

Risk Management Strategy

This category asks whether the district has decided which cyber risks matter most, how much risk leadership will accept, and how those decisions get made and communicated — instead of treating every...

Why it matters

- A small technology team will always have more open issues than time. A written, scored risk register lets the superintendent and technology director agree on what gets fixed first, so untested backups or staff accounts without multi-factor authentication (MFA) are not pushed aside by the newest urgent ticket.
- When the district decides not to fund a fix, a signed risk acceptance with a revisit date shows leadership made an informed choice. Without it, the technology director carries the blame for a decision that was never theirs, and the board first hears about the risk after an incident.
- Ranked risks give budget requests, grant applications and E-Rate planning a clear rationale. A request that points to a specific risk with a named owner is easier for the business office and board to approve than a list of products.

A one-to-five-person shop cannot fix everything, so an unwritten strategy means the loudest issue wins while untested backups or exposed remote access wait. Documented risk decisions also protect the technology director when leadership declines to fund a fix, and underwriters commonly ask how risk is assessed and prioritized before quoting coverage.

What good looks like at each level

Level	What you would see	Artifacts that show it
1 · Initial	<p>Risks are handled as they surface. There is no agreed list of top risks, no statement of how much risk leadership will accept, and technology spending follows vendor pitches, breakdowns or the last incident.</p> <p>Moving up: Start defining risk priorities, tolerances, and assumptions — even a rough top-10 register and draft tolerance statements — and begin using them for operational decisions instead of reacting incident by incident.</p>	<ul style="list-style-type: none"> • No risk register; known gaps live in the technology director's notes or memory • Purchases and projects with no documented link to a risk they reduce • No record of any decision to accept a risk, even where leadership declined funding
2 · Repeatable	<p>A first risk register and draft tolerance statements exist and are starting to guide decisions, such as finishing multi-factor authentication (MFA) rollout before a new device purchase. The process is still being built and depends on one or two people.</p> <p>Moving up: Document the risk process and get stakeholder sign-off: cybersecurity risk objectives and outcomes, defined supply chain risk processes, tracked action plans that disseminate risks to stakeholders, and a written communication plan.</p>	<ul style="list-style-type: none"> • Spreadsheet register with likelihood and impact scores, updated irregularly • Draft risk tolerance statements not yet signed by the superintendent • Risk discussions in cabinet notes, usually right after an incident or insurance renewal
3 · Defined	<p>The risk process is written down and agreed to by cabinet: how risks are scored, who owns them, how vendor risks enter the register and who is told what. Action plans are tracked, and accepting a risk is a signed decision.</p> <p>Moving up: Make the strategy cultural: staff beyond IT know the desired response patterns, and stakeholders visibly commit to tracking changing threat tactics through briefings, drills, and cross-department participation.</p>	<ul style="list-style-type: none"> • Risk register with owners, next actions and due dates, including vendor and supply chain risks • Signed risk tolerance statements and risk acceptance memos with revisit dates • One-page communication plan naming who briefs the board, how often, and how principals and department heads hear about new risks
4 · Managed	<p>Staff beyond IT understand the district's risk priorities and the expected response. Principals, the business office and HR know what to do with a suspicious payment request or a vendor breach notice, and new threat advisories show up in the register.</p> <p>Moving up: Deploy the strategy without significant gaps across every school and department, and share processes and lessons learned with the K12 community through K12 SIX, state associations, or regional consortia.</p>	<ul style="list-style-type: none"> • Register updates traced to K12 SIX or Multi-State Information Sharing and Analysis Center (MS-ISAC) advisories • Department heads presenting their own risk items at quarterly reviews • Staff briefings or drills that walk through expected responses, with attendance records

Level	What you would see	Artifacts that show it
5 · Optimized	The strategy is applied consistently in every school and department, with no significant gaps found in the annual check. The district shares its risk process and lessons learned with other districts through K12 SIX, state associations or its Regional Educational Service Agency (RESA).	<ul style="list-style-type: none"> Annual verification that every school and department is covered by the register and its action plans Lessons from incidents and exercises written back into the strategy Templates, presentations or after-action summaries shared with peer districts

Quick wins

Quick win and how	Cost	Effort	Usual owner
Start a 10-row risk register in a spreadsheet today Create columns for risk, affected systems, likelihood (1 to 5), impact (1 to 5), owner, next action and due date. Seed it with known gaps such as accounts without MFA, restores never tested, unsupported servers, shared admin passwords and vendors without agreements.	Free	Hours	Technology director
Draft three risk tolerance statements and get superintendent sign-off Have the technology director draft short plain-language statements, for example 'no account with access to student records operates without MFA' and 'student data leaves district systems only under a signed agreement'. Review them with the business official, then sign and file them with the register.	Free	Days	Superintendent
Document one known accepted risk in a signed memo this quarter Pick a gap leadership has already declined to fund, such as an unsupported server kept for a legacy application, and write a half-page memo covering the risk, what could happen, the cost to fix and a revisit date. Have the superintendent sign it and file it with the register.	Free	Hours	Technology director
Add cyber risk as a standing item on the existing safety or ERM committee agenda Ask the chair of the school safety committee or the enterprise risk management (ERM) group to add a quarterly cyber risk item, and have the technology director bring the top five register entries each time. This keeps cyber risk next to physical safety and insurance decisions instead of in a separate IT meeting.	Free	Hours	Superintendent
Download the free K12 SIX Essential Cybersecurity Protections as your prioritization baseline Download the Essentials from the K12 SIX website and mark each protection as in place, partial or missing. Add every missing protection to the register as a risk with an owner, which gives the register a school-specific starting point.	Free	Hours	Information security lead

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

Common pitfalls

- Scoring every risk as high. When everything is urgent nothing gets sequenced; force a ranking and limit the top tier to what the team can actually work on this quarter.
- Keeping the register as a private IT document. If the superintendent and business official never see it, they cannot accept risks or fund fixes, so review it with them on a set schedule and record the decisions.
- Accepting risks by silence. A fix that is never funded is still an accepted risk, only an undocumented one; write a short acceptance memo with a revisit date so the decision is visible and comes back up.
- Running vendor risk in a separate spreadsheet. A breach at the SIS vendor or an expired data privacy agreement is a district risk, so keep vendor risks in the same register where they compete for attention on equal terms.
- Writing a strategy that never changes. Threats and district systems shift every year; update the register when advisories, incidents, audits or new systems arrive, not only at the annual review.

Evidence that proves it

- Risk register with likelihood/impact scores, owners, and next actions
- Superintendent-signed risk tolerance statements
- Signed risk acceptance memos with revisit dates
- Quarterly risk review meeting notes with the superintendent and business official
- One-page cyber risk communication plan
- Board briefing materials summarizing top cyber risks
- Register entries mapped to the K12 SIX Essential Protections or Cybersecurity Rubric categories

Who usually owns it

Technology director	Maintains the risk register, scores and ranks risks, and tracks action plans to completion.
Superintendent	Approves risk priorities and tolerance statements and signs risk acceptance decisions.
Business and finance officer	Joins quarterly risk reviews and lines up budget requests and insurance coverage with the ranked risks.
School board	Receives regular briefings on top risks and supports the risk tolerance the superintendent sets.

Insurance relevance · Medium

Underwriters want evidence that the district assesses risk on a schedule and acts on the results, not only that a strategy document exists. Renewal questionnaires often ask when the last risk assessment happened and how its gaps are tracked to closure.

- Have you completed a formal cybersecurity risk assessment in the past year, and who performed it?
- How do you prioritize and track remediation of the gaps the assessment found?
- Has leadership reviewed and approved the district's cyber risk priorities?
- Are there known security gaps you have chosen not to address, and why?

Tip: Give the date and scope of your most recent assessment exactly as recorded, and be ready to show the register entries that track its findings.

Funding and free help

State and Local Cybersecurity Grant Program (SLCGP) — Georgia subawards

Georgia FY2024 round closed May 15, 2026 · watch for the FY2025 round

Federal cyber grant passed through the state to local governments, including school districts. Georgia accepted FY2024 subaward applications April 1 – May 15, 2026. Federal authority beyond September 30, 2026 depends on Congress.

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

- Cybersecurity Framework (NIST) <https://www.nist.gov/cyberframework>
- CSF 2.0 Quick-Start Guides (NIST) <https://www.nist.gov/cyberframework/quick-start-guides>
- The K12 SIX Essentials Series (K12 SIX) <https://www.k12six.org/essentials-series>
- Cross-Sector Cybersecurity Performance Goals (CISA) <https://www.cisa.gov/cross-sector-cybersecurity-performance-goals>

- Protecting Our Future: Partnering to Safeguard K-12 Organizations from Cybersecurity Threats (CISA)
<https://www.cisa.gov/resources-tools/resources/report-partnering-safeguard-k-12-organizations-cybersecurity-threats>