

# Risk Assessment

Risk assessment asks whether you find your own weaknesses before attackers do, and whether you understand what a successful attack would cost: days of canceled instruction, missed payroll, or a mass...

## Why it matters

- Attackers scan the internet for exposed, unpatched systems such as old virtual private network (VPN) appliances and remote desktop servers. Regular external scanning and a patch calendar let you find those openings on your schedule, not during a ransomware event that closes schools.
- Leaders cannot fund what they cannot see. A short risk register that describes impact in school terms (no SIS during state testing, delayed payroll, unrouted buses) gives the superintendent and board a clear basis for budget and insurance decisions.
- A backup that has never been restored may not work when you need it. A dated restore test shows the carrier real evidence and tells you whether the SIS or finance system could actually be rebuilt.

Unpatched internet-facing systems remain a common path to district ransomware, and insurers now ask for scan results, backup testing, and evidence that someone actually reviews risk. A documented, repeating assessment process is what separates 'we think we're fine' from a defensible answer at renewal time or after an incident.

## What good looks like at each level

| Level                 | What you would see                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Artifacts that show it                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>1 · Initial</b>    | <p>No one looks for weaknesses until something breaks. Patching happens when someone has time, nobody can say what an outage of a key system would cost the schools, and the district does not take part in information-sharing groups.</p> <p>Moving up: Get leadership visibly engaged — a cabinet cyber-risk briefing counts — and start the shift from reactive to proactive: join information-sharing forums like MS-ISAC and K12 SIX and stand up a basic vulnerability-identification process such as CISA's free scanning.</p>                               | <ul style="list-style-type: none"> <li>• No vulnerability scanning; exposed systems come to light through a vendor, the news or an incident</li> <li>• No record of which servers or network devices are behind on updates</li> <li>• Backups run, but no one has ever restored from them as a test</li> </ul>                                                                                                                                                           |
| <b>2 · Repeatable</b> | <p>Leadership has heard the risks and wants a plan. The district has started free external scanning, joined information-sharing groups and drafted a first risk list, though the process is still being written.</p> <p>Moving up: Document the process and build it into daily operations: scheduled scans and patching, threat intelligence actually collected and reviewed, instructional and business impact recorded for top risks, and backup and recovery systems tested and evaluated at least annually with evidence.</p>                                   | <ul style="list-style-type: none"> <li>• Cabinet agenda or notes showing a cybersecurity risk briefing</li> <li>• Enrollment in CISA Cyber Hygiene scanning or a first scan report, plus MS-ISAC or K12 SIX membership</li> <li>• Draft risk register with the district's worst-case scenarios</li> </ul>                                                                                                                                                                |
| <b>3 · Defined</b>    | <p>Finding and fixing weaknesses is written down and part of the monthly routine: scheduled scans, a patch calendar, reviewed threat advisories and a risk register that records instructional and business impact. Server rooms and network closets are secured, and backup recovery is tested at least annually.</p> <p>Moving up: Adopt a risk management strategy that goes beyond compliance minimums, and invest in people: train staff on conducting risk assessments and make risk review a standing leadership agenda item with real metrics behind it.</p> | <ul style="list-style-type: none"> <li>• Written vulnerability and patch procedure, patch calendar and exception log, with scan findings tracked to a fix or a documented exception</li> <li>• Risk register with likelihood, impact on instruction and operations, owner and review date, reviewed on a set schedule</li> <li>• Locked server room and network closets limited to named staff, plus a dated backup restore test report with scope and result</li> </ul> |
| <b>4 · Managed</b>    | <p>Risk is managed by a strategy, not just a checklist. Leadership has set how much risk the district will accept, goes beyond insurance and compliance minimums, and invests in training the people who assess risk.</p> <p>Moving up: Move to a disciplined, fact-based improvement cycle run by qualified practitioners — in-house staff, a regional co-op, or a contracted vCISO — who measure and assess every part of the school system on a continuing schedule.</p>                                                                                          | <ul style="list-style-type: none"> <li>• Board-approved risk management strategy or risk tolerance statement</li> <li>• Training records for staff who conduct risk assessments or vendor reviews</li> <li>• Remediation measures such as time to fix critical findings and open exceptions, reviewed by cabinet</li> </ul>                                                                                                                                              |

| Level                | What you would see                                                                                                                                                                             | Artifacts that show it                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>5 · Optimized</b> | Qualified practitioners assess every part of the school system on a continuing schedule, and the results drive a fact-based improvement cycle that also refines the assessment process itself. | <ul style="list-style-type: none"> <li>Annual written assessment by a qualified practitioner (district staff, the Regional Educational Service Agency (RESA) or a contracted virtual chief information security officer) covering technology, business office, facilities and vendors</li> <li>Periodic external penetration test with findings tracked to closure</li> <li>Trend reports on risk and remediation used to change priorities and the assessment method</li> </ul> |

## Quick wins

| Quick win and how                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Cost     | Effort | Usual owner                       |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|--------|-----------------------------------|
| <b>Enroll in CISA's free Cyber Hygiene external vulnerability scanning</b><br>To enroll with the Cybersecurity and Infrastructure Security Agency (CISA), email <a href="mailto:vulnerability@cisa.dhs.gov">vulnerability@cisa.dhs.gov</a> with the subject "Requesting Cyber Hygiene Services", return the signed service agreement, and list your public IP address ranges (your internet provider can confirm them). Weekly reports then arrive by email; save them as evidence. | Free     | Hours  | Technology director               |
| <b>Join MS-ISAC and subscribe to K12 SIX's free resources</b><br>Apply through the Multi-State Information Sharing and Analysis Center (MS-ISAC) website with a district email address and pick the membership tier that fits; confirm any cost with the business office. Sign up for K12 SIX's free resources and route both advisory feeds to a shared mailbox someone reads weekly.                                                                                              | Low cost | Hours  | Technology director               |
| <b>Draft a 10-row risk register of your worst-case scenarios and walk leadership through it</b><br>Use columns for scenario, what stops working at school, likelihood, impact, owner and next action, with rows such as ransomware on the SIS during state testing, payroll diverted by a fake vendor email, or a vendor breach of student records. Walk cabinet through it in 30 minutes and record the decisions.                                                                 | Free     | Days   | Technology director               |
| <b>Restore one file or VM from backup and write down what happened</b><br>Pick a business-critical item, such as the finance server virtual machine or a shared folder, and restore it to a separate location so production is not overwritten. Record the date, what was restored, how long it took and any problems, and file the note as evidence.                                                                                                                               | Free     | Hours  | Network and systems administrator |
| <b>Confirm automatic updates are enforced for Chromebooks, browsers, and Windows endpoints</b><br>In Google Admin, check Devices > Chrome > Settings > Device (Device update settings) so updates are allowed and not pinned to an old version, and review the Auto Update Expiration date column for aging Chromebooks. For Windows and browsers, confirm update rings or update policies in Intune or Group Policy and review the compliance report.                              | Free     | Hours  | Network and systems administrator |

Free means staff time, existing licenses or free government services. Effort: hours, days or weeks.

## Common pitfalls

- Scanning without fixing. A report that shows the same critical findings month after month documents a known, unaddressed risk for carriers and auditors; track each critical finding to a fix date or a written exception with compensating controls.
- Keeping risk inside IT. A register entry that only says "old firewall" gives leadership nothing to weigh; describe the school impact (attendance, payroll, state testing, transportation) and assign business owners where it fits.
- Assuming cloud data is backed up. Google Workspace and Microsoft 365 keep services running, and Google Vault is built for retention and legal holds rather than restoring whole accounts or shared drives; decide whether you need a separate backup and test whatever you rely on.
- Letting exceptions become permanent. A legacy server kept for one state reporting or finance application stays exposed until someone acts; give every exception a review date, isolation from student networks and a retirement plan.
- Skipping review for free or grant-funded tools. Classroom apps and new services can arrive through a teacher, a principal or a grant without a security or privacy check; route every acquisition, including free sign-ups, through the same review and data privacy agreement.

## Evidence that proves it

- Recent external vulnerability scan report (e.g., CISA Cyber Hygiene weekly report)
- Risk register with scenarios, impact ratings, owners, and review dates
- Documented backup restore test with date, scope, and outcome
- MS-ISAC membership confirmation and samples of advisories acted on
- Patch schedule and patch-compliance reports for servers and endpoints
- Vendor security review checklist and signed DPAs from recent purchases
- Cabinet or board briefing notes covering top cyber risks

## Who usually owns it

|                                          |                                                                                                                                                |
|------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Technology director</b>               | Runs scanning, patching and threat-advisory review, keeps the risk register current and briefs leadership on the top risks.                    |
| <b>Network and systems administrator</b> | Applies patches, works scan findings to closure, documents exceptions and performs the scheduled backup restore tests.                         |
| <b>Superintendent</b>                    | Reviews the risk register with cabinet, sets how much risk the district will accept and carries top risks into budget and insurance decisions. |
| <b>Procurement and contracts lead</b>    | Makes sure software, cloud services and suppliers pass a security and privacy review, with a signed agreement, before purchase.                |

### Insurance relevance · High

Carriers commonly scan an applicant's internet-facing systems before quoting and ask how often you scan, how fast you patch and whether you assess risk on a schedule. Exposed remote access or known exploited vulnerabilities can lead to follow-up questions or conditions at renewal.

- Do you scan internet-facing and internal systems for vulnerabilities, and how often?
- How quickly are critical patches applied, and how much faster for actively exploited vulnerabilities?
- Do you complete a formal cybersecurity risk assessment at least annually and track the gaps it finds?
- When did you last restore a critical system from backup, and was the result documented?

Tip: Review your latest CISA Cyber Hygiene or other external scan before submitting, so your answers match what the carrier's own scan will show.

## Funding and free help

### GaDOE/GTA statewide security rating platform (Bitsight)

Launched 2022 · 2026 status unverified

GaDOE funded licenses for an external security rating and monitoring platform for every Georgia school district at no cost to districts, showing external vulnerabilities and a security scorecard.

### CISA Cyber Hygiene Services (vulnerability and web application scanning)

Rolling enrollment

Free, continuous external vulnerability scanning of a district's public IP addresses with weekly reports and urgent alerts; optional web application scanning is also free.

**CISA K-12 cybersecurity resources and toolkit**

Always available

Free federal guidance for K-12: the K-12 cybersecurity report and toolkit, plus access to regional CISA advisors and no-cost services. A resource, not funding.

Programs, eligibility and deadlines change; confirm on the official page before applying.

**Learn more**

- Cyber Hygiene Services (CISA) <https://www.cisa.gov/cyber-hygiene-services>
- Known Exploited Vulnerabilities Catalog (CISA) <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
- Multi-State Information Sharing and Analysis Center (MS-ISAC) (CIS) <https://www.cisecurity.org/ms-isac>
- The K12 SIX Essentials Series (K12 SIX) <https://www.k12six.org/essentials-series>
- No-Cost Cybersecurity Services and Tools (CISA)  
<https://www.cisa.gov/resources-tools/resources/no-cost-cybersecurity-services-and-tools>