

Improvement

Improvement asks whether the district actually learns — from incidents, outages, drills, audits, and self-assessments — and folds those lessons back into its response and recovery plans.

Why it matters

- Without a lessons-learned step, the same weakness causes the next outage: the same unmonitored circuit, the same phishing lure, the same missing phone list. A short review after each event turns it into one or two concrete fixes.
- A plan nobody has rehearsed fails on details such as who calls the carrier's breach hotline, who can approve emergency spending and how to reach families when district email is down. A tabletop exercise finds those gaps in a conference room instead of during an incident.
- Carriers ask whether the incident response plan was exercised in the past year and whether lessons were folded back in. A corrective-action list and a short annual board report give you evidence for that answer and keep leadership and budget behind the program.

Without that loop, the same phishing technique works twice and the incident response plan is stale the day servers get encrypted. It is also exactly what underwriters probe when they ask whether your IR plan is 'tested and maintained,' and it is what turns a bad incident into a documented recovery story instead of an audit finding.

What good looks like at each level

Level	What you would see	Artifacts that show it
1 · Initial	Service gets restored after outages and incidents, and then everyone moves on. There is little recovery capacity, and response and recovery planning is not coordinated across departments. Moving up: Secure visible leadership commitment and a budget line for recovery capability, and start capturing what went wrong after every incident or outage instead of just restoring service and moving on.	<ul style="list-style-type: none"> • No written record of what went wrong in past outages or incidents • No incident response plan, or a template plan that no one outside IT has read • No tabletop exercise or drill has been held
2 · Repeatable	Leaders have committed to improving recovery and money is starting to follow. The district captures notes after outages and has begun building a recovery plan, though capacity is still limited. Moving up: Make retrospectives routine: analyze restoration actions after each incident, hold lessons-learned sessions, and actually update response and recovery strategies based on what you found — the update is what earns Level 3.	<ul style="list-style-type: none"> • Short incident notes captured after major outages • Budget line or grant request for recovery capability, such as backup storage or plan development • Named lead for developing the incident response and recovery plan
3 · Defined	After every significant incident or outage the district reviews what it did to restore service, records lessons learned and updates its response and recovery plans. The update is the step that counts. Moving up: Evaluate incident response performance against expectations, feed identified challenges into the district's strategic and technology plans, and get stakeholders beyond IT to own the response and recovery plan.	<ul style="list-style-type: none"> • After-action reports on a standard template for incidents and major outages • Plan revision history showing changes made after a specific exercise or incident • Corrective-action tracker with owners and target dates
4 · Managed	Departments beyond IT own their parts of the response and recovery plan. The district evaluates how it performed against the plan and carries the gaps into strategic and technology plans. Moving up: Capture metrics — time to detect, time to restore, corrective actions closed — and let them drive improvement; use advanced tooling to support recovery and continuously optimize incident response, business continuity, and disaster recovery planning.	<ul style="list-style-type: none"> • Tabletop attendance that includes the superintendent, business office, communications, principals, transportation and nutrition • Post-exercise evaluation comparing what happened with what the plan expected • Strategic or technology plan items that trace back to exercise or incident findings

Level	What you would see	Artifacts that show it
5 · Optimized	Response and recovery are measured and improved continuously. Metrics drive decisions, recovery tools speed restoration, and incident response, business continuity and disaster recovery plans are exercised together.	<ul style="list-style-type: none"> Metrics reviewed on a schedule: time to detect, time to restore critical systems, corrective actions closed on time Recovery tooling, such as automated or orchestrated restores, tested against recovery time targets Integrated incident response, continuity and disaster recovery plans with a joint exercise record

Quick wins

Quick win and how	Cost	Effort	Usual owner
Schedule one tabletop this quarter using CISA's free exercise packages or K12 SIX materials Pick a ransomware scenario from the Tabletop Exercise Packages from the Cybersecurity and Infrastructure Security Agency (CISA) or ask your regional CISA cybersecurity advisor for help, and book 90 minutes with the superintendent, business officer, communications director, a principal, and the transportation and nutrition leads. Bring the insurance policy and carrier hotline number, and record every decision and gap.	Free	Weeks	Technology director
Add a 15-minute lessons-learned step to the close of every major outage or incident Add a closing checklist to the ticket template for major outages and incidents with five questions: what happened, what worked, what didn't, what will change, and who owns each change by when. Do not close the ticket until the answers are filled in.	Free	Hours	Help desk
Put the incident response plan on the calendar for annual review with a named owner Name the plan owner in writing, add a version table to the plan's first page, and set a recurring calendar review before the school year starts, plus a review after every exercise or real incident. Have cabinet sign off on each reviewed version.	Free	Hours	Superintendent
Start a corrective-action list in your ticket system and triage it monthly Create a ticket category for corrective actions with fields for source (tabletop, incident, audit, rubric self-assessment, insurance questionnaire), owner and due date. Review open items for 30 minutes each month and report open and closed counts to cabinet.	Free	Hours	Technology director

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

Common pitfalls

- Holding the tabletop with IT only. Ransomware decisions such as closing schools, paying for outside help and notifying families belong to the superintendent, business office, communications and principals; invite them and give each a decision to make during the exercise.
- Writing the after-action report and stopping there. The rubric's Level 3 depends on plans actually changing; turn each finding into a tracked item with an owner and date, then update the plan and note the change in its revision history.
- Waiting for a cyber incident to practice. A fiber cut, an SIS vendor outage or a power failure in the server room exercises the same communication and recovery steps; review those events the same way.
- Keeping the plan only on the network it protects. If the plan, contact list and carrier hotline number live only on a file server or in district email, they may be out of reach during an incident; keep printed and offline copies with key leaders.
- Running reviews that assign blame. Staff who expect blame for clicking a link or missing an alert report late; keep reviews focused on process and fixes, not on people.

Evidence that proves it

- After-action reports from incidents and major outages with tracked action items
- Tabletop exercise agenda, attendance list, and findings from the past year
- Incident response plan with version history and annual review dates
- Corrective-action tracker showing items opened, owned, and closed
- Year-over-year rubric or self-assessment results showing movement
- Board or cabinet presentation summarizing cybersecurity improvements

Who usually owns it

Technology director	Facilitates after-action reviews and exercises, maintains the corrective-action list and keeps response and recovery plans current.
Superintendent	Requires cross-department participation, evaluates response performance and carries improvement needs into strategic plans and budgets.
Emergency management lead	Connects cyber exercises with the district's school safety and continuity planning so the same command structure and family notification steps apply.
Communications director	Keeps staff, family and media message templates in the plan and tests backup communication channels during exercises.

Insurance relevance · Medium

Applications usually ask whether the incident response plan exists, has been exercised in the past year and has been updated from lessons learned. Carriers and their breach response teams look for a plan that names who calls the carrier's hotline first.

- Have you exercised your incident response plan in the past 12 months through a tabletop or live drill?
- Were lessons learned from the exercise or from real incidents incorporated into the plan?
- Who maintains the plan, and when was it last reviewed?

Tip: Keep the tabletop agenda, attendance list, after-action report and the plan's revision history together, so a yes on the application points to dated evidence.

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

- CISA Tabletop Exercise Packages (CISA) <https://www.cisa.gov/resources-tools/services/cisa-tabletop-exercise-packages>
- SP 800-61 Rev. 3, Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile (NIST) <https://csrc.nist.gov/pubs/sp/800/61/r3/final>
- SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems (NIST) <https://csrc.nist.gov/pubs/sp/800/34/r1/upd1/final>
- 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>
- The K12 SIX Essentials Series (K12 SIX) <https://www.k12six.org/essentials-series>