment screening, background checks, and ongoing personnel security requirements based on position risk designation and access to sensitive systems or data.

RECOMMENDATION

Scoring: 1=No personnel security policy; employees are hired and granted access without background checks. 2=Background checks are conducted inconsistently or only for certain roles. 3=Personnel security policy exists but background check scope is minimal, contractors are not consistently screened, or rescreening is not conducted. 4=Policy defines background check requirements by position risk level, covers criminal, employment, education, and reference checks; contractors are screened to the same standard; and rescreening is conducted for employees in sensitive roles. 5=Policy includes social media screening for sensitive roles, international background check processes are defined, rescreening is conducted every 3 years for sensitive positions, and contractor screening compliance is verified before access is granted. Key elements to verify: Background check scope by position risk level; contractor and vendor personnel screening requirements; rescreening frequency for sensitive roles; social media screening for elevated risk positions; reference check requirements; criminal history and credit check requirements for financial roles. Evidence: Personnel security policy, position risk designation matrix, background check vendor agreement, sample background check completion records (redacted).

HIGH · EFFORT TO FIX: MEDIUM

IT POLICY LIBRARY REVIEW · COMPLIANCE & AUDIT POLICIES

Audit & Assessment Policy

QUESTION ASKED

A policy governing internal and external security assessments, audits, and penetration testing including frequency, scope, assessor qualifications, findings management, and reporting.

District 101 Response - 2

RISK & IMPACT

Audit & Assessment Policy scored 2/5 (Partial / Developing). A policy governing internal and external security assessments, audits, and penetration testing including frequency, scope, assessor qualifications, findings management, and reporting.

RECOMMENDATION

Scoring: 1=No audit or assessment policy; security assessments have never been conducted. 2=Occasional assessments are conducted reactively but no policy defines frequency, scope, or findings management. 3=Audit policy exists but findings are not tracked to remediation, assessors are not required to be independent, or penetration testing is not included. 4=Policy requires annual third-party security assessment or penetration test, defines scope and independence requirements, mandates POA&M for all findings, and requires findings to be reported to leadership. 5=Policy requires annual external penetration test plus quarterly vulnerability assessments, all findings are tracked in a risk register, closure is verified through retesting, and assessment results are reported to the board or audit committee. Key elements to verify: Assessment types required (vulnerability assessment, penetration test, security audit); frequency requirements; independence requirements for external assessors; scope definition; findings management process (POA&M or risk register); reporting hierarchy (leadership, board, audit committee); follow-up retest requirement. Evidence: Audit and assessment policy, most recent penetration test report, POA&M or findings tracking register, retesting confirmation.

HIGH · EFFORT TO FIX: MEDIUM — EDUCATION POLICY & COMPLIANCE REVIEW · GOVERNANCE & POLICY PROGRAM

Information Security & Privacy Policy Framework

QUESTION ASKED

The institution has an established, comprehensive set of information security and privacy policies that are reviewed annually, approved by leadership, and communicated to all staff.

District 101 Response - 2

RISK & IMPACT

District 101's Information Security & Privacy Policy Framework is not comprehensive or up-to-date, which could lead to security gaps.

Affected: All systems and data

RECOMMENDATION

Review and update the Information Security & Privacy Policy Framework to ensure it is comprehensive and up-to-date.

HIGH · EFFORT TO FIX: MEDIUM — EDUCATION POLICY & COMPLIANCE REVIEW · GOVERNANCE & POLICY PROGRAM

Security & Privacy Program Leadership

QUESTION ASKED

Designated leadership roles exist with authority and accountability for information security and student privacy compliance across the institution.

District 101 Response - 2

RISK & IMPACT

District 101 lacks a clear security and privacy program leadership structure, which could lead to confusion and inefficiencies.

Affected: Security team and stakeholders

RECOMMENDATION

Establish a clear security and privacy program leadership structure to ensure effective management of security initiatives.

HIGH · EFFORT TO FIX: MEDIUM — EDUCATION POLICY & COMPLIANCE REVIEW · GOVERNANCE & POLICY PROGRAM

Security & Privacy Awareness Training

QUESTION ASKED

All staff receive role-appropriate security and privacy training, including FERPA obligations, phishing awareness, and data handling responsibilities.

District 101 Response - 2

RISK & IMPACT

District 101's security awareness training program is not comprehensive or regular, which could lead to employee mistakes and security incidents.

Affected: Employee systems and data

RECOMMENDATION

Implement a security awareness training program to educate employees on security best practices.

HIGH · EFFORT TO FIX: MEDIUM EDUCATION POLICY & COMPLIANCE REVIEW · FERPA — STUDENT RECORDS PRIVACY

Annual FERPA Notification

QUESTION ASKED

The institution provides annual notification to eligible students (Higher Ed) or parents (K-12) of their FERPA rights, including the right to inspect records, amend records, and consent to disclosure.

District 101 Response - 2

RISK & IMPACT

District 101's annual FERPA notification is not comprehensive or timely, which could lead to non-compliance with federal regulations.

Affected: Student data and systems

RECOMMENDATION

Review and update the annual FERPA notification process to ensure it is comprehensive and timely.

HIGH · EFFORT TO FIX: MEDIUM EDUCATION POLICY & COMPLIANCE REVIEW · FERPA — STUDENT RECORDS PRIVACY

Legitimate Educational Interest & Access Controls

QUESTION ASKED

Access to student education records is limited to school officials with a legitimate educational interest, and access controls are enforced technically and procedurally.

District 101 Response - 2

RISK & IMPACT

District 101's legitimate educational interest and access controls are not well-established, which could lead to unauthorized access to student data.

Affected: Student data and systems

RECOMMENDATION

Establish clear legitimate educational interest and access controls to ensure only authorized personnel have access to student data.

HIGH · EFFORT TO FIX: MEDIUM EDUCATION POLICY & COMPLIANCE REVIEW · COPPA — CHILDREN'S ONLINE PRIVACY (K-12)

Parental Consent Mechanisms

QUESTION ASKED

[K-12] For applications subject to COPPA where the school operator acts on behalf of parents, the district has school consent agreements or has obtained verifiable parental consent.

District 101 Response - 2

RISK & IMPACT

District 101's parental consent mechanisms are not comprehensive or clear, which could lead to non-compliance with federal regulations.

Affected: Student data and systems

RECOMMENDATION

Review and update the parental consent mechanisms to ensure they are comprehensive and clear.

HIGH · EFFORT TO FIX: MEDIUM

EDUCATION POLICY & COMPLIANCE REVIEW · COPPA — CHILDREN'S ONLINE PRIVACY (K-12)

Data Minimization & Retention for Student Data

QUESTION ASKED

[K-12] The district enforces data minimization principles — collecting only necessary student data — and has defined retention and deletion schedules for student information collected through digital tools.

District 101 Response - 2

RISK & IMPACT

District 101's data minimization and retention practices for student data are not well-established, which could lead to unnecessary collection and storage of sensitive data.

Affected: Student data and systems

RECOMMENDATION

Establish clear data minimization and retention practices for student data to ensure only necessary data is collected and stored.

HIGH · EFFORT TO FIX: MEDIUM

EDUCATION POLICY & COMPLIANCE REVIEW · EDTECH & THIRD-PARTY APP GOVERNANCE

Technology Asset & Software Inventory

QUESTION ASKED

The institution maintains a current, complete inventory of all hardware, software, and cloud/SaaS applications, with data classification for systems that store student or sensitive data.

District 101 Response - 2

RISK & IMPACT

District 101's technology asset and software inventory is not comprehensive or up-to-date, which could lead to security gaps and inefficiencies.

Affected: All systems and data

RECOMMENDATION

Conduct a comprehensive technology asset and software inventory to ensure all systems and software are accounted for and secure.

HIGH · EFFORT TO FIX: MEDIUM

EDUCATION POLICY & COMPLIANCE REVIEW · STATE STUDENT PRIVACY LAWS

Student Data Transparency & Public Reporting

QUESTION ASKED

Where required by state law, the institution publishes a student data inventory, privacy notices, or annual reports on data collection and use practices.

District 101 Response - 2

RISK & IMPACT

District 101's student data transparency and public reporting practices are not well-established, which could lead to non-compliance with state regulations.

Affected: Student data and systems

RECOMMENDATION

Establish clear student data transparency and public reporting practices to ensure compliance with state regulations.

HIGH · EFFORT TO FIX: MEDIUM

VULNERABILITY MANAGEMENT DISCOVERY · SCANNING & DISCOVERY

Cloud and SaaS Vulnerability Coverage

QUESTION ASKED

Vulnerability management extends to cloud workloads, infrastructure-as-code, container images, and SaaS configurations — not just on-premises systems.

District 101 Response - 2

RISK & IMPACT

District 101's cloud and SaaS vulnerability coverage is incomplete, leaving potential risks undetected. This gap increases the risk of exploitation and potential security breaches in cloud-based systems.

Affected: Cloud-based systems and SaaS applications

RECOMMENDATION

Implement a comprehensive cloud and SaaS vulnerability scanning program to identify and address potential risks.

HIGH · EFFORT TO FIX: MEDIUM

VULNERABILITY MANAGEMENT DISCOVERY · REMEDIATION & PATCHING

End-of-Life System Management

QUESTION ASKED

Systems running end-of-life (EOL) operating systems or software are inventoried, isolated, and subject to compensating controls — or have a documented replacement plan.

District 101 Response - 2

RISK & IMPACT

District 101 lacks an end-of-life system management process, which can lead to outdated systems introducing vulnerabilities. This gap increases the risk of exploitation and potential security breaches.

Affected: Outdated systems

RECOMMENDATION

Develop a process for managing end-of-life systems, including timely upgrades or replacements.

HIGH · EFFORT TO FIX: MEDIUM

VULNERABILITY MANAGEMENT DISCOVERY · VISIBILITY & REPORTING

Attack Surface Inventory

QUESTION ASKED

The external attack surface — all internet-facing IP addresses, domains, exposed services, and cloud assets — is inventoried, monitored, and minimized.

District 101 Response - 2

RISK & IMPACT

District 101 lacks an attack surface inventory, making it difficult to maintain visibility into the organization's assets and potential vulnerabilities. This gap increases the risk of exploitation and potential security breaches.

Affected: All systems

RECOMMENDATION

Create an attack surface inventory to maintain visibility into the organization's assets and potential vulnerabilities.

HIGH · EFFORT TO FIX: MEDIUM

SECURITY AWARENESS & PHISHING DISCOVERY · TRAINING PROGRAM

Training Coverage and Completion

QUESTION ASKED

Security awareness training is required for all employees and contractors, with completion tracked and enforced — not optional or voluntary.

District 101 Response - 2

RISK & IMPACT

The current training coverage and completion rates are below baseline, indicating that not all employees are receiving necessary security awareness training.

Affected: Employee training records and HR systems

RECOMMENDATION

Develop a plan to increase training coverage and completion rates, including regular reminders and notifications for employees who have not completed training.

HIGH · EFFORT TO FIX: MEDIUM

SECURITY AWARENESS & PHISHING DISCOVERY · PHISHING SIMULATION

Phishing Simulation Program

QUESTION ASKED

Regular simulated phishing campaigns test employee ability to recognize and avoid phishing attacks — with results used to improve training and identify high-risk individuals.

District 101 Response - 2

RISK & IMPACT

The phishing simulation program is not comprehensive, lacking variety and realism in its templates and scenarios.

Affected: Phishing simulation software and employee email

RECOMMENDATION

Conduct a thorough review of the phishing simulation program to identify areas for improvement and expansion, including the development of new templates and scenarios.

HIGH · EFFORT TO FIX: MEDIUM

SECURITY AWARENESS & PHISHING DISCOVERY · REPORTING CULTURE

Report Triage and Response

QUESTION ASKED

Reported suspicious emails and incidents are triaged by security staff in a timely manner, with confirmed threats escalated and acted upon — and reporters kept informed.

District 101 Response - 2

RISK & IMPACT

The report triage and response process is inadequate, leading to delays in responding to and addressing reported security incidents.

Affected: Security incident reporting system and employee email

RECOMMENDATION

Develop a comprehensive incident response plan that includes clear procedures for triaging and responding to reported security incidents.

HIGH · EFFORT TO FIX: MEDIUM — SECURITY AWARENESS & PHISHING DISCOVERY · MEASUREMENT & IMPROVEMENT

Program Metrics and KPIs

QUESTION ASKED

The security awareness program tracks meaningful metrics — phishing click rates, training completion, report rates, and repeat offender rates — and uses them to drive decisions.

District 101 Response - 2

RISK & IMPACT

The current program metrics and KPIs are inadequate, making it difficult to measure the effectiveness of the security awareness program.

Affected: Security awareness program metrics and analytics tools

RECOMMENDATION

Develop and track key performance indicators (KPIs) for the security awareness program, including metrics on employee engagement and reporting.

HIGH · EFFORT TO FIX: MEDIUM — SECURITY AWARENESS & PHISHING DISCOVERY · MEASUREMENT & IMPROVEMENT

Leadership Engagement and Tone from the Top

QUESTION ASKED

Senior leadership visibly supports, participates in, and advocates for the security awareness program — including completing their own training and being included in phishing simulations.

District 101 Response - 2

RISK & IMPACT

Leadership engagement and tone from the top are lacking, with limited executive involvement in promoting security awareness.

Affected: Executive communications and employee email

RECOMMENDATION

Enhance leadership engagement and tone from the top by incorporating security awareness into regular executive communications and town hall meetings.

HIGH · EFFORT TO FIX: MEDIUM — ASSET & DATA INVENTORY DISCOVERY · SOFTWARE & SAAS MANAGEMENT

Software and Application Inventory

QUESTION ASKED

A comprehensive inventory of all software — installed applications, licensed software, open-source components, and internally developed applications — is maintained and kept current.

District 101 Response - 2

RISK & IMPACT

The district lacks a comprehensive software inventory, making it challenging to track and manage applications across the network. This gap increases the risk of unapproved or malicious software being installed, potentially compromising sensitive data.

Affected: All district systems, including endpoints, servers, and network devices

RECOMMENDATION

Conduct a thorough software inventory using automated tools and manual processes to identify all applications, including those installed on endpoints and servers

HIGH · EFFORT TO FIX: MEDIUM

ASSET & DATA INVENTORY DISCOVERY · SOFTWARE & SAAS MANAGEMENT

SaaS Application Governance

QUESTION ASKED

The organization knows which SaaS applications are in use — including those approved by IT and those procured by departments without central review (shadow IT) — and governs them appropriately.

District 101 Response - 2

RISK & IMPACT

The district lacks effective SaaS governance policies and procedures, leading to uncontrolled adoption of cloud-based applications. This gap increases the risk of sensitive data being exposed or compromised through insecure SaaS applications.

Affected: All district systems accessing SaaS applications

RECOMMENDATION

Establish clear SaaS governance policies and procedures, including guidelines for secure adoption, configuration, and management of cloud-based applications

HIGH · EFFORT TO FIX: MEDIUM

ASSET & DATA INVENTORY DISCOVERY · DATA ASSET MANAGEMENT

Data Classification Coverage

QUESTION ASKED

Sensitive data is classified at creation or discovery and handled according to its classification level — with classification enforced through labeling, access controls, and DLP.

District 101 Response - 2

RISK & IMPACT

The district's data classification coverage is incomplete, making it challenging to apply appropriate security controls to sensitive data. This gap increases the risk of sensitive data being exposed or compromised.

Affected: All district systems storing or processing sensitive data

RECOMMENDATION

Develop a comprehensive data classification framework to categorize sensitive data and apply corresponding security controls

HIGH · EFFORT TO FIX: MEDIUM

ASSET & DATA INVENTORY DISCOVERY · CLOUD ASSET VISIBILITY

Cloud Configuration Baseline

QUESTION ASKED

Cloud environments are configured against a documented security baseline — not left in default insecure configurations — with deviation from baseline detected and remediated.

District 101 Response - 2

RISK & IMPACT

The district lacks a cloud configuration baseline, making it challenging to monitor and enforce secure configurations for cloud resources. This gap increases the risk of insecure cloud configurations being exploited by attackers.

Affected: All district cloud resources, including AWS, Azure, and Google Cloud

RECOMMENDATION

Implement a cloud configuration baseline using automated tools and manual processes to monitor and enforce secure configurations for all cloud resources

HIGH · EFFORT TO FIX: MEDIUM

INCIDENT RESPONSE READINESS DISCOVERY · IR PLAN & POLICY

Incident Response Plan Existence and Quality

QUESTION ASKED

A written, current, organization-specific Incident Response Plan (IRP) exists, is accessible to key personnel, and covers the most likely incident scenarios.

District 101 Response - 2

RISK & IMPACT

The Incident Response Plan lacks quality and completeness, increasing the risk of ineffective incident response and prolonged recovery.

Affected: All systems and data

RECOMMENDATION

Review and update the Incident Response Plan to address gaps in content, ensuring it is comprehensive, accessible, and regularly reviewed.

HIGH · EFFORT TO FIX: MEDIUM

INCIDENT RESPONSE READINESS DISCOVERY · TEAM & CONTACTS

Incident Response Team Structure and Roles

QUESTION ASKED

An Incident Response Team (IRT) is defined with clear roles, responsibilities, and backups — covering technical response, legal, communications, leadership, and external coordination.

District 101 Response - 2

RISK & IMPACT

The Incident Response Team Structure lacks clear roles and responsibilities, hindering effective incident response and increasing the risk of confusion and miscommunication.

Affected: Incident Response Team

RECOMMENDATION

Define clear roles and responsibilities within the Incident Response Team Structure, ensuring each member understands their duties and expectations.

HIGH · EFFORT TO FIX: MEDIUM

INCIDENT RESPONSE READINESS DISCOVERY · NOTIFICATION & COMMUNICATION

Regulatory Breach Notification Obligations

QUESTION ASKED

All regulatory breach notification obligations are documented — including which regulation applies, what triggers notification, the timeline, required content, and who is the notifying authority.

District 101 Response - 2

RISK & IMPACT

Regulatory Breach Notification Obligations are not fully addressed, increasing the risk of non-compliance and reputational damage.

Affected: Customer data, regulatory compliance

RECOMMENDATION

Review and update incident response plans to ensure compliance with relevant breach notification regulations, incorporating clear procedures for notification and disclosure.

HIGH · EFFORT TO FIX: MEDIUM

CLOUD SECURITY POSTURE DISCOVERY · IDENTITY & ACCESS IN CLOUD

Cloud Admin Account Security

QUESTION ASKED

Cloud global and privileged administrator accounts are protected with phishing-resistant MFA, minimized in number, and not used for day-to-day tasks.

District 101 Response - 2

RISK & IMPACT

Cloud Admin Account Security is not fully implemented, leaving administrative accounts vulnerable to unauthorized access.

Affected: All cloud-based systems and applications

RECOMMENDATION

Implement strong password policies, multi-factor authentication (MFA), and least privilege access for all administrative accounts.

HIGH · EFFORT TO FIX: MEDIUM

CLOUD SECURITY POSTURE DISCOVERY · IDENTITY & ACCESS IN CLOUD

Guest and External User Access

QUESTION ASKED

Guest accounts and external collaborators in cloud platforms are inventoried, limited in access, and reviewed regularly — a commonly neglected vector for data exposure.

District 101 Response - 2

RISK & IMPACT

Guest and External User Access is not properly configured, allowing unauthorized access to sensitive data.

Affected: All cloud-based systems and applications

RECOMMENDATION

Configure guest and external user access controls to restrict access to sensitive data and implement least privilege access for all users.

HIGH · EFFORT TO FIX: MEDIUM

CLOUD SECURITY POSTURE DISCOVERY · CONFIGURATION & HARDENING

Cloud Storage and Sharing Controls

QUESTION ASKED

Cloud storage (SharePoint, OneDrive, Google Drive, S3 buckets) is configured to prevent unintended public or external sharing of sensitive data — a common source of data exposure incidents.

District 101 Response - 2

RISK & IMPACT

Cloud Storage and Sharing Controls are not properly configured, allowing unauthorized access to sensitive data.

Affected: All cloud-based storage systems

RECOMMENDATION

Configure cloud storage and sharing controls to restrict access to sensitive data and implement least privilege access for all users.

HIGH · EFFORT TO FIX: MEDIUM

CLOUD SECURITY POSTURE DISCOVERY · DATA PROTECTION IN CLOUD

Email Security in Cloud

QUESTION ASKED

Cloud-hosted email (M365 Exchange Online, Google Workspace Gmail) is configured with anti-phishing, anti-spoofing, and data loss prevention controls beyond default settings.

District 101 Response - 2

RISK & IMPACT

Email Security in Cloud is not fully implemented, leaving email communications vulnerable to spam, phishing, and other threats.

Affected: All cloud-based email systems

RECOMMENDATION

Implement additional security measures such as encryption, spam filtering, and malware protection for all cloud-based email systems.

HIGH · EFFORT TO FIX: MEDIUM

CLOUD SECURITY POSTURE DISCOVERY · MONITORING & LOGGING

Cloud Threat Detection and Alerting

QUESTION ASKED

Cloud platforms are monitored for security threats — including anomalous sign-ins, admin privilege changes, suspicious data access, and known attack patterns — with alerts reviewed and acted upon.

District 101 Response - 2

RISK & IMPACT

Cloud Threat Detection and Alerting is not implemented, leaving the organization vulnerable to potential security threats.

Affected: All cloud-based systems and applications

RECOMMENDATION

Implement a cloud threat detection and alerting system to identify potential security threats and provide real-time alerts for incident response.

HIGH · EFFORT TO FIX: MEDIUM

CLOUD SECURITY POSTURE DISCOVERY · MONITORING & LOGGING

Cloud Security Posture Reporting

QUESTION ASKED

Cloud security posture is measured, trended, and reported to leadership on a defined schedule — providing visibility into configuration compliance, threats, and improvement over time.

District 101 Response - 2

RISK & IMPACT

Cloud Security Posture Reporting is not fully implemented, leaving the organization without visibility into security risks.

Affected: All cloud-based systems and applications

RECOMMENDATION

Develop a comprehensive cloud security posture reporting framework to provide visibility into security risks and identify areas for improvement.

HIGH · EFFORT TO FIX: MEDIUM

BACKUP & DISASTER RECOVERY DISCOVERY · RECOVERY TESTING

Ransomware Recovery Testing

QUESTION ASKED

Recovery from a ransomware scenario — including recovery from clean, pre-infection backups with production systems isolated — is specifically tested, not just theorized about.

District 101 Response - 2

RISK & IMPACT

Ransomware Recovery Testing is inadequate, with no regular testing performed to ensure that backups can be successfully restored in case of a ransomware attack.

Affected: All systems with sensitive data

RECOMMENDATION

Implement regular ransomware-specific recovery testing, including simulation exercises and restore tests, to ensure that District 101's backups are protected against this growing threat.

HIGH · EFFORT TO FIX: MEDIUM

VENDOR & THIRD-PARTY RISK DISCOVERY · VENDOR INVENTORY

Vendor Risk Classification

QUESTION ASKED

Vendors are classified by risk tier based on the sensitivity of data they access and the criticality of services they provide — so higher-risk vendors receive proportionately more scrutiny.

District 101 Response - 2

RISK & IMPACT

Incomplete Vendor Risk Classification hinders accurate risk assessments and prioritization of vendor risks.

Affected: All systems and data handled by third-party vendors

RECOMMENDATION

Conduct a thorough review of Vendor Risk Classification to ensure accurate risk assessments, categorize vendors based on risk levels, and prioritize risk mitigation efforts accordingly.

HIGH · EFFORT TO FIX: MEDIUM

VENDOR & THIRD-PARTY RISK DISCOVERY · CONTRACT CONTROLS

Security and Privacy Contract Requirements

QUESTION ASKED

All contracts with vendors that access sensitive data include specific, enforceable security and privacy requirements — not just a generic "shall comply with applicable laws" clause.

District 101 Response - 2

RISK & IMPACT

Inadequate Security and Privacy Contract Requirements expose District 101 to potential security breaches and non-compliance with regulations.

Affected: All systems and data handled by third-party vendors

RECOMMENDATION

Establish clear Security and Privacy Contract Requirements for all vendors, including specific security controls, incident response procedures, and data protection requirements.

HIGH · EFFORT TO FIX: MEDIUM

VENDOR & THIRD-PARTY RISK DISCOVERY · MONITORING & OFFBOARDING

Supply Chain Risk Program Governance

QUESTION ASKED

Vendor risk management is governed as a formal program — with executive ownership, defined policies, regular reporting, and continuous improvement — not managed ad hoc by individual teams.

District 101 Response - 2

RISK & IMPACT

Lack of Supply Chain Risk Program Governance hinders effective oversight and management of vendor risk activities.

Affected: All systems and data handled by third-party vendors

RECOMMENDATION

Develop a Supply Chain Risk Program Governance framework to oversee vendor risk management activities, including risk assessments, mitigation efforts, and continuous monitoring.

HIGH · EFFORT TO FIX: MEDIUM

PHYSICAL SECURITY DISCOVERY · MEDIA & DOCUMENT SECURITY

Print and Fax Security

QUESTION ASKED

Printers, copiers, fax machines, and multifunction devices are secured to prevent unauthorized retrieval of printed documents and access to cached document data.

District 101 Response - 2

RISK & IMPACT

Inadequate print and fax security controls increase the risk of sensitive information being compromised through unauthorized access or interception.

Affected: Sensitive information transmitted via print or fax

RECOMMENDATION

Implement secure print and fax procedures that include features such as encryption, secure disposal, and access controls.

HIGH · EFFORT TO FIX: MEDIUM

AI & EMERGING TECHNOLOGY RISK DISCOVERY · AI GOVERNANCE & POLICY

AI Use Case Inventory and Risk Assessment

QUESTION ASKED

AI tools and use cases deployed within the organization are inventoried, with their data inputs, outputs, and risk profiles assessed before deployment.

District 101 Response - 2

RISK & IMPACT

The lack of a comprehensive AI Use Case Inventory and Risk Assessment hinders the organization's ability to identify potential security risks associated with AI usage.

Affected: All systems and data utilizing AI tools

RECOMMENDATION

Develop and maintain a comprehensive AI Use Case Inventory and conduct regular risk assessments to identify potential security risks.

HIGH · EFFORT TO FIX: MEDIUM

AI & EMERGING TECHNOLOGY RISK DISCOVERY · AI VENDOR RISK

AI Vendor and Tool Due Diligence

QUESTION ASKED

AI-powered tools and services procured from vendors are assessed for security, privacy, and data handling practices before adoption — including how training data is used and what happens to organizational data submitted to the AI.

District 101 Response - 2

RISK & IMPACT

The lack of adequate AI Vendor and Tool Due Diligence increases the risk of security breaches or reputational damage, as the organization may not be able to identify potential security risks associated with AI vendors and tools.

Affected: All systems and data utilizing AI tools

RECOMMENDATION

Develop and implement a comprehensive AI Vendor and Tool Due Diligence framework that includes regular risk assessments and monitoring of AI vendors and tools.

HIGH · EFFORT TO FIX: MEDIUM

AI & EMERGING TECHNOLOGY RISK DISCOVERY · AI VENDOR RISK

AI in Security Tools

QUESTION ASKED

AI-powered security tools (SIEM, EDR, email security, fraud detection) are configured, tuned, and reviewed to ensure they provide genuine risk reduction rather than alert noise without action.

District 101 Response - 2

RISK & IMPACT

The lack of adequate AI in Security Tools management increases the risk of security breaches or reputational damage, as the organization may not be able to identify potential security risks associated with AI usage in security tools.

Affected: All systems utilizing AI in security tools

RECOMMENDATION

Develop and implement a comprehensive AI in Security Tools management framework that includes regular testing, validation, and monitoring of AI models and outputs.

HIGH · EFFORT TO FIX: MEDIUM

AI & EMERGING TECHNOLOGY RISK DISCOVERY · AI-ENABLED THREATS

Deepfake and Synthetic Media Risk

QUESTION ASKED

The organization has considered and addressed the risk of deepfake audio, video, and synthetic identity attacks — particularly for executive impersonation, fraud, and credential theft scenarios.

District 101 Response - 2

RISK & IMPACT

Deepfake and Synthetic Media Risk poses a significant risk to the organization, as it may lead to reputational damage or security breaches.

Affected: All systems and data accessible via media

RECOMMENDATION

Develop and implement a comprehensive Deepfake and Synthetic Media Risk management framework that includes regular monitoring and detection mechanisms.

MEDIUM · EFFORT TO FIX: LOW — IDENTITY & ACCESS MANAGEMENT DISCOVERY · AUTHENTICATION & MFA

Legacy Authentication and Protocol Blocking

QUESTION ASKED

Legacy authentication protocols that do not support MFA — such as basic authentication, NTLM, POP3, IMAP, and SMTP AUTH — are blocked, preventing attackers from bypassing MFA by downgrading authentication.

District 101 Response - 3

RISK & IMPACT

Legacy authentication protocols pose a significant risk to District 101, as they can be exploited by attackers to gain unauthorized access. This gap can lead to data breaches and compliance issues.

Affected: All systems and applications with legacy authentication protocols

RECOMMENDATION

Conduct regular reviews of legacy authentication protocols to identify opportunities for blocking or disabling. Consider implementing modern authentication protocols, such as OAuth and OpenID Connect.

MEDIUM · EFFORT TO FIX: LOW — IDENTITY & ACCESS MANAGEMENT DISCOVERY · PRIVILEGED ACCESS

Privileged Account Inventory and Separation

QUESTION ASKED

All privileged accounts — domain admins, local admins, service accounts, cloud admins, and application admins — are inventoried and separated from standard user accounts.

District 101 Response - 3

RISK & IMPACT

Inadequate privileged account inventory and separation pose a significant risk to District 101, as these accounts often have elevated privileges and can be used by attackers to move laterally within the network. This gap can lead to unauthorized access, data breaches, and compliance issues.

Affected: All systems and applications with privileged accounts

RECOMMENDATION

Develop and implement a comprehensive privileged access management program that includes privileged account inventory and separation. Ensure that all privileged accounts are properly inventoried, monitored, and controlled.

MEDIUM · EFFORT TO FIX: LOW — IDENTITY & ACCESS MANAGEMENT DISCOVERY · ACCESS GOVERNANCE

Single Sign-On Coverage

QUESTION ASKED

Single Sign-On (SSO) is deployed for all major applications — reducing password sprawl, enforcing centralized MFA, and providing complete visibility into application access.

District 101 Response - 3

RISK & IMPACT

Insufficient single sign-on coverage leaves District 101 vulnerable to password fatigue and phishing attacks. This gap can lead to unauthorized access, data breaches, and compliance issues.

Affected: All critical systems and applications

RECOMMENDATION

Implement single sign-on coverage for all critical systems and applications. Consider implementing a cloud-based identity and access management solution to simplify user authentication and authorization.

MEDIUM · EFFORT TO FIX: LOW

MOBILE & ENDPOINT SECURITY DISCOVERY · BYOD POLICY & CONTROLS

BYOD Security Controls

QUESTION ASKED

Personal devices used to access organizational resources meet minimum security standards — enforced through conditional access, MAM, or equivalent — without requiring full MDM management of the personal device.

District 101 Response - 3

RISK & IMPACT

Although the BYOD security controls are relatively strong, scoring 3/5, there is still room for improvement. This gap allows potential security risks and data breaches.

Affected: All personal devices used for work purposes.

RECOMMENDATION

Continuously monitor and refine BYOD security controls, ensuring alignment with organizational security objectives and industry best practices.

MEDIUM · EFFORT TO FIX: LOW

DATA PRIVACY BASELINE DISCOVERY · REGULATORY AWARENESS

Privacy Regulatory Inventory

QUESTION ASKED

The organization has identified all privacy laws and regulations that apply to its operations — including federal, state, and international requirements — and understands what each requires.

District 101 Response - 3

RISK & IMPACT

District 101's Privacy Regulatory Inventory is incomplete, which may result in non-compliance with relevant regulations.

Affected: All systems handling personal data

RECOMMENDATION

Conduct a thorough review of applicable privacy regulations and update the inventory to ensure comprehensive coverage.

MEDIUM · EFFORT TO FIX: LOW

DATA PRIVACY BASELINE DISCOVERY · PRIVACY NOTICES & CONSENT

Children's Data Protection

QUESTION ASKED

If the organization processes data from or about children, enhanced protections are applied — including age verification, parental consent where required, and data minimization.

District 101 Response - 3

RISK & IMPACT

District 101's Children's Data Protection measures are insufficient, potentially putting sensitive data at risk.

Affected: Systems handling children's personal data

RECOMMENDATION

Implement additional controls to protect children's data, such as age verification mechanisms and restricted access protocols.

MEDIUM · EFFORT TO FIX: LOW

DATA PRIVACY BASELINE DISCOVERY · INDIVIDUAL RIGHTS

Data Subject Access Request Fulfillment

QUESTION ASKED

When individuals request access to their personal data, the organization can actually locate, compile, and provide their data in a usable format — which requires knowing where data lives.

District 101 Response - 3

RISK & IMPACT

District 101's Data Subject Access Request Fulfillment process is not fully effective, which may lead to delays or incomplete responses.

Affected: Systems storing personal data

RECOMMENDATION

Streamline the request fulfillment process through automation and employee training, ensuring timely and accurate responses.

MEDIUM · EFFORT TO FIX: LOW

DATA PRIVACY BASELINE DISCOVERY · DATA HANDLING & BREACH

Sensitive Data Handling and Minimization

QUESTION ASKED

The organization processes only the personal data necessary for defined purposes — and applies enhanced protections to special categories of sensitive data such as health, biometric, financial, and children's information.

District 101 Response - 3

RISK & IMPACT

District 101's Sensitive Data Handling and Minimization practices are inadequate, potentially exposing sensitive data to unauthorized access.

Affected: Systems storing sensitive personal data

RECOMMENDATION

Implement enhanced data handling procedures, including encryption, access controls, and regular data minimization reviews.

MEDIUM · EFFORT TO FIX: LOW

DATA PRIVACY BASELINE DISCOVERY · DATA HANDLING & BREACH

Data Breach Detection and Notification Readiness

QUESTION ASKED

The organization can detect personal data breaches, assess their scope and risk to individuals, and notify the appropriate regulators and affected individuals within legally required timeframes.

District 101 Response - 3

RISK & IMPACT

District 101's Data Breach Detection and Notification Readiness is insufficient, which may lead to delayed or inadequate responses in the event of a breach.

Affected: All systems handling personal data

RECOMMENDATION

Develop an incident response plan that includes breach detection protocols, notification procedures, and employee training.

MEDIUM · EFFORT TO FIX: LOW

ZERO TRUST MATURITY ASSESSMENT · IDENTITY

Identity as the Control Plane

QUESTION ASKED

The organization has adopted identity — not network location — as the primary means of granting access, with authentication and authorization decisions made per-request rather than per-session.

District 101 Response - 3

RISK & IMPACT

District 101's identity as the control plane is not fully implemented, leaving some identities without proper governance and oversight. This gap increases the risk of unauthorized access and malicious activity.

Affected: All systems and applications with identity-based access controls

RECOMMENDATION

Implement a more comprehensive identity governance strategy, utilizing techniques such as identity lifecycle management, role-based access control (RBAC), and attribute-based access control (ABAC).

MEDIUM · EFFORT TO FIX: LOW

ZERO TRUST MATURITY ASSESSMENT · IDENTITY

Non-Human Identity Governance

QUESTION ASKED

Service accounts, application identities, API keys, certificates, and other non-human identities are governed with the same rigor as human identities — inventoried, least-privileged, and continuously monitored.

District 101 Response - 3

RISK & IMPACT

District 101's non-human identity governance is inadequate, leaving some service accounts and machine identities without proper management and oversight. This gap increases the risk of unauthorized access and malicious activity.

Affected: All systems and applications with non-human identities

RECOMMENDATION

Develop and enforce robust non-human identity governance policies, utilizing techniques such as service account management, machine identity management, and privileged access management (PAM).

MEDIUM · EFFORT TO FIX: LOW

ZERO TRUST MATURITY ASSESSMENT · NETWORKS

Encrypted Traffic and Protocol Controls

QUESTION ASKED

All network traffic — internal and external — is encrypted in transit, and unencrypted legacy protocols are eliminated or strictly controlled.

District 101 Response - 3

RISK & IMPACT

District 101's encrypted traffic and protocol controls are not fully implemented, leaving some network traffic vulnerable to interception and eavesdropping. This gap increases the risk of data breaches and reputational damage.

Affected: All network-connected systems and devices

RECOMMENDATION

Implement a comprehensive encryption strategy, utilizing techniques such as TLS, IPsec, and SSH to protect sensitive network traffic.

MEDIUM · EFFORT TO FIX: LOW

ZERO TRUST MATURITY ASSESSMENT · DATA

Data Visibility and Classification

QUESTION ASKED

The organization has comprehensive visibility into its data estate — knowing where data lives, how sensitive it is, and who accesses it — as the foundation for zero-trust data controls.

District 101 Response - 3

RISK & IMPACT

District 101's data visibility and classification controls are inadequate, leaving some sensitive information without proper labeling and handling. This gap increases the risk of unauthorized access and malicious activity.

Affected: All systems and devices storing or processing sensitive data

RECOMMENDATION

Develop and enforce robust data classification policies, utilizing techniques such as data discovery, data labeling, and data handling procedures to ensure sensitive information is properly protected.

MEDIUM · EFFORT TO FIX: LOW

THIRD-PARTY RISK MANAGEMENT PROGRAM · PROGRAM GOVERNANCE

TPRM Program Governance and Reporting

QUESTION ASKED

TPRM is governed as an organizational program with cross-functional oversight, regular reporting to leadership, and integration with enterprise risk management.

District 101 Response - 3

RISK & IMPACT

While the TPRM program has a clear governance structure, there is room for improvement in terms of reporting and metrics

Affected: All systems and data managed by third-party vendors

RECOMMENDATION

Develop and implement a comprehensive reporting framework to track key performance indicators (KPIs) and provide regular updates to stakeholders

MEDIUM · EFFORT TO FIX: LOW

THIRD-PARTY RISK MANAGEMENT PROGRAM · VENDOR INVENTORY

Vendor Inventory Completeness and Currency

QUESTION ASKED

The organization maintains a comprehensive, current inventory of all third-party relationships — covering all vendors with data access, system access, or physical access — updated continuously.

District 101 Response - 3

RISK & IMPACT

While the vendor inventory is generally complete and up-to-date, there are some gaps in terms of vendor risk tiering and classification

Affected: Systems and data managed by third-party vendors

RECOMMENDATION

Review and update the vendor inventory to ensure that all vendors are accurately risk-tiered and classified, including implementation of a clear methodology for assessing vendor criticality and concentration risk

MEDIUM · EFFORT TO FIX: LOW

THIRD-PARTY RISK MANAGEMENT PROGRAM · VENDOR INVENTORY

Vendor Contact and Relationship Management

QUESTION ASKED

Vendor relationships have designated owners, documented business contacts, and security contacts — enabling effective communication during normal operations and rapid escalation during incidents.

District 101 Response - 3

RISK & IMPACT

While the program has a good understanding of vendor contact and relationship management, there is room for improvement in terms of contract requirements and vendor access controls

Affected: Systems and data managed by third-party vendors with access to sensitive information

RECOMMENDATION

Review and update contract templates to include clear requirements for vendor access controls, including authentication, authorization, and accounting (AAA) protocols

MEDIUM · EFFORT TO FIX: LOW

THIRD-PARTY RISK MANAGEMENT PROGRAM · DUE DILIGENCE

Vendor Security Assessment Methodology

QUESTION ASKED

The organization uses a consistent, documented methodology for vendor security assessments — covering the right domains, using appropriate evidence, and producing comparable results across vendors.

District 101 Response - 3

RISK & IMPACT

While the program has a clear methodology for assessing vendor security risks, there is room for improvement in terms of pre-onboarding security assessments

Affected: Systems and data managed by new vendors

RECOMMENDATION

Implement a process for conducting pre-onboarding security assessments, including reviewing vendor security questionnaires and conducting site visits as needed

MEDIUM · EFFORT TO FIX: LOW

THIRD-PARTY RISK MANAGEMENT PROGRAM · DUE DILIGENCE

Assessment Finding Management

QUESTION ASKED

Security findings identified in vendor assessments are communicated to vendors, tracked to remediation, and risk-accepted when remediation is not possible — with escalation for unacceptable residual risk.

District 101 Response - 3

RISK & IMPACT

While the program has a good understanding of assessment finding management, there is room for improvement in terms of tracking vendor remediation efforts

Affected: Systems and data managed by third-party vendors with identified security risks

RECOMMENDATION

Implement a process for tracking vendor remediation efforts, including regular reporting and verification of remediation activities

MEDIUM · EFFORT TO FIX: LOW

THIRD-PARTY RISK MANAGEMENT PROGRAM · CONTRACT MANAGEMENT

Data Processing Agreements

QUESTION ASKED

Formal Data Processing Agreements (DPAs) or equivalent privacy agreements are in place with all vendors that process personal data — defining purpose, data types, retention, and obligations.

District 101 Response - 3

RISK & IMPACT

While the program has clear requirements for data processing agreements, there is room for improvement in terms of contract templates and vendor access controls

Affected: Systems and data managed by third-party vendors with access to sensitive information

RECOMMENDATION

Review and update contract templates to include clear requirements for vendor access controls, including authentication, authorization, and accounting (AAA) protocols

MEDIUM · EFFORT TO FIX: LOW

THIRD-PARTY RISK MANAGEMENT PROGRAM · CONTRACT MANAGEMENT

Incident Notification and Cooperation Requirements

QUESTION ASKED

Vendor contracts require timely notification of security incidents affecting the organization, cooperation with investigations, and participation in incident response — with enforceable timelines.

District 101 Response - 3

RISK & IMPACT

While the program has clear incident notification and cooperation requirements, there is room for improvement in terms of contract templates and vendor access controls

Affected: Systems and data managed by third-party vendors with access to sensitive information

RECOMMENDATION

Review and update contract templates to include clear requirements for vendor access controls, including authentication, authorization, and accounting (AAA) protocols

MEDIUM · EFFORT TO FIX: LOW

THIRD-PARTY RISK MANAGEMENT PROGRAM · ONGOING MONITORING

Continuous Security Posture Monitoring

QUESTION ASKED

The security posture of high-risk vendors is monitored continuously between formal assessments — providing early warning of deterioration that would require intervention before the next scheduled re-assessment.

District 101 Response - 3

RISK & IMPACT

While the program has a good understanding of continuous security posture monitoring, there is room for improvement in terms of tracking vendor performance and SLA adherence

Affected: Systems and data managed by third-party vendors with service level agreements (SLAs)

RECOMMENDATION

Implement a continuous monitoring program to track vendor performance and SLA adherence, including regular reporting and remediation as needed

MEDIUM · EFFORT TO FIX: LOW

THIRD-PARTY RISK MANAGEMENT PROGRAM · VENDOR LIFECYCLE

Vendor Onboarding Process

QUESTION ASKED

A formal, consistent vendor onboarding process ensures all security requirements are met before vendors receive access — including assessment completion, contract execution, and access provisioning controls.

District 101 Response - 3

RISK & IMPACT

While the program has a clear vendor onboarding process, there is room for improvement in terms of contract requirements and vendor access controls

Affected: Systems and data managed by third-party vendors with access to sensitive information

RECOMMENDATION

Review and update contract templates to include clear requirements for vendor access controls, including authentication, authorization, and accounting (AAA) protocols

MEDIUM · EFFORT TO FIX: LOW

THIRD-PARTY RISK MANAGEMENT PROGRAM · VENDOR LIFECYCLE

Vendor Offboarding and Access Termination

QUESTION ASKED

When vendor relationships end, all access is promptly revoked, data is returned or deleted, and the termination is documented — closing the loop on the relationship completely.

District 101 Response - 3

RISK & IMPACT

While the program has a good understanding of vendor offboarding and access termination, there is room for improvement in terms of contract requirements and vendor access controls

Affected: Systems and data managed by third-party vendors with access to sensitive information

RECOMMENDATION

Review and update contract templates to include clear requirements for vendor access controls, including authentication, authorization, and accounting (AAA) protocols

MEDIUM · EFFORT TO FIX: LOW

BUSINESS CONTINUITY MANAGEMENT · BCM GOVERNANCE & POLICY

Executive Leadership and BCM Governance

QUESTION ASKED

Senior leadership actively supports and governs the BCM program — providing resources, making risk decisions, and ensuring BCM is integrated into organizational strategy.

District 101 Response - 3

RISK & IMPACT

District 101's executive leadership and BCM governance are not fully aligned, which may lead to inadequate support for continuity efforts.

Affected: Executive leadership systems, governance databases

RECOMMENDATION

Ensure that executive leadership is fully engaged in and supportive of the organization's continuity efforts, and that BCM governance is integrated into organizational decision-making processes.

MEDIUM · EFFORT TO FIX: LOW

BUSINESS CONTINUITY MANAGEMENT · BCM GOVERNANCE & POLICY

BCM Integration with Organizational Risk Management

QUESTION ASKED

BCM is integrated with enterprise risk management — with continuity risks in the risk register, BCM metrics in risk reporting, and BCM investment informed by organizational risk tolerance.

District 101 Response - 3

RISK & IMPACT

District 101's BCM integration with organizational risk management is not fully effective, which may lead to inadequate identification and mitigation of continuity risks.

Affected: Risk management systems, BCM programme databases

RECOMMENDATION

Enhance the integration of BCM into organizational risk management processes by ensuring that continuity risks are identified and mitigated through regular risk assessments and reviews.

MEDIUM · EFFORT TO FIX: LOW

BUSINESS CONTINUITY MANAGEMENT · BUSINESS IMPACT ANALYSIS

Dependency Mapping and Single Points of Failure

QUESTION ASKED

The dependencies of critical functions — people, technology, facilities, suppliers, and data — are mapped, and single points of failure are identified and managed.

District 101 Response - 3

RISK & IMPACT

District 101's dependency mapping and single points of failure identification process is not fully effective, which may lead to inadequate business impact analysis and ineffective recovery strategies.

Affected: Business process management systems, stakeholder engagement platforms

RECOMMENDATION

Enhance the dependency mapping and single points of failure identification process by engaging with stakeholders and conducting a thorough review of organizational processes.

MEDIUM · EFFORT TO FIX: LOW

BUSINESS CONTINUITY MANAGEMENT · BUSINESS IMPACT ANALYSIS

Financial Impact and Cost of Downtime

QUESTION ASKED

The financial and reputational impact of critical function disruptions is quantified — providing a basis for BCM investment decisions and demonstrating the value of BCM capability.

District 101 Response - 3

RISK & IMPACT

District 101's financial impact and cost of downtime analysis is not fully effective, which may lead to inadequate business impact analysis and ineffective recovery strategies.

Affected: Financial management systems, business process databases

RECOMMENDATION

Enhance the financial impact and cost of downtime analysis by engaging with stakeholders and conducting a thorough review of organizational processes and financial data.

MEDIUM · EFFORT TO FIX: LOW

BUSINESS CONTINUITY MANAGEMENT · RECOVERY STRATEGY

Workforce Continuity and Alternate Work Arrangements

QUESTION ASKED

Workforce continuity strategies address scenarios where normal work locations or working arrangements are unavailable — including remote work, split teams, cross-training, and key person succession.

District 101 Response - 3

RISK & IMPACT

District 101's workforce continuity and alternate work arrangements are not fully effective, which may lead to disruptions in critical operations.

Affected: Human resources systems, workforce management databases

RECOMMENDATION

Develop a comprehensive workforce continuity plan that includes identification of alternative work arrangements, training, and support for employees.

MEDIUM · EFFORT TO FIX: LOW

BUSINESS CONTINUITY MANAGEMENT · PLANS AND PROCEDURES

Business Continuity Plans

QUESTION ASKED

Documented Business Continuity Plans (BCPs) provide step-by-step procedures for maintaining and restoring critical functions during a disruption — accessible, actionable, and validated through exercises.

District 101 Response - 3

RISK & IMPACT

District 101's business continuity plans are not fully effective, which may lead to inadequate response to disruptions and reputational damage.

Affected: Business process management systems, continuity planning databases

RECOMMENDATION

Develop comprehensive business continuity plans that include roles, responsibilities, and procedures for responding to disruptions.

MEDIUM · EFFORT TO FIX: LOW

BUSINESS CONTINUITY MANAGEMENT · EXERCISES AND IMPROVEMENT

Exercise Programme

QUESTION ASKED

A formal BCM exercise programme tests BCM capabilities through progressively challenging exercises — from tabletop discussions through full operational simulations — on a defined schedule.

District 101 Response - 3

RISK & IMPACT

District 101's exercise programme is not fully effective, which may lead to inadequate testing of recovery strategies and ineffective response to crises.

Affected: Exercise management systems, crisis management databases

RECOMMENDATION

Develop a comprehensive exercise programme that includes regular exercises and reviews to test recovery strategies and identify areas for improvement.

MEDIUM · EFFORT TO FIX: LOW

BUSINESS CONTINUITY MANAGEMENT · EXERCISES AND IMPROVEMENT

BCM Awareness and Training

QUESTION ASKED

All personnel with BCM responsibilities are trained on their roles — and all staff have baseline awareness of BCM plans and their role in organizational continuity.

District 101 Response - 3

RISK & IMPACT

District 101's BCM awareness and training are not fully effective, which may lead to inadequate understanding of continuity risks and ineffective response to disruptions.

Affected: Training management systems, employee engagement platforms

RECOMMENDATION

Develop a comprehensive BCM awareness and training programme that includes regular training sessions and awareness campaigns to educate employees on continuity risks and response procedures.

MEDIUM · EFFORT TO FIX: LOW

SECURE SDLC AND APPLICATION SECURITY · GOVERNANCE & SECURITY REQUIREMENTS

Application Security Policy and Strategy

QUESTION ASKED

A formal application security policy defines expectations for secure software development, establishes accountability, and drives a consistent, risk-based approach to AppSec across all development teams.

District 101 Response - 3

RISK & IMPACT

While District 101 has an Application Security Policy and Strategy in place, it is not fully aligned with industry best practices. This gap may lead to inconsistent application of security controls across the organization.

Affected: All applications developed and maintained by District 101

RECOMMENDATION

Review and update the Application Security Policy and Strategy to ensure alignment with industry standards and best practices.

MEDIUM · EFFORT TO FIX: LOW

SECURE SDLC AND APPLICATION SECURITY · GOVERNANCE & SECURITY REQUIREMENTS

Security Requirements Definition

QUESTION ASKED

Security requirements are systematically identified for all applications — covering functional security requirements (authentication, authorization, encryption) and non-functional requirements (logging, error handling, resilience).

District 101 Response - 3

RISK & IMPACT

District 101's security requirements definition process is not fully integrated into the SDLC, leading to potential security gaps in application development. This gap may result in insufficient security controls being applied during development.

Affected: All applications developed and maintained by District 101

RECOMMENDATION

Establish clear security requirements definition processes that are integrated into the SDLC, ensuring security is considered throughout the development lifecycle.

MEDIUM · EFFORT TO FIX: LOW — SECURE SDLC AND APPLICATION SECURITY · GOVERNANCE & SECURITY REQUIREMENTS

Security Champion and Developer Training Programs

QUESTION ASKED

Developers receive security training calibrated to their role, and Security Champions in development teams serve as embedded security advocates who extend AppSec capacity without requiring a security expert on every team.

District 101 Response - 3

RISK & IMPACT

While District 101 has a Security Champion and Developer Training Programs in place, there may be opportunities to enhance these programs. This gap may lead to insufficient security awareness among developers.

Affected: All development teams

RECOMMENDATION

Review and enhance the Security Champion and Developer Training Programs to ensure they are comprehensive and effective in promoting secure development practices.

MEDIUM · EFFORT TO FIX: LOW — IT POLICY LIBRARY REVIEW · GOVERNANCE & PROGRAM POLICIES

Information Security Policy (Master)

QUESTION ASKED

A top-level organizational information security policy establishing executive commitment, scope, objectives, and high-level security requirements across the enterprise.

District 101 Response - 3

RISK & IMPACT

Information Security Policy (Master) scored 3/5 (Defined / Compensating control). A top-level organizational information security policy establishing executive commitment, scope, objectives, and high-level security requirements across the enterprise.

RECOMMENDATION

Scoring: 1=No master security policy exists. 2=Draft policy in progress. 3=Policy exists but has not been formally approved by executive leadership or reviewed in the past 2 years. 4=Policy approved by executive leadership, communicated to all staff, and reviewed within the past 2 years. 5=Policy approved, annually reviewed, version-controlled, and cascaded to all sub-policies and procedures with documented acknowledgment from leadership. Key elements to verify: Executive or board-level approval signature and date; defined scope covering all systems, users, and third parties; high-level security objectives aligned to business goals; reference to all subordinate policies; review schedule defined; version history maintained. Evidence: Signed master security policy document, approval date, distribution records, version history.

MEDIUM · EFFORT TO FIX: LOW — IT POLICY LIBRARY REVIEW · GOVERNANCE & PROGRAM POLICIES

Risk Management Policy

QUESTION ASKED

A policy establishing the organization's approach to identifying, assessing, treating, and monitoring information security and privacy risks across the enterprise.

District 101 Response - 3

RISK & IMPACT

Risk Management Policy scored 3/5 (Defined / Compensating control). A policy establishing the organization's approach to identifying, assessing, treating, and monitoring information security and privacy risks across the enterprise.

RECOMMENDATION

Scoring: 1=No formal risk management policy. 2=Informal risk conversations occur but no documented policy or process. 3=Risk management policy exists but risk assessments are not conducted on a defined schedule. 4=Policy defines risk tolerance, risk assessment frequency, treatment options, and risk acceptance authority; annual risk assessments are conducted. 5=Policy is fully implemented with documented risk register, risk acceptance records, and quarterly reporting to leadership; integrated into business decisions. Key elements to verify: Defined risk tolerance or risk appetite statement; risk assessment methodology and frequency; treatment options (accept, mitigate, transfer, avoid); risk acceptance authority and sign-off process; risk register maintained. Evidence: Risk management policy, most recent risk assessment report, risk register, risk acceptance records.

MEDIUM · EFFORT TO FIX: LOW

IT POLICY LIBRARY REVIEW · GOVERNANCE & PROGRAM POLICIES

Records Management & Legal Hold Policy

QUESTION ASKED

A policy defining how organizational records are created, classified, retained, protected, and disposed of in compliance with legal, regulatory, and business requirements.

District 101 Response - 3

RISK & IMPACT

Records Management & Legal Hold Policy scored 3/5 (Defined / Compensating control). A policy defining how organizational records are created, classified, retained, protected, and disposed of in compliance with legal, regulatory, and business requirements.

RECOMMENDATION

Scoring: 1=No records management policy; records are retained indefinitely or deleted without process. 2=Basic retention guidelines exist informally. 3=Records management policy exists with retention schedules but is not consistently applied or technically enforced. 4=Policy is approved, retention schedules are defined per record type, technical enforcement is in place, and legal hold procedures are documented. 5=Policy is fully enforced, legal holds are tracked in a system, retention compliance is audited annually, and disposal is documented with certificates of destruction. Key elements to verify: Retention schedule by record type with legal basis; legal hold notification and preservation procedure; disposal authorization and documentation; responsibility assignment; intersection with privacy regulations (GDPR, CCPA). Evidence: Records management policy, retention schedule, legal hold procedure, sample disposal records.

MEDIUM · EFFORT TO FIX: LOW

IT POLICY LIBRARY REVIEW · ACCESS CONTROL & IDENTITY POLICIES

Password & Authenticator Policy

QUESTION ASKED

A policy governing password complexity, length, lifecycle, multi-factor authentication requirements, and prohibited practices across all systems.

District 101 Response - 3

RISK & IMPACT

Password & Authenticator Policy scored 3/5 (Defined / Compensating control). A policy governing password complexity, length, lifecycle, multi-factor authentication requirements, and prohibited practices across all systems.

RECOMMENDATION

Scoring: 1=No password policy; default or weak passwords are in use. 2=Basic password requirements exist but are not technically enforced or are outdated. 3=Password policy exists with complexity and length requirements but MFA is not mandated or is only partially deployed. 4=Policy mandates MFA for privileged and remote access; passwords meet minimum length (12+ characters); breached password detection is in place. 5=Policy requires phishing-resistant MFA for all users; passwords meet NIST 800-63B standards; breached password detection is automated; policy is reviewed annually. Key elements to verify: Minimum password length and complexity; MFA requirements by role and access type; prohibition on password sharing and reuse; temporary password requirements; alignment to NIST SP 800-63B. Evidence: Password/authenticator policy, MFA coverage report, password configuration screenshots.

MEDIUM · EFFORT TO FIX: LOW

IT POLICY LIBRARY REVIEW · ACCESS CONTROL & IDENTITY POLICIES

Privileged Access Management Policy

QUESTION ASKED

A policy governing the identification, provisioning, use, monitoring, and periodic review of privileged (administrative) accounts across all systems.

District 101 Response - 3

RISK & IMPACT

Privileged Access Management Policy scored 3/5 (Defined / Compensating control). A policy governing the identification, provisioning, use, monitoring, and periodic review of privileged (administrative) accounts across all systems.

RECOMMENDATION

Scoring: 1=No PAM policy; administrative accounts are used for daily work and not tracked. 2=Privileged accounts are somewhat controlled but shared admin accounts exist and are not reviewed. 3=PAM policy exists; privileged accounts are inventoried and separate from standard accounts but monitoring is limited. 4=Policy requires separate privileged accounts, prohibits shared admin credentials, mandates MFA, and requires privileged session logging. 5=Policy requires just-in-time privileged access, all privileged sessions are recorded, access is reviewed quarterly, and a PAM tool is deployed. Key elements to verify: Prohibition on shared administrative accounts; MFA requirement for all privileged access; privileged account inventory and justification; privileged session monitoring and logging; access review frequency; just-in-time or least-privilege elevation. Evidence: PAM policy, privileged account inventory with business justification, privileged session logs, MFA enrollment confirmation.

MEDIUM · EFFORT TO FIX: LOW

IT POLICY LIBRARY REVIEW · INCIDENT RESPONSE & PLAYBOOKS

Ransomware Response Playbook

QUESTION ASKED

A specific step-by-step playbook providing tactical guidance for detecting, containing, and recovering from a ransomware attack, including offline communication procedures and ransom payment decision framework.

District 101 Response - 3

RISK & IMPACT

Ransomware Response Playbook scored 3/5 (Defined / Compensating control). A specific step-by-step playbook providing tactical guidance for detecting, containing, and recovering from a ransomware attack, including offline communication procedures and ransom payment decision framework.

RECOMMENDATION

Scoring: 1=No ransomware playbook; the organization would improvise response entirely. 2=General IR plan mentions ransomware but no specific tactical steps exist. 3=A ransomware playbook exists with containment steps but recovery procedures are incomplete, offline backup access is undefined, or ransom decision authority is unclear. 4=Playbook covers detection indicators, immediate isolation steps, offline communication method, backup restoration procedure, ransom decision authority, and law enforcement notification. 5=Playbook is tested through tabletop simulation annually, offline communication channel is validated, backup restoration is tested from ransomware-isolated backups, and legal/FBI notification contacts are current. Key elements to verify: Network isolation steps by system type; offline communication method (pre-established out-of-band channel); ransom payment decision authority and legal review process; FBI/CISA notification procedure; immutable backup location and restoration procedure; decryption key negotiation process; business continuity during recovery. Evidence: Ransomware playbook, tabletop exercise record, immutable backup test record, offline communication channel documentation.

MEDIUM · EFFORT TO FIX: LOW

IT POLICY LIBRARY REVIEW · INCIDENT RESPONSE & PLAYBOOKS

Distributed Denial of Service (DDoS) Response Playbook

QUESTION ASKED

A playbook providing tactical response steps for detecting, mitigating, and recovering from distributed denial of service attacks targeting organizational systems or services.

District 101 Response - 3

RISK & IMPACT

Distributed Denial of Service (DDoS) Response Playbook scored 3/5 (Defined / Compensating control). A playbook providing tactical response steps for detecting, mitigating, and recovering from distributed denial of service attacks targeting organizational systems or services.

RECOMMENDATION

Scoring: 1=No DDoS playbook; the organization has no defined response and would scramble to contact ISP or cloud provider. 2=Basic awareness of DDoS mitigation services but no documented response steps. 3=Playbook exists but ISP upstream filtering contacts are not pre-established, escalation thresholds are undefined, or business communication procedures are not included. 4=Playbook defines detection thresholds, ISP and CDN/scrubbing provider contact procedures, internal escalation path, business communication template, and recovery validation steps. 5=Playbook includes pre-negotiated ISP null-routing or scrubbing activation, is tested via tabletop, and upstream filtering is contractually pre-arranged with defined activation SLAs. Key elements to verify: Detection thresholds and alerting; ISP upstream filtering or null-routing contact and procedure; CDN or DDoS scrubbing service activation steps; business stakeholder communication template; estimated recovery timeline; post-incident traffic analysis. Evidence: DDoS playbook, ISP mitigation service contract or contact record, CDN/scrubbing service agreement.

MEDIUM · EFFORT TO FIX: LOW

IT POLICY LIBRARY REVIEW · DATA MANAGEMENT & CLASSIFICATION POLICIES

Encryption & Cryptography Policy

QUESTION ASKED

A policy governing the use of cryptography and encryption for protecting data at rest and in transit, including approved algorithms, key management requirements, and prohibited practices.

District 101 Response - 3

RISK & IMPACT

The Encryption & Cryptography Policy is not comprehensive, which may lead to inadequate protection of sensitive data. A clear policy is necessary for ensuring proper encryption and cryptography practices.

Affected: Systems containing sensitive data

RECOMMENDATION

Develop an Encryption & Cryptography Policy that outlines procedures for encrypting and decrypting sensitive data.

MEDIUM · EFFORT TO FIX: LOW

IT POLICY LIBRARY REVIEW · NETWORK & INFRASTRUCTURE SECURITY POLICIES

Vulnerability Management Policy

QUESTION ASKED

A policy governing the regular scanning, assessment, prioritization, and remediation of vulnerabilities across organizational systems, applications, and infrastructure.

District 101 Response - 3

RISK & IMPACT

The Vulnerability Management Policy is not well-defined, which may lead to inadequate patch management and vulnerability remediation. A clear policy is necessary for ensuring timely and effective vulnerability management.

Affected: All systems

RECOMMENDATION

Develop a Vulnerability Management Policy that outlines procedures for identifying, prioritizing, and remediating vulnerabilities.

MEDIUM · EFFORT TO FIX: LOW

IT POLICY LIBRARY REVIEW · NETWORK & INFRASTRUCTURE SECURITY POLICIES

Wireless Network Security Policy

QUESTION ASKED

A policy governing the deployment, configuration, and monitoring of wireless networks including corporate WLAN, guest networks, and IoT wireless, specifying authentication and encryption requirements.

District 101 Response - 3

RISK & IMPACT

The Wireless Network Security Policy is not comprehensive, which may lead to inadequate protection of wireless networks. A clear policy is necessary for ensuring secure wireless network configuration and access controls.

Affected: Wireless networks

RECOMMENDATION

Develop a Wireless Network Security Policy that outlines procedures for securing wireless networks and preventing unauthorized access.

MEDIUM · EFFORT TO FIX: LOW

IT POLICY LIBRARY REVIEW · ENDPOINT & DEVICE SECURITY POLICIES

Removable Media & USB Policy

QUESTION ASKED

A policy governing the use of removable media (USB drives, external hard drives, optical media) including permitted use cases, encryption requirements, and technical controls.

District 101 Response - 3

RISK & IMPACT

The Removable Media & USB Policy is not well-defined, which may lead to inadequate protection of sensitive data on removable media. A clear policy is necessary for ensuring proper handling and storage of removable media.

Affected: Systems containing sensitive data

RECOMMENDATION

Develop a Removable Media & USB Policy that outlines procedures for handling, storing, and disposing of removable media.

MEDIUM · EFFORT TO FIX: LOW

IT POLICY LIBRARY REVIEW · ENDPOINT & DEVICE SECURITY POLICIES

Clean Desk & Screen Lock Policy

QUESTION ASKED

A policy governing physical security of workspaces including screen lock requirements, secure storage of sensitive documents, and preventing unauthorized viewing of sensitive information.

District 101 Response - 3

RISK & IMPACT

The Clean Desk & Screen Lock Policy is not comprehensive, which may lead to inadequate protection of sensitive information. A clear policy is necessary for ensuring proper handling and storage of sensitive information.

Affected: All systems

RECOMMENDATION

Develop a Clean Desk & Screen Lock Policy that outlines procedures for securing workstations and preventing unauthorized access to sensitive information.

MEDIUM · EFFORT TO FIX: LOW

IT POLICY LIBRARY REVIEW · VENDOR & THIRD-PARTY RISK POLICIES

Third-Party Access Policy

QUESTION ASKED

A policy governing how third-party vendors, contractors, and service providers are granted, managed, and revoked access to organizational systems, networks, and data.

District 101 Response - 3

RISK & IMPACT

The Third-Party Access Policy is not well-defined, which may lead to inadequate protection of sensitive data accessed by third-party vendors. A clear policy is necessary for ensuring secure access controls and monitoring.

Affected: All systems and data

RECOMMENDATION

Develop a Third-Party Access Policy that outlines procedures for granting, revoking, and monitoring access to sensitive systems and data by third-party vendors.

MEDIUM · EFFORT TO FIX: LOW

IT POLICY LIBRARY REVIEW · HUMAN RESOURCES & ACCEPTABLE USE POLICIES

Security Awareness & Training Policy

QUESTION ASKED

A policy governing the security awareness and training program including required training for all employees, role-based training for security roles, phishing simulation requirements, and training frequency.

District 101 Response - 3

RISK & IMPACT

The Security Awareness & Training Policy is not comprehensive, which may lead to inadequate security awareness among employees. A clear policy is necessary for ensuring regular security training and awareness programs.

Affected: All systems

RECOMMENDATION

Develop a Security Awareness & Training Policy that outlines procedures for providing regular security training and awareness programs to employees.

MEDIUM · EFFORT TO FIX: LOW

IT POLICY LIBRARY REVIEW · COMPLIANCE & AUDIT POLICIES

Log Management & SIEM Policy

QUESTION ASKED

A policy governing the collection, storage, retention, protection, and review of security logs from all systems, applications, and network devices, including SIEM integration requirements.

District 101 Response - 3

RISK & IMPACT

The Log Management & SIEM Policy is not well-defined, which may lead to inadequate log collection, monitoring, and analysis. A clear policy is necessary for ensuring proper log management and security information and event management (SIEM) practices.

Affected: All systems

RECOMMENDATION

Develop a Log Management & SIEM Policy that outlines procedures for collecting, storing, and analyzing logs, as well as implementing SIEM systems.

MEDIUM · EFFORT TO FIX: LOW

IT POLICY LIBRARY REVIEW · COMPLIANCE & AUDIT POLICIES

Security Metrics & Reporting Policy

QUESTION ASKED

A policy governing the definition, collection, reporting, and escalation of information security metrics to leadership, including key risk indicators (KRIs) and key performance indicators (KPIs).

District 101 Response - 3

RISK & IMPACT

The Security Metrics & Reporting Policy is not comprehensive, which may lead to inadequate security metrics collection and reporting. A clear policy is necessary for ensuring proper security metrics collection and reporting practices.

Affected: All systems

RECOMMENDATION

Develop a Security Metrics & Reporting Policy that outlines procedures for collecting, analyzing, and reporting security metrics.

MEDIUM · EFFORT TO FIX: LOW

EDUCATION POLICY & COMPLIANCE REVIEW · GOVERNANCE & POLICY PROGRAM

Incident Response & Breach Notification

QUESTION ASKED

A documented incident response plan exists, is tested at least annually, and includes student data breach notification procedures aligned with FERPA and applicable state law.

District 101 Response - 3

RISK & IMPACT

District 101's incident response plan is not comprehensive or well-established, which could lead to ineffective response to security incidents.

Affected: All systems and data

RECOMMENDATION

Develop an incident response plan that includes procedures for responding to security incidents and breaches.

MEDIUM · EFFORT TO FIX: LOW

EDUCATION POLICY & COMPLIANCE REVIEW · GOVERNANCE & POLICY PROGRAM

Vendor & Third-Party Risk Management

QUESTION ASKED

A formal vendor risk management program exists that evaluates the security and privacy practices of all vendors who access or process institutional or student data.

District 101 Response - 3

RISK & IMPACT

District 101's vendor and third-party risk management practices are not comprehensive or well-established, which could lead to security gaps and inefficiencies.

Affected: Vendor systems and data

RECOMMENDATION

Establish clear vendor and third-party risk management practices to ensure all vendors and third-parties are properly vetted and managed.

MEDIUM · EFFORT TO FIX: LOW EDUCATION POLICY & COMPLIANCE REVIEW · FERPA — STUDENT RECORDS PRIVACY

Third-Party Disclosure Controls & School Official Agreements

QUESTION ASKED

Disclosures of student records to third parties (vendors, contractors, other institutions) are made only under FERPA-permitted exceptions and are documented.

District 101 Response - 3

RISK & IMPACT

District 101's third-party disclosure controls and school official agreements are not comprehensive or well-established, which could lead to unauthorized disclosure of student data.

Affected: Student data and systems

RECOMMENDATION

Establish clear third-party disclosure controls and school official agreements to ensure only authorized personnel have access to student data.

MEDIUM · EFFORT TO FIX: LOW EDUCATION POLICY & COMPLIANCE REVIEW · FERPA — STUDENT RECORDS PRIVACY

FERPA Breach & Unauthorized Disclosure Procedures

QUESTION ASKED

The institution has defined procedures for responding to unauthorized disclosures of student education records, including notification to the U.S. Department of Education when required.

District 101 Response - 3

RISK & IMPACT

District 101's FERPA breach and unauthorized disclosure procedures are not comprehensive or well-established, which could lead to ineffective response to security incidents.

Affected: Student data and systems

RECOMMENDATION

Develop FERPA breach and unauthorized disclosure procedures that include steps for responding to security incidents and breaches.

MEDIUM · EFFORT TO FIX: LOW EDUCATION POLICY & COMPLIANCE REVIEW · COPPA — CHILDREN'S ONLINE PRIVACY (K-12)

EdTech App Inventory & COPPA Applicability Assessment

QUESTION ASKED

[K-12] The institution maintains an inventory of all digital tools and applications used with students under 13, and has assessed each for COPPA applicability.

District 101 Response - 3

RISK & IMPACT

District 101's EdTech app inventory and COPPA applicability assessment are not comprehensive or well-established, which could lead to non-compliance with federal regulations.

Affected: Student data and systems

RECOMMENDATION

Conduct a comprehensive EdTech app inventory and COPPA applicability assessment to ensure all apps are properly vetted and managed.

MEDIUM · EFFORT TO FIX: LOW

Internet Safety Policy

QUESTION ASKED

[K-12] The district has adopted and enforces an Internet Safety Policy (ISP) as required for E-Rate funding recipients under CIPA, covering all required content areas.

District 101 Response - 3

RISK & IMPACT

District 101's internet safety policy is well-established, but could be improved with more comprehensive guidelines for employee and student behavior online.

Affected: Employee systems and data

RECOMMENDATION

Review and update the internet safety policy to ensure it includes comprehensive guidelines for employee and student behavior online.

MEDIUM · EFFORT TO FIX: LOW

Technology Protection Measures & Content Filtering

QUESTION ASKED

[K-12] The district operates technology protection measures (content filtering) on all school internet connections and devices, and has processes for monitoring online activities.

District 101 Response - 3

RISK & IMPACT

District 101's technology protection measures and content filtering are well-established, but could be improved with more comprehensive monitoring and incident response procedures.

Affected: All systems and data

RECOMMENDATION

Review and update the technology protection measures and content filtering to ensure they include comprehensive monitoring and incident response procedures.

MEDIUM · EFFORT TO FIX: LOW

Acceptable Use Policy — Students & Staff

QUESTION ASKED

[K-12] The district has Acceptable Use Policies (AUPs) for both students and staff governing use of district technology, networks, and devices, including personal devices (BYOD).

District 101 Response - 3

RISK & IMPACT

District 101's acceptable use policy for students and staff is well-established, but could be improved with more comprehensive guidelines for employee and student behavior online.

Affected: Employee systems and data

RECOMMENDATION

Review and update the acceptable use policy to ensure it includes comprehensive guidelines for employee and student behavior online.

MEDIUM · EFFORT TO FIX: LOW EDUCATION POLICY & COMPLIANCE REVIEW · EDTECH & THIRD-PARTY APP GOVERNANCE

EdTech Procurement & Review Process

QUESTION ASKED

The institution has a formal procurement process for educational technology that includes security, privacy, and compliance review before adoption.

District 101 Response - 3

RISK & IMPACT

District 101's EdTech procurement and review process is well-established, but could be improved with more comprehensive vetting of vendors and third-parties.

Affected: Vendor systems and data

RECOMMENDATION

Review and update the EdTech procurement and review process to ensure it includes comprehensive vetting of vendors and third-parties.

MEDIUM · EFFORT TO FIX: LOW EDUCATION POLICY & COMPLIANCE REVIEW · EDTECH & THIRD-PARTY APP GOVERNANCE

Data Processing Agreements & Student Data Contracts

QUESTION ASKED

All EdTech vendors who access, process, or store student data have signed Data Processing Agreements (DPAs) or equivalent contracts that define permissible data use, security requirements, and breach notification obligations.

District 101 Response - 3

RISK & IMPACT

District 101's data processing agreements and student data contracts are well-established, but could be improved with more comprehensive guidelines for vendor and third-party management.

Affected: Vendor systems and data

RECOMMENDATION

Review and update the data processing agreements and student data contracts to ensure they include comprehensive guidelines for vendor and third-party management.

MEDIUM · EFFORT TO FIX: LOW EDUCATION POLICY & COMPLIANCE REVIEW · STATE STUDENT PRIVACY LAWS

State Privacy Law Inventory & Applicability Assessment

QUESTION ASKED

The institution has identified and assessed all applicable state student privacy laws, including SOPIPA-type laws, biometric data regulations, and student data transparency requirements.

District 101 Response - 3

RISK & IMPACT

District 101's state privacy law inventory and applicability assessment are well-established, but could be improved with more comprehensive monitoring and incident response procedures.

Affected: All systems and data

RECOMMENDATION

Review and update the state privacy law inventory and applicability assessment to ensure they include comprehensive monitoring and incident response procedures.

MEDIUM · EFFORT TO FIX: LOW

VULNERABILITY MANAGEMENT DISCOVERY · SCANNING & DISCOVERY

Vulnerability Scan Coverage

QUESTION ASKED

Vulnerability scans are performed on all systems — including internet-facing, internal, cloud, and network devices — on a defined and enforced schedule.

District 101 Response - 3

RISK & IMPACT

District 101's vulnerability scan coverage is incomplete, leaving some systems unscanned for vulnerabilities. This gap increases the risk of exploitation and potential security breaches in unscanned systems.

Affected: Unscanned systems

RECOMMENDATION

Improve vulnerability scan coverage to ensure that all systems are properly scanned for vulnerabilities.

MEDIUM · EFFORT TO FIX: LOW

VULNERABILITY MANAGEMENT DISCOVERY · PRIORITIZATION & RISK

Risk Acceptance Process

QUESTION ASKED

Vulnerabilities that cannot be remediated within SLA have a formal risk acceptance process — documented, owner-approved, time-limited, and tracked to re-review.

District 101 Response - 3

RISK & IMPACT

District 101's risk acceptance process is not well-defined, which can lead to inconsistent or ineffective risk management. This gap increases the risk of exploitation and potential security breaches.

Affected: All systems with identified vulnerabilities

RECOMMENDATION

Develop a clear risk acceptance process to ensure consistent and effective risk management.

MEDIUM · EFFORT TO FIX: LOW

VULNERABILITY MANAGEMENT DISCOVERY · REMEDIATION & PATCHING

Patch Deployment Process

QUESTION ASKED

A defined, automated patch deployment process covers operating systems, applications, and firmware across all managed systems, with defined SLAs enforced through tooling.

District 101 Response - 3

RISK & IMPACT

District 101's patch deployment process is not well-defined, which can lead to delayed or ineffective vulnerability remediation. This gap increases the risk of exploitation and potential security breaches.

Affected: All systems with identified vulnerabilities

RECOMMENDATION

Establish a clear patch deployment process to ensure timely and effective vulnerability remediation.

MEDIUM · EFFORT TO FIX: LOW

VULNERABILITY MANAGEMENT DISCOVERY · VISIBILITY & REPORTING

Penetration Testing

QUESTION ASKED

Periodic penetration tests — conducted by qualified internal or external testers — validate that vulnerability management controls are working and identify vulnerabilities that automated scanning misses.

District 101 Response - 3

RISK & IMPACT

District 101's penetration testing is not comprehensive, which can leave potential risks undetected. This gap increases the risk of exploitation and potential security breaches.

Affected: All systems

RECOMMENDATION

Conduct regular, comprehensive penetration testing to identify and address potential risks.

MEDIUM · EFFORT TO FIX: LOW

SECURITY AWARENESS & PHISHING DISCOVERY · TRAINING PROGRAM

Role-Based Security Training

QUESTION ASKED

Employees in high-risk roles — finance, HR, IT, executives, and those with access to sensitive data — receive targeted training beyond the standard all-staff program.

District 101 Response - 3

RISK & IMPACT

Role-based security training is not comprehensive, with some job functions lacking specific security training programs.

Affected: Employee training records and HR systems

RECOMMENDATION

Develop role-based security training programs that cater to specific job functions and responsibilities.

MEDIUM · EFFORT TO FIX: LOW

SECURITY AWARENESS & PHISHING DISCOVERY · REPORTING CULTURE

Suspicious Activity Reporting Mechanism

QUESTION ASKED

A simple, accessible, and well-publicized mechanism exists for employees to report suspicious emails, calls, and activities — and reports are acted upon promptly.

District 101 Response - 3

RISK & IMPACT

The suspicious activity reporting mechanism is adequate but could be improved, with some employees unsure of how to report security incidents.

Affected: Security incident reporting system and employee email

RECOMMENDATION

Develop a comprehensive incident response plan that includes clear procedures for reporting security incidents, and provide regular reminders and notifications to employees.

MEDIUM · EFFORT TO FIX: LOW

ASSET & DATA INVENTORY DISCOVERY · HARDWARE ASSET MANAGEMENT

Unauthorized Device Detection

QUESTION ASKED

Unauthorized or unmanaged devices connecting to the network are detected, alerted on, and investigated — preventing attackers from using rogue devices as persistent footholds.

District 101 Response - 3

RISK & IMPACT

The district's unauthorized device detection capabilities are limited, making it challenging to identify and respond to potential security threats. This gap increases the risk of malicious devices being connected to the network.

Affected: All district systems, including endpoints, servers, and network devices

RECOMMENDATION

Enhance unauthorized device detection capabilities using automated tools and manual processes to identify and respond to potential security threats

MEDIUM · EFFORT TO FIX: LOW

ASSET & DATA INVENTORY DISCOVERY · DATA ASSET MANAGEMENT

Sensitive Data Discovery and Location

QUESTION ASKED

The organization knows where its sensitive data lives — including structured databases, unstructured file shares, email, cloud storage, and endpoint devices — through active discovery rather than assumption.

District 101 Response - 3

RISK & IMPACT

The district's sensitive data discovery and location capabilities are incomplete, making it challenging to track and protect sensitive data. This gap increases the risk of sensitive data being exposed or compromised.

Affected: All district systems storing or processing sensitive data

RECOMMENDATION

Conduct a thorough sensitive data discovery exercise using automated tools and manual processes to identify and locate all sensitive data

MEDIUM · EFFORT TO FIX: LOW

ASSET & DATA INVENTORY DISCOVERY · CLOUD ASSET VISIBILITY

Cloud Account and Resource Inventory

QUESTION ASKED

All cloud accounts, subscriptions, and resources — including production, development, and shadow cloud usage — are inventoried and managed under centralized oversight.

District 101 Response - 3

RISK & IMPACT

The district's cloud account and resource inventory is incomplete, making it challenging to track and manage cloud resources. This gap increases the risk of unapproved or malicious cloud resources being created.

Affected: All district cloud resources, including AWS, Azure, and Google Cloud

RECOMMENDATION

Conduct a thorough cloud account and resource inventory using automated tools and manual processes to identify all cloud resources

MEDIUM · EFFORT TO FIX: LOW — INCIDENT RESPONSE READINESS DISCOVERY · TEAM & CONTACTS

External Incident Response Support

QUESTION ASKED

External IR support — through a retainer agreement, MDR provider, or cyber insurance — is established before an incident occurs, not researched in the middle of a crisis.

District 101 Response - 3

RISK & IMPACT

External Incident Response Support is not fully established, limiting the organization's ability to respond effectively to complex incidents.

Affected: Incident Response Team, IT systems

RECOMMENDATION

Establish relationships with external incident response providers, ensuring access to specialized expertise and resources during incidents.

MEDIUM · EFFORT TO FIX: LOW — INCIDENT RESPONSE READINESS DISCOVERY · NOTIFICATION & COMMUNICATION

Internal and Executive Communications

QUESTION ASKED

Pre-approved internal communications templates and an escalation path to executive leadership are in place — so the first hour of an incident is spent responding, not drafting emails.

District 101 Response - 3

RISK & IMPACT

Internal and Executive Communications are not fully established, increasing the risk of ineffective incident response and reputational damage.

Affected: Executive team, employees

RECOMMENDATION

Develop and implement clear internal and executive communication procedures, ensuring timely and effective information sharing during incidents.

MEDIUM · EFFORT TO FIX: LOW — INCIDENT RESPONSE READINESS DISCOVERY · NOTIFICATION & COMMUNICATION

External and Public Communications

QUESTION ASKED

A plan exists for communicating with external stakeholders — customers, partners, media, and the public — during and after a significant incident, including who is authorized to speak and what can be said.

District 101 Response - 3

RISK & IMPACT

External and Public Communications are not fully established, increasing the risk of reputational damage and ineffective incident response.

Affected: Customers, stakeholders

RECOMMENDATION

Develop and implement clear external and public communication procedures, ensuring timely and effective information sharing during incidents.

MEDIUM · EFFORT TO FIX: LOW

CLOUD SECURITY POSTURE DISCOVERY · CONFIGURATION & HARDENING

Cloud Tenant Security Baseline

QUESTION ASKED

Cloud tenants (M365, Google Workspace, AWS, Azure) are configured against a documented security baseline — with deviation from baseline detected and remediated.

District 101 Response - 3

RISK & IMPACT

Cloud Tenant Security Baseline is well-implemented, with a score of 3/5.

Affected: All cloud-based systems and applications

RECOMMENDATION

Continue to monitor and maintain the cloud tenant security baseline to ensure ongoing security and compliance.

MEDIUM · EFFORT TO FIX: LOW

CLOUD SECURITY POSTURE DISCOVERY · CONFIGURATION & HARDENING

Cloud Application and OAuth Consent Controls

QUESTION ASKED

Third-party applications requesting OAuth access to cloud data are governed — preventing malicious or unauthorized apps from gaining persistent access to email, files, and contacts.

District 101 Response - 3

RISK & IMPACT

Cloud Application and OAuth Consent Controls are well-implemented, with a score of 3/5.

Affected: All cloud-based applications

RECOMMENDATION

Continue to monitor and maintain the cloud application and OAuth consent controls to ensure ongoing security and compliance.

MEDIUM · EFFORT TO FIX: LOW

CLOUD SECURITY POSTURE DISCOVERY · DATA PROTECTION IN CLOUD

Cloud Data Encryption

QUESTION ASKED

Sensitive data in cloud platforms is encrypted at rest and in transit, with encryption keys managed appropriately and not solely controlled by the cloud provider.

District 101 Response - 3

RISK & IMPACT

Cloud Data Encryption is well-implemented, with a score of 3/5.

Affected: All cloud-based storage systems

RECOMMENDATION

Continue to monitor and maintain the cloud data encryption controls to ensure ongoing security and compliance.

MEDIUM · EFFORT TO FIX: LOW

CLOUD SECURITY POSTURE DISCOVERY · MONITORING & LOGGING

Cloud Audit Logging

QUESTION ASKED

Audit logs are enabled across all cloud platforms — capturing admin actions, user sign-ins, data access, and configuration changes — and retained for a sufficient period to support investigations.

District 101 Response - 3

RISK & IMPACT

Cloud Audit Logging is well-implemented, with a score of 3/5.

Affected: All cloud-based systems and applications

RECOMMENDATION

Continue to monitor and maintain the cloud audit logging controls to ensure ongoing security and compliance.

MEDIUM · EFFORT TO FIX: LOW

BACKUP & DISASTER RECOVERY DISCOVERY · BACKUP COVERAGE & STRATEGY

Backup Frequency and Retention

QUESTION ASKED

Backup frequency and retention periods align to business requirements — capturing enough recovery points to meet RPOs while retaining history long enough to recover from delayed-discovery ransomware.

District 101 Response - 3

RISK & IMPACT

Backup Frequency and Retention policies are not aligned with business requirements, resulting in potential data loss or corruption.

Affected: All systems with sensitive data

RECOMMENDATION

Review and update backup frequency and retention policies to ensure they align with business requirements and industry best practices, including regular review of data classification and retention schedules.

MEDIUM · EFFORT TO FIX: LOW

BACKUP & DISASTER RECOVERY DISCOVERY · BACKUP SECURITY

Immutable and Air-Gapped Backups

QUESTION ASKED

At least one backup copy is immutable (cannot be modified or deleted for a defined period) or air-gapped (physically disconnected from the network) — protecting against ransomware that encrypts or deletes backups.

District 101 Response - 3

RISK & IMPACT

Immutable and air-gapped backups are not implemented, leaving District 101's backups vulnerable to data loss or corruption.

Affected: All systems with sensitive data

RECOMMENDATION

Implement immutable and air-gapped backups to provide an additional layer of protection against data loss and corruption, including the use of write-once media and secure storage solutions.

MEDIUM · EFFORT TO FIX: LOW

BACKUP & DISASTER RECOVERY DISCOVERY · BACKUP SECURITY

Backup Monitoring and Alerting

QUESTION ASKED

Backup jobs are monitored continuously and failures are alerted promptly — so that a failed backup is discovered and remediated before an incident, not after.

District 101 Response - 3

RISK & IMPACT

Backup Monitoring and Alerting capabilities are inadequate, resulting in potential delays in detecting and responding to backup-related issues.

Affected: All systems with sensitive data

RECOMMENDATION

Enhance backup monitoring and alerting capabilities to quickly detect and respond to potential issues, including the implementation of real-time monitoring tools and automated alerting systems.

MEDIUM · EFFORT TO FIX: LOW

BACKUP & DISASTER RECOVERY DISCOVERY · DR PLANNING & RTO/RPO

Business Continuity During Recovery

QUESTION ASKED

The organization has documented plans for continuing essential operations during a recovery period — including manual workarounds, communication to staff and customers, and prioritization of what to restore first.

District 101 Response - 3

RISK & IMPACT

Business Continuity During Recovery is not adequately planned, resulting in potential disruptions to business operations during the recovery process.

Affected: All systems with sensitive data

RECOMMENDATION

Develop a plan for maintaining business continuity during the recovery process, including communication strategies and resource allocation, to minimize disruptions to business operations.

MEDIUM · EFFORT TO FIX: LOW

VENDOR & THIRD-PARTY RISK DISCOVERY · VENDOR ASSESSMENT

Periodic Vendor Re-Assessment

QUESTION ASKED

Vendor security posture is re-assessed periodically — not just at onboarding — because vendor security degrades, ownership changes, and new vulnerabilities emerge after a vendor relationship begins.

District 101 Response - 3

RISK & IMPACT

Periodic Vendor Re-Assessment is not conducted regularly, which may lead to undetected changes in vendor risk profiles.

Affected: All systems and data handled by third-party vendors

RECOMMENDATION

Establish a regular schedule for Periodic Vendor Re-Assessments to ensure timely detection of changes in vendor risk profiles and adjust mitigation efforts accordingly.

MEDIUM · EFFORT TO FIX: LOW

VENDOR & THIRD-PARTY RISK DISCOVERY · VENDOR ASSESSMENT

Vendor Incident and Breach Notification Tracking

QUESTION ASKED

The organization has a process to receive, track, and respond to security incidents and breaches reported by vendors — including incidents at sub-processors and fourth parties.

District 101 Response - 3

RISK & IMPACT

Vendor Incident and Breach Notification Tracking is not comprehensive, which may lead to delayed or inadequate incident response.

Affected: All systems and data handled by third-party vendors

RECOMMENDATION

Develop a comprehensive Vendor Incident and Breach Notification Tracking process to ensure timely detection and response to security incidents involving vendors.

MEDIUM · EFFORT TO FIX: LOW

VENDOR & THIRD-PARTY RISK DISCOVERY · MONITORING & OFFBOARDING

Vendor Offboarding and Access Termination

QUESTION ASKED

When vendor relationships end, all vendor access is promptly revoked, data is returned or deleted, and the termination is documented — closing the loop on the relationship.

District 101 Response - 3

RISK & IMPACT

Vendor Offboarding and Access Termination processes are not comprehensive, which may lead to residual access risks.

Affected: All systems accessed by vendors

RECOMMENDATION

Develop a comprehensive Vendor Offboarding and Access Termination process to ensure timely revocation of vendor access rights and minimize residual access risks.

MEDIUM · EFFORT TO FIX: LOW

PHYSICAL SECURITY DISCOVERY · SERVER ROOM & EQUIPMENT

Server Room and Data Center Physical Security

QUESTION ASKED

Server rooms, data closets, and data centers are physically secured to a higher standard than general office areas — with restricted access, environmental monitoring, and tamper detection.

District 101 Response - 3

RISK & IMPACT

While the server room and data center physical security controls are in place, there is room for improvement to ensure the protection of sensitive equipment and data.

Affected: Server room and data center equipment and data

RECOMMENDATION

Conduct a thorough assessment of the server room and data center physical security controls and implement additional measures as necessary, such as enhanced surveillance or access controls.

MEDIUM · EFFORT TO FIX: LOW

PHYSICAL SECURITY DISCOVERY · SERVER ROOM & EQUIPMENT

Physical Device Security and Tamper Prevention

QUESTION ASKED

Physical IT assets — servers, network equipment, workstations — are secured against theft, tampering, and unauthorized hardware modification.

District 101 Response - 3

RISK & IMPACT

Physical device security and tamper prevention controls are in place but could be improved to prevent unauthorized access or tampering with sensitive equipment.

Affected: Sensitive equipment within the facility

RECOMMENDATION

Implement additional physical device security and tamper prevention measures, such as secure cabinets or tamper-evident tape, to protect sensitive equipment.

MEDIUM · EFFORT TO FIX: LOW

PHYSICAL SECURITY DISCOVERY · SERVER ROOM & EQUIPMENT

Cabling and Network Port Security

QUESTION ASKED

Network infrastructure — patch panels, network ports, cabling, and wireless access points — is physically secured to prevent unauthorized network connections or interception.

District 101 Response - 3

RISK & IMPACT

Cabling and network port security controls are in place but could be improved to prevent unauthorized access or tampering with sensitive networks and systems.

Affected: Sensitive networks and systems within the facility

RECOMMENDATION

Implement additional cabling and network port security measures, such as secure patch panels or network port locks, to protect sensitive networks and systems.

MEDIUM · EFFORT TO FIX: LOW

PHYSICAL SECURITY DISCOVERY · VISITOR & SOCIAL ENGINEERING

Visitor Management Process

QUESTION ASKED

All visitors — including contractors, vendors, service technicians, and guests — are registered, identified, badged, and escorted appropriately, with access limited to areas required for their visit.

District 101 Response - 3

RISK & IMPACT

The visitor management process is effective but could be improved to prevent unauthorized access or tailgating.

Affected: All systems and data within the facility

RECOMMENDATION

Implement additional visitor management measures, such as enhanced surveillance or access controls, to prevent unauthorized access or tailgating.

MEDIUM · EFFORT TO FIX: LOW

PHYSICAL SECURITY DISCOVERY · VISITOR & SOCIAL ENGINEERING

CCTV and Physical Surveillance

QUESTION ASKED

Camera systems provide adequate coverage of critical access points and sensitive areas, with footage retained long enough to support incident investigations.

District 101 Response - 3

RISK & IMPACT

CCTV and physical surveillance controls are in place but could be improved to provide more comprehensive coverage and deterrence.

Affected: All systems and data within the facility

RECOMMENDATION

Conduct a thorough assessment of the CCTV and physical surveillance controls and implement additional measures as necessary, such as enhanced camera placement or monitoring protocols.

MEDIUM · EFFORT TO FIX: LOW

AI & EMERGING TECHNOLOGY RISK DISCOVERY · SHADOW AI & DATA LEAKAGE

AI Tool Security Awareness

QUESTION ASKED

Employees understand the data security and privacy risks of AI tool usage — specifically the risk of entering organizational data into public LLMs — and can make informed decisions about what to enter.

District 101 Response - 3

RISK & IMPACT

The lack of adequate AI Tool Security Awareness increases the risk of security breaches or reputational damage, as employees may not be aware of potential security risks associated with AI tools.

Affected: All systems and data utilizing AI tools

RECOMMENDATION

Provide regular training on AI Tool Security Awareness to employees, and implement robust access controls and monitoring mechanisms for AI tools.