

Readiness Check

Data Protection & Recovery Checklist

Practical steps to strengthen
resilience and reduce downtime
across your organization.



January 2026

Introduction



When public sector systems go down - whether from ransomware, a storm, or a simple system failure - the ripple effects reach far beyond IT. Licensing stops. Payroll pauses. Constituents lose access to essential services.

Technology is only as powerful as the visibility and confidence behind it. With the right tools and clear practices, agencies can protect, recover, and continue delivering critical services no matter what happens.

This checklist helps your organization identify where protection is strong and where small improvements can have an outsized impact. It's not about being perfect. It's about being prepared.

How to Use This Checklist

Use this tool to assess how well your organization can protect, recover, and continue operations when systems are compromised or disrupted.

For each item, mark:

- Yes – Fully implemented and verified.
- Partial – Some elements in place. Note what's covered and what's missing.
- No – Not yet implemented. Note follow-up actions to prioritize.

The goal isn't perfection; it's visibility. Knowing where you're strong, where you're improving, and where small changes could have a big impact.

Checklist

1. Backup & Recovery Foundations

Goal: Ensure your most important data can be recovered quickly and completely.

Question	Yes	Partial	No	Notes
Do you maintain verified backups for all mission-critical systems?				
Are backups stored separately from live environments (on-prem or cloud)?				
Do you test your recovery process on a regular schedule?				
Are any backups immutable (cannot be changed or deleted)?				

Tip: Immutable, isolated backups act as a guaranteed “clean copy” after ransomware or accidental deletion.

2. Cyber Resilience & Protection

Goal: Strengthen defenses against ransomware and data-layer attacks.

Question	Yes	Partial	No	Notes
Do you maintain verified backups for all mission-critical systems?				
Are backups stored separately from live environments (on-prem or cloud)?				
Do you test your recovery process on a regular schedule?				
Are any backups immutable (cannot be changed or deleted)?				

Tip: Detecting anomalies within the data layer itself gives IT teams an early warning, catching threats before they spread.

Checklist

3. Storage Optimization & Cost Efficiency

Goal: Store data smartly — securely, efficiently, and affordably.

Question	Yes	Partial	No	Notes
Do you automatically tier data based on use (hot, warm, cold)?				
Do you know which data can be archived or safely deleted?				
Can you track storage costs by department, workload, or project?				

Tip: Tiering keeps high-value “hot” data accessible while shifting “cold” archives to lower-cost storage, reducing costs and improving performance.

4. Continuity & Automation

Goal: Reduce manual effort and keep essential services online during disruptions.

Question	Yes	Partial	No	Notes
Are backups, replication, and verification automated across systems?				
Can systems fail over automatically if a data center or service goes offline?				
Do you have a documented recovery playbook for staff to follow under pressure?				

Tip: Automation reduces errors and ensures protection tasks happen even when staff bandwidth is limited.

Checklist

5. Governance & Leadership Confidence

Goal: Build transparency and alignment between IT, leadership, and finance.

Question	Yes	Partial	No	Notes
Do leaders receive regular updates on backup health and recovery readiness?				
Are resilience metrics tied to compliance or audit requirements?				
Have you quantified the cost of downtime or data loss?				

Tip: Reporting recovery readiness in terms of uptime, costs, and audit preparedness helps keep resilience a long-term budget priority.



Scoring Your Results

To interpret your responses:

- Count Yes = 1 point, Partial = 0.5 points, No = 0 points.
- Add your total from all five sections (max score: 15).

Score	Rating	Meaning
13-15	Resilient	Strong recovery readiness and proactive data management. Continue refining automation and analytics.
8-12.5	Developing	Solid foundation with clear opportunities to strengthen visibility and process consistency.
Below 8	Needs Improvement	Critical systems may take longer to recover after an incident. Prioritize automation, isolation, and immutability.

Use this as a snapshot, not a static grade. It's a benchmark for ongoing improvement, not a judgment on where you stand today.



When Every Minute Matters

If this checklist revealed areas for improvement, you're not alone.

Few state, local, or educational organizations are overstaffed or overfunded. Most are doing more with less... and still delivering essential services every day.

But even with limited bandwidth, meaningful progress is possible. It starts with small, strategic steps that improve recovery times, reduce risk, and increase confidence across your organization.

Communicating Your Assessment: Up, Down, In, and Out

Completing this checklist gives you a clearer view of your organization's data protection and recovery posture. Communicating those findings effectively is how you build alignment, secure support, and turn insight into action.

Use the Up, Down, In, Out model to share results with clarity and intention.



UP — Communicating to CXOs & Executive Leadership

Who “up” includes:

- If you’re in IT operations → CXO, county administrator, agency head, and similar roles
- If you’re the CXO (or an IT leader) → department directors, elected officials, or cabinet-level leadership

What leadership needs:

- A clear, plain-language summary of where you stand (e.g., “We can recover core systems, but some backups aren’t verified automatically.”)
- What that actually means in practice (e.g., “This could slow service restoration during an outage if a manual step fails.”)
- Why the gaps matter in terms anyone can understand — not technical risk, but operational impact:
 - Longer service delays
 - Slower response times during emergencies
 - Higher budget impact if downtime extends
 - Reduced public trust if critical services go offline
- Three to five recommended next steps with high-level benefits (e.g., “Automating backup checks could cut restoration time significantly when every minute counts.”)

How to communicate:

- Short and visual (one-page brief, bullets, simple language)
- Focus on constituent outcomes and continuity, not tools or configurations

Why it matters:

Clarity “upward” builds confidence. Leaders invest in what they understand, especially when the risks and benefits are framed in real-world terms.



DOWN — Communicating to Departments & Program Teams

Who “down” includes:

Permitting offices, benefits teams, public safety departments, call centers, field staff, and anyone whose work depends on IT systems.

What they need:

- What the assessment means for their operations (e.g., “Our permitting system relies on a manual backup process, and here’s what that means for workflow reliability.”)
- How potential improvements could stabilize, speed up, or simplify their work
- How their collaboration or awareness plays a role in improvement (data cleanup, workflow changes, scheduling downtime, etc.)
- Clear expectations about timelines and upcoming changes

Why it matters:

Departments experience the real-world impact of outages, like slower processing times, longer lines, delayed cases, frustrated constituents. When they understand “why,” they help accelerate progress instead of resisting it.

How to communicate:

- Use examples tied directly to their daily responsibilities
- Avoid technical terminology; focus on predictability, reliability, and reduced disruption
- Give advanced notice before changes occur



IN — Communicating to Internal Technical & Operational Teams

Who “in” includes:

IT, security, networking, DBAs, app owners, infrastructure teams, operations analysts — the people who execute the work.

What they need:

- A clear breakdown of strengths and gaps (no sugarcoating or jargon)
- The practical implications of the gaps (e.g., “If a failure happens during off-hours, this manual process may extend recovery by several hours.”)
- Prioritization tied to mission impact, not just technical logic
- Defined owners for each improvement area
- A realistic timeline and what’s required to move from “partial” to “strong”

Why it matters:

Technical teams are already stretched thin. Clarity helps them focus on what matters most: Improvements that reduce unnecessary work, speed up recovery, and protect the organization from avoidable trouble.

How to communicate:

- Use existing tools (ticket system, shared dashboards, internal channels)
- Keep communication focused on action, not documentation
- Reinforce how improvements reduce the team’s long-term burden



OUT — Communicating Externally (When Appropriate)

Who “out” includes:

Partner agencies, oversight bodies, key vendors, regional collaboratives, and only when necessary — the public.

What they need (and what they don't):

- High-level awareness of improvements tied to reliability and continuity
- Expected or upcoming changes that may impact shared systems
- Reassurance that resilience improvements are underway
- No exposure of vulnerabilities, weaknesses, system names, or gaps
- No recovery timelines that are speculative or technical in nature

Plain-language examples:

- “We’re strengthening backup and recovery processes to improve service reliability.”
- “We’re modernizing some behind-the-scenes systems to reduce the risk of downtime.”

Why it matters:

External communication should reinforce trust, not reveal operational risk. The goal is confidence, not transparency for transparency’s sake.

How to communicate:

- Keep it extremely high-level
- Use existing public communication channels (status pages, scheduled updates)
- Default to “less is more”

Resilience starts here.

Explore the Public Sector Playbook for Data Resilience

Learn how to build on this checklist with a step-by-step framework for assessing risk, prioritizing data, and implementing resilience at scale, designed specifically for the public sector.



January 2026