

Organizational Context

This category asks whether the district understands its own operating reality: the teaching-and-learning mission cybersecurity exists to protect, the legal obligations it carries (FERPA, CIPA, COPPA, state privacy...

Why it matters

- When ransomware or an outage hits, the first question is which systems come back first. A district that has already ranked its student information system (SIS), identity platform, payroll and transportation routing can restore in a sensible order instead of debating it while buses, lunch lines and attendance wait.
- Obligations under the Family Educational Rights and Privacy Act (FERPA), the Children's Online Privacy Protection Act (COPPA) and Georgia's student data privacy law follow student data to every app and vendor. If no one has mapped which vendor holds which records under which agreement, a single vendor breach notice turns into days of searching contracts while families and reporters ask questions.
- The board, state auditors and the cyber insurance application all ask, in different words, what the district runs on and what data it holds. A written picture kept current means those answers are consistent and defensible instead of rebuilt from memory each time someone asks.

It is the foundation the rest of the rubric builds on — you cannot prioritize defenses for systems and data you have never named. The stakes are concrete: unvetted apps leaking student data, a missing data-sharing agreement surfacing during a breach investigation or state audit, and a board that learns which systems matter only when ransomware takes them down.

What good looks like at each level

Level	What you would see	Artifacts that show it
1 · Initial	<p>The district's systems, data and legal obligations live in people's heads. Teachers sign up for apps on their own, vendor data terms are whatever the click-through said, and technology plans do not mention cyber risk.</p> <p>Moving up: Move from handshakes to writing: get contractual data-sharing agreements in place with your highest-risk vendors (SIS and LMS first) and make operational processes and responsibilities consistent, even if still mostly reactive.</p>	<ul style="list-style-type: none"> • No list of critical systems; asking which systems hold student data gets different answers from different people • Edtech vendors in use without signed data privacy agreements (DPAs), or agreements no one can locate • Technology plan and budget requests with no section on cybersecurity risks or priorities
2 · Repeatable	<p>Key people know the main systems and handle data in roughly the same way each time, but the work is reactive. The largest vendors have signed agreements while smaller apps and older contracts do not, and no one checks whether data-handling rules are followed.</p> <p>Moving up: Document risk mitigation operations, bring every third-party data-sharing agreement up to legal and regulatory requirements, and start measuring and enforcing sensitive-data handling; put cybersecurity roles into the strategic plan so risk decisions trace to mission and contracts.</p>	<ul style="list-style-type: none"> • Signed data privacy agreements (DPAs) for the SIS and learning management system (LMS), with gaps for supplemental and teacher-adopted apps • A partial systems list, often built for an insurance application or E-Rate filing and not maintained since • Data-handling expectations in the staff handbook with no spot checks or follow-up
3 · Defined	<p>The district keeps a current critical-systems list, an obligations map with named owners, and a signed agreement that meets legal requirements for every vendor that receives student or staff data. Sensitive-data rules are written, checked and enforced, and the strategic plan names who is responsible for cybersecurity.</p> <p>Moving up: Add department-level performance controls, make resiliency — anticipate, prepare, recover — a funded priority, and run regular assessments so strategic planning and budget requests are driven by needs-assessment data rather than anecdote.</p>	<ul style="list-style-type: none"> • Critical-systems and data inventory listing vendor, data types, owner and restore priority for each system • Data privacy agreement (DPA) registry showing a current signed agreement for every approved app that handles student data, published as the approved-apps list • Strategic or technology plan section naming cybersecurity roles, plus records of periodic checks such as a sharing-settings review of student folders in Google Drive or OneDrive

Level	What you would see	Artifacts that show it
4 · Managed	<p>Departments such as finance, nutrition, transportation and special education track risk for their own systems and data, and resilience (backups, continuity plans, downtime procedures) is funded as a priority. Regular assessments feed directly into strategic planning and budget requests.</p> <p>Moving up: Close the loop: strategic plans actively drive roles and risk decisions, controls are demonstrably effective and responsive, and assessments are refined through organization-wide analysis of results.</p>	<ul style="list-style-type: none"> • Department-level risk or control scorecards reviewed at cabinet • Funded resilience items such as protected offline or immutable backups and written downtime procedures for the SIS, food service point of sale and transportation routing • Budget narrative that cites assessment findings, such as this rubric's results, as the reason for each cybersecurity request
5 · Optimized	<p>Cybersecurity is a normal part of how the district plans: each strategic plan update visibly shapes roles and risk decisions, and controls are adjusted promptly when systems, laws or threats change. The assessment approach itself is refined each year from a district-wide look at results.</p>	<ul style="list-style-type: none"> • Strategic plan updates that show how cybersecurity roles and risk decisions changed as a result • Multi-year trend of assessment results across departments, with documented changes to how the assessment is run • New systems, programs and laws triggering an update to the inventory and obligations map before launch, with records to show it

Quick wins

Quick win and how	Cost	Effort	Usual owner
<p>Draft the top-10 critical-systems list in a spreadsheet this week</p> <p>Give each system one row with columns for vendor, data held, business owner, vendor support contact and how long schools can run without it. Pull candidates from accounts payable and the single sign-on dashboard so nothing obvious is missed, then have each business owner confirm their row.</p>	Free	Hours	Technology director
<p>Join your state SDPC alliance and adopt the NDPA for new edtech contracts</p> <p>Sign up through your state's Student Data Privacy Consortium (SDPC) alliance, or the national SDPC if your state has none, and confirm any membership fee first. Use the National Data Privacy Agreement (NDPA) as the standard agreement for new edtech purchases, and search the SDPC registry for vendors that have already signed one you can join.</p>	Low cost	Days	Data privacy officer
<p>Assign one named owner to each legal obligation in a single cabinet meeting</p> <p>Bring a one-page table listing the Family Educational Rights and Privacy Act (FERPA), the Protection of Pupil Rights Amendment (PPRA), the Children's Online Privacy Protection Act (COPPA), the Children's Internet Protection Act (CIPA), Georgia's student data privacy law and breach notification duties, with the owner column blank. Fill in a name for each at the meeting and record the assignments in the minutes.</p>	Free	Hours	Superintendent
<p>Publish the approved-apps list so teachers stop adopting unvetted tools</p> <p>Post the apps that have signed agreements on the staff intranet or a shared Google Site, with grade bands and approved uses, plus a short request form for anything not listed. Ask principals to point teachers to it at the next staff meeting so it becomes the first stop for new tools.</p>	Free	Days	Curriculum and instruction lead
<p>Add a standing cybersecurity item to the cabinet agenda</p> <p>Add a recurring ten-minute item to the cabinet agenda template. Have the technology director bring the same three things each time: changes to critical systems, new vendors or data-sharing requests, and any open risk that needs a decision.</p>	Free	Hours	Superintendent

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

Common pitfalls

- Listing systems without listing the data. An inventory that says 'transportation software' but not that it holds home addresses and medical notes misses why it matters; record data types for each system, because they drive both notification exposure and restore priority.
- Treating click-through terms as a data privacy agreement. Free apps adopted by teachers often carry terms allowing data uses the district would never sign; route every app that collects student data through the agreement process, including free ones.
- Building the inventory once for an insurance application or audit and never touching it again. New systems arrive every year through grants, state requirements and curriculum adoptions, so tie inventory updates to purchase approval and the start-of-year checklist.
- Leaving building systems out of scope. Door access, cameras, HVAC controls, phone systems and cafeteria point of sale are network-connected and keep schools open; include them and note which vendors have remote access to each.
- Keeping the obligations map inside the technology department. Family Educational Rights and Privacy Act (FERPA) requests, Protection of Pupil Rights Amendment (PPRA) survey consent and Children's Internet Protection Act (CIPA) certification are handled by student services, curriculum and the E-Rate filer, so give each obligation an owner who does the work, with IT supporting.

Evidence that proves it

- Critical-systems and dependencies list with vendor, data types, and owner for each
- Compliance matrix mapping FERPA, CIPA, COPPA, PPRA, and state privacy laws to named owners
- Signed data privacy agreements (SDPC NDPA) and a published approved-apps registry
- Superintendent-signed statement tying cybersecurity to instructional continuity
- Technology plan or strategic plan section naming cybersecurity roles and priorities
- Cabinet or board minutes showing annual review of systems and obligations
- Completed cyber insurance application reflecting an accurate system inventory

Who usually owns it

Technology director	Maintains the critical-systems and data inventory and keeps it current as systems are added or retired.
Superintendent	Ties cybersecurity to instructional continuity, assigns an owner to each legal obligation and puts cybersecurity roles into the strategic plan.
Data privacy officer	Runs the data privacy agreement process and the approved-apps list and tracks student privacy obligations.
Business and finance officer	Makes sure contracts and purchase orders capture data terms and supplies vendor and spending records for the inventory.

Insurance relevance · Medium

Carriers use this area mainly to size the district's exposure rather than to test controls: applications ask what kinds of sensitive records the district holds, roughly how many, and which outside providers run critical systems. An accurate inventory makes those answers quick and consistent with what a forensic firm would find after an incident.

- What types of personal information do you store, such as student records, Social Security numbers, health information or payment data, and about how many records?
- Which critical systems are hosted by outside providers and which run on district servers?
- Do you know where sensitive data is stored and who can access it?
- Do you have written agreements with the vendors that receive student or staff data?

Tip: Take record counts and data types straight from the inventory, and keep a copy of the version you used alongside the submitted application.

Funding and free help

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>
- Protecting Student Privacy (U.S. Department of Education) <https://studentprivacy.ed.gov/>
- Student Data Privacy Consortium (SDPC) (Access 4 Learning Community) <https://privacy.a4l.org/>
- Cybersecurity Rubric (CR) (CoSN) <https://www.cosn.org/cybersecurity-rubric/>
- 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>