

Oversight

This category asks whether leadership checks that the security program is working — on a schedule, with measures — rather than approving documents once and moving on.

Why it matters

- Security programs drift quietly: multi-factor authentication (MFA) exceptions pile up, a backup job fails without anyone noticing, and training lapses for new hires. Regular review of a few measures catches that drift before an incident, audit or insurance claim exposes it.
- The superintendent and board answer for a risk that can close schools, disrupt state testing windows and delay payroll. Scheduled briefings with real measures give them a basis for decisions and a record that they exercised oversight.
- Trend data from annual self-assessments and outside reviews makes budget conversations concrete. Showing that a funded control moved a score, or that a finding stayed open for a year, is more persuasive to a board than general concern.

Programs drift: MFA exceptions accumulate, policies age, and training lapses, until an incident, audit finding, or denied insurance claim reveals the gap. Regular review of outcomes and metrics is also how superintendents and boards discharge their duty over a risk that can close schools for weeks.

What good looks like at each level

Level	What you would see	Artifacts that show it
1 · Initial	<p>Policies and plans were approved once, if at all, and no one checks whether they are still followed. Leadership hears about cybersecurity mainly when something breaks.</p> <p>Moving up: Put executive leadership formally in the approval chain and establish at least annual review of cybersecurity documentation and risk management outcomes, adjusting them to cover district requirements and risks.</p>	<ul style="list-style-type: none"> • No cybersecurity item in cabinet or board minutes apart from incidents or purchases • Security documents with no review history • No measures of MFA coverage, patching, backups or training reported to anyone
2 · Repeatable	<p>Executive leadership formally approves security policies and plans, and documentation is reviewed at least once a year. Leadership looks at outcomes such as incidents and audit findings and adjusts priorities, though without consistent measures.</p> <p>Moving up: Start measuring program performance — a metrics dashboard reviewed on a schedule — and use the results to adjust strategic direction, while moving key document reviews from annual to quarterly.</p>	<ul style="list-style-type: none"> • Signed approval or cabinet minutes for each security policy and plan • Annual documentation review notes • Year-end summary of incidents, findings and changes made
3 · Defined	<p>A short set of measures is reviewed with the superintendent on a schedule, and the results change priorities. Key documents are reviewed each quarter and every review is logged.</p> <p>Moving up: Verify governance against every applicable federal, state, and local regulation using a compliance matrix with evidence, and close the gaps you find.</p>	<ul style="list-style-type: none"> • One-page dashboard covering MFA coverage, patch status, restore test results, training completion, phishing reports and open findings • Quarterly document review log with owners and next-review dates • Corrective-action log showing findings assigned, dated and verified closed

Level	What you would see	Artifacts that show it
4 · Managed	<p>The district can show, requirement by requirement, how its governance meets federal, state and local rules, with evidence linked for each. Gaps found in the compliance review are tracked and closed.</p> <p>Moving up: Add an annual independent review by an outside party — a third-party assessment, audit, or penetration-test-backed evaluation — and act on its findings.</p>	<ul style="list-style-type: none"> Compliance matrix covering the Family Educational Rights and Privacy Act (FERPA), Children's Internet Protection Act (CIPA) certification, the Children's Online Privacy Protection Act (COPPA), the Protection of Pupil Rights Amendment (PPRA), Georgia student data privacy requirements and breach notification, with evidence links Annual board briefing on performance and compliance, with sensitive details handled as counsel advises Year-over-year self-assessment results kept and compared
5 · Optimized	<p>An independent outside party reviews the cybersecurity program every year, and its findings flow into the corrective-action log with owners and deadlines. Leadership reports progress on those findings to the board.</p>	<ul style="list-style-type: none"> Annual independent assessment or audit report stating its scope and methods Penetration test or external vulnerability scan results included in the review Board minutes showing review of the independent findings and the status of corrective actions

Quick wins

Quick win and how	Cost	Effort	Usual owner
<p>Assemble a one-page metrics dashboard from Google/Microsoft admin, filter, and backup consoles</p> <p>Pull MFA enrollment from the Google Admin console or Microsoft Entra admin center, the last successful backup and restore test from the backup console, filter and phishing-report data, training completion from HR, and open findings from the corrective-action log. Keep the same six to eight measures every time so trends are visible.</p>	Free	Days	Technology director
<p>Add a standing 15-minute cybersecurity slot to the monthly cabinet agenda</p> <p>Add the item to the cabinet agenda template, have the technology director walk through the dashboard and any decisions needed, and record decisions in the minutes so oversight is documented.</p>	Free	Hours	Superintendent
<p>Enroll in CISA's free Cyber Hygiene vulnerability scanning service</p> <p>Email the Cybersecurity and Infrastructure Security Agency (CISA) at vulnerability@cisa.dhs.gov to request Cyber Hygiene services, then sign the service agreement and list the district's public IP addresses and domains. Reports arrive by email; add critical findings to the corrective-action log.</p>	Free	Days	Network and systems administrator
<p>Create the document review log with next-review dates</p> <p>In a shared spreadsheet, list every governance document (policies, procedures, incident response plan, continuity plan, vendor contract template) with owner, last review, next review and notes. Sort by next review date and check it at each monthly cabinet slot.</p>	Free	Hours	Technology director
<p>Put the annual Cybersecurity Rubric self-assessment on the calendar with a named owner</p> <p>Pick a fixed month ahead of budget planning, name the technology director as owner with cabinet members taking part, and keep each year's results so the board and the insurer can see the trend.</p>	Free	Hours	Technology director

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

Common pitfalls

- Reporting activity instead of outcomes. Counts of tickets closed or emails filtered say little about risk; report measures tied to risk, such as MFA coverage, restore test results and how long critical findings stay open.
- Treating document approval as oversight. Signing a policy once does not show it is followed, so pair each approval with a scheduled check that the control is still in place.
- Briefing the board only after an incident. A board that first hears about cybersecurity during a crisis cannot make informed decisions; schedule at least an annual briefing and handle sensitive details as counsel advises under open-meetings and records law.
- Logging findings without verifying closure. A corrective-action log full of items marked done but never rechecked gives false comfort; have someone other than the person who made the fix confirm closure of high-priority findings.
- Waiting for budget before seeking outside review. Free Cybersecurity and Infrastructure Security Agency (CISA) scanning and state or risk-pool assessment programs give independent findings now; add a paid assessment or penetration test as funding allows.

Evidence that proves it

- Quarterly cybersecurity dashboard and cabinet report
- Board minutes showing at least annual cybersecurity briefings
- Document review log with owners and next-review dates
- Annual Cybersecurity Rubric self-assessment results showing year-over-year trend
- Compliance matrix with linked evidence for CIPA, FERPA, and state laws
- Independent assessment or penetration test report
- Corrective-action log showing findings tracked to closure

Who usually owns it

Superintendent	Reviews performance reports, adjusts priorities and delivers the cybersecurity briefing to the board.
Technology director	Builds the dashboard, maintains the review and corrective-action logs and coordinates outside assessments.
School board	Receives regular briefings, asks about trends and open findings, and supports funding for independent review.
Business and finance officer	Keeps compliance evidence for federal program certifications and aligns oversight findings with audit and insurance needs.

Insurance relevance · Medium

Underwriters look for signs that leadership actually monitors the program: regular reporting to the superintendent and board, vulnerability scanning, and outside testing. At renewal, these answers may be checked against scan reports or assessment summaries.

- Does the person responsible for security report to senior leadership and the board on a regular schedule?
- Do you scan internet-facing systems for vulnerabilities, and how often?
- Has an outside party performed a security assessment or penetration test recently, and were critical findings fixed?
- How do you track remediation of findings from audits and assessments?

Tip: State scan and assessment frequencies that match your logs, and attach the latest report summary if the carrier accepts supporting documents.

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

- Cyber Hygiene Services (CISA) <https://www.cisa.gov/cyber-hygiene-services>
- No-Cost Cybersecurity Services and Tools (CISA) <https://www.cisa.gov/resources-tools/resources/no-cost-cybersecurity-services-and-tools>
- Cross-Sector Cybersecurity Performance Goals (CISA) <https://www.cisa.gov/cross-sector-cybersecurity-performance-goals>
- Cybersecurity Framework (NIST) <https://www.nist.gov/cyberframework>
- Cybersecurity Rubric (CR) (CoSN) <https://www.cosn.org/cybersecurity-rubric/>