Hitachi Vantara

Defending Public Trust

Building Cyber-Resilient Data Foundations for State and Local Government

Introduction

Technology as Public Infrastructure

At their core, state and local governments are service providers. But now, as operators of critical infrastructure, they are increasingly held to regulatory standards for how that infrastructure is governed and secured.

From water treatment facilities and transportation systems to law enforcement databases and public health platforms, government agencies now depend on digital systems to deliver essential services. When those systems fail, services halt. Communities are disrupted, trust erodes, and agencies face regulatory scrutiny, reporting obligations, and potential legal exposure.

This is what makes modernization in the public sector fundamentally different from modernization in the private sector. It is not driven by competition or innovation for its own sake. It is driven by responsibility.

Today, agencies are navigating a convergence of pressures: aging environments, rising cyber threats, increasing regulatory oversight, and constrained budgets. These forces are reshaping how IT leaders think about risk, resilience, and investment.

This playbook explores how state and local government agencies can strengthen cyber resilience, protect data integrity, and ensure uninterrupted service delivery

in an increasingly high-risk environment. It outlines practical strategies for building secure, predictable, and trustworthy data foundations that support essential public services.

The Converging Pressures Facing State and Local Government

Regulation, Risk, and Readiness

State and local governments are operating in an environment increasingly defined by regulatory expectation. Cybersecurity and resilience are no longer just internal priorities. They are subject to formal requirements, oversight, and public accountability. Agencies must not only respond to incidents, but demonstrate that they can operate securely, recover predictably, and maintain control under scrutiny.

This shift reframes risk. Systems must still be protected, but now resilience must be proven. At the same time, two forces make this harder to achieve: a more disruptive threat landscape and fragmented, aging environments.

Regulatory Pressure: The Primary Driver

Regulatory expectations are becoming more explicit and more demanding. Agencies are required to demonstrate control over data, enforce consistent access governance, and validate recovery processes. It is no longer enough to have backups or response plans. Resilience must be measurable, tested, and auditable.

This includes:

- Verifiable data integrity
- Defined and tested recovery timelines
- Enforced access controls
- Documented, repeatable incident response

Failure carries real consequences: audit findings, legal exposure, funding risk, and loss of public trust. As a result, technology decisions must be defensible, not just effective, and aligned with regulatory expectations.

External Pressures: Threats That Trigger Scrutiny

Cyber threats increasingly test regulatory readiness. Ransomware now targets access, leaving systems online but unusable. At the same time, expanding digital infrastructure increases the risk of real-world disruption across essential services. Research shows that almost 50% of local governments in the USA experience daily cyber-attacks; however, one-third are unaware of their cybersecurity status, and two-thirds are uncertain about potential breaches.

These incidents are not just operational. They are compliance events. Breaches trigger reporting requirements, audits, and public scrutiny. The question is no longer “Can we recover?” but “Can we recover in a controlled, compliant way?”

Internal Pressures: Gaps That Undermine Compliance

Many environments are not equipped to meet these expectations. Legacy systems, siloed data, and inconsistent governance limit visibility and control. Agencies often lack clear answers to where data resides, who can access it, and how it is protected. These are not just technical gaps. They are compliance risks.

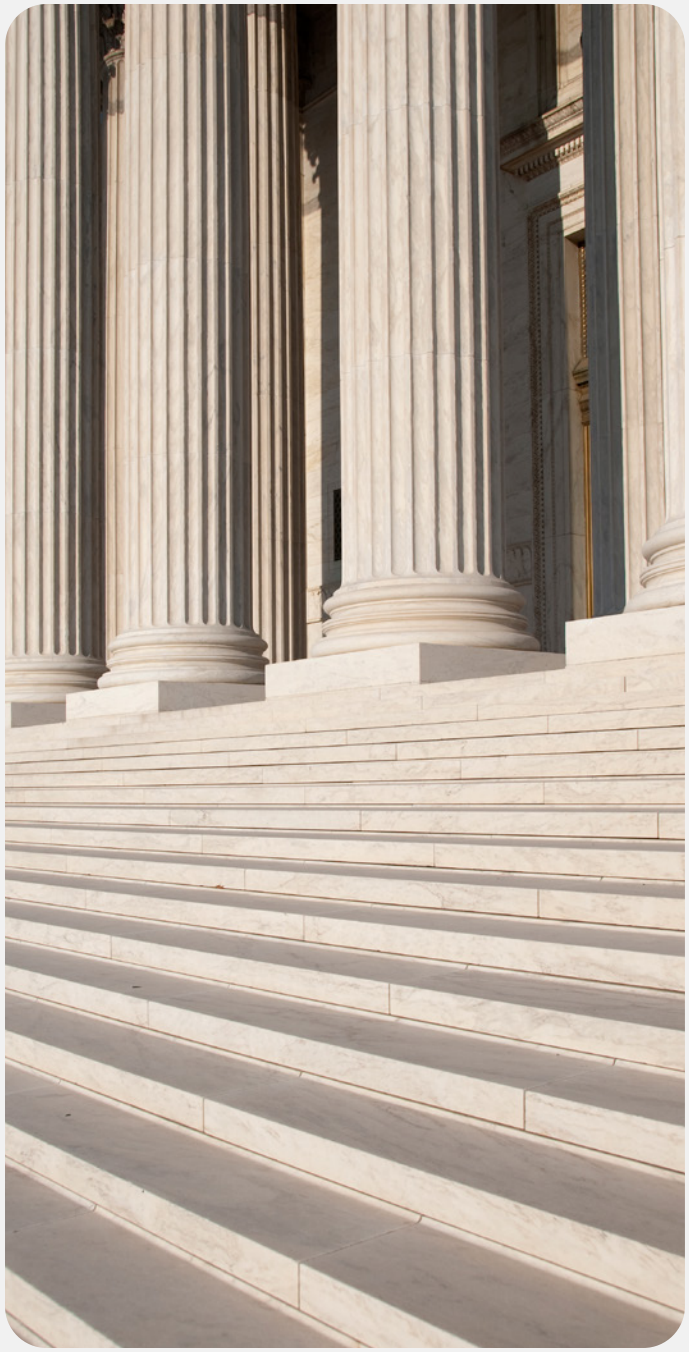
Approaches like unvalidated replication can spread corrupted data, while workforce constraints make consistent control harder to maintain. The result is a growing mismatch between regulatory expectations and operational reality.

A Compliance-Driven Imperative

These pressures are interconnected, but regulation now sets the standard.

- Regulation defines what resilience requires
- Threats test whether it holds
- Internal gaps determine whether it's achievable

To succeed, agencies must build resilience that is not only operationally effective, but measurable, testable, and able to withstand scrutiny.



CONVERGING PRESSURES ON STATE AND LOCAL GOVERNMENT

Primary Driver

Regulatory Pressure: Defines requirements for security, recovery, and accountability

Amplifying Forces

Cyber Threats: Test resilience and trigger compliance events

Internal Fragmentation: Limits visibility, control, and recoverability

Resulting Imperative

Resilience must be measurable, testable, and defensible

Cyber Resilience as a Public Trust Strategy

In the public sector, resilience is both a technical objective *and* a trust imperative. Citizens expect government services to function reliably and securely. When systems fail or data is compromised, it affects confidence in the institution itself.

At its core, cyber resilience strategy centers on data integrity. Agencies are prioritizing approaches that ensure data cannot be altered, corrupted, or silently compromised. Practices such as immutability, where data can be read but not changed, are becoming more common.

At the same time, additional safeguards are being implemented to prevent deletion, ensuring that critical records remain intact over long periods of time. These approaches are particularly important in environments such as public records, legal documentation, and citizen information systems.

Clearly, a resilience strategy must protect data. It must also ensure it can be recovered in a predictable and controlled way. This requires a shift away from assumptions of instant recovery. In reality, incident response follows a defined process. Security teams assess and isolate the threat. Leadership evaluates legal and regulatory obligations. Only then does recovery begin.

While this process introduces delays, it also ensures that recovery is safe and compliant. Organizations that understand and have tested this process are better positioned to respond effectively. They know how long recovery will take. They know which systems to prioritize, and they can communicate confidently with stakeholders.

Regulators increasingly expect this predictability. This means compliance must meet requirements and demonstrate that risk is understood, managed, and continuously validated.

Key Components of Cyber Resilience Strategy

For state and local government agencies, cyber resilience is built on a few critical components:

- Data integrity (unchanged, trustworthy data)
- Immutability and retention (cannot be altered or deleted)
- Predictable recovery (tested, known recovery timelines)
- Incident isolation and response processes
- Access control and zero trust principles
- Continuous validation and testing

Enabling Secure, Controlled Modernization

Modernization in state and local government is about leveraging technology to enable safer, more reliable operations.

Unlike the private sector, where innovation may be driven by competitive advantage, public sector modernization must be defensible. Every investment is subject to scrutiny. Every decision must align with mission outcomes. This has led to a more measured approach to emerging technologies.

Artificial intelligence, for example, is being adopted cautiously. While it offers benefits in areas such as anomaly detection and operational efficiency, it also introduces new risks. Over-reliance on automated systems can reduce human vigilance, creating blind spots. At the same time, adversaries are using AI to enhance their own capabilities.

As a result, agencies are moving toward more controlled implementations. AI is being applied to specific use cases, with clear governance and human oversight. Regulatory frameworks are reinforcing this approach, requiring organizations to define, monitor, and validate how AI is used.

This reflects a broader trend: modernization must enhance control, not reduce it.

Hybrid architectures are also playing a role. While cloud adoption continues, many agencies are recognizing the need for greater control over critical workloads. Sensitive data, particularly in areas such as law enforcement and infrastructure management, often remains on-premises or within tightly controlled environments. The goal is flexibility without dependency.

At the same time, modernization is enabling new capabilities. Data analytics can improve decision-making in areas such as urban planning and resource allocation. Monitoring systems can provide real-time visibility into infrastructure performance. But these capabilities must be built on secure, reliable data foundations.

Without that foundation, innovation introduces risk rather than value.

Common Modernization Pitfalls—and What to Do Instead

Risky Approach		Better Approach
"Adopt everything new"	→	Focus on mission-aligned use cases
Full cloud dependence	→	Hybrid for control and flexibility
Fully automated security	→	Human oversight + governance
Performance-first mindset	→	Resilience-first mindset
Siloed innovation	→	Integrated, secure data foundation

Use Case: Securing Municipal Water Infrastructure

A regional water authority modernizes its monitoring systems to improve visibility across treatment facilities. Rather than moving critical operations fully to the cloud, it adopts a hybrid approach. This keeps core control systems in a secure, on-prem environment while using analytics tools to detect anomalies in real time.

When a cyber incident targets access credentials, the attack is contained before it spreads. Because data integrity controls and recovery processes were already in place and tested, operations continue without disruption. This ensures uninterrupted water service and maintains public trust.

A Practical Framework for State and Local IT Leaders

For IT leaders navigating these challenges, the path forward requires clarity and prioritization.

Identify mission-critical systems

Determine which systems and services cannot fail without disrupting essential public operations.

These are the systems that must be prioritized first in any resilience or recovery strategy.

Map and prioritize critical data

Understand where data resides, who can access it, and which datasets carry the highest risk.

This ensures protection efforts are focused on the data that matters most, not spread too thin.

Strengthen data integrity and recoverability

Ensure data cannot be altered or deleted improperly, and validate that recovery processes are tested and predictable.

The goal is not instant recovery, but confident, reliable restoration when it matters most.

Reduce fragmentation where possible

Simplify architectures to improve visibility, control, and response speed.

Fewer silos mean faster decisions and fewer blind spots during an incident.

Align modernization with risk reduction

Prioritize investments that improve resilience, continuity, and security—not just performance.

Every technology decision should directly support the agency's ability to operate under pressure.

Agencies should focus on protecting critical data, ensuring predictable recovery, and reducing risk where it impacts operations the most. A clear path should be charted to build resilience that supports continuous, reliable public service.

Conclusion

Reliability Is the New Innovation

For state and local governments, innovation is no longer about adopting more technology. It's about delivering services that are secure, reliable, and always available. Success depends on shifting focus from systems to data, and from reactive recovery to predictable resilience.

This is where experienced partners play a critical role. Providers like Hitachi Vantara bring decades of expertise in managing and protecting mission-critical data, helping agencies build environments that are not only high-performing, but secure, resilient, and predictable under pressure.

Because in the public sector, the most powerful innovation is the one that citizens never notice.

It is the system that does not fail. The service that remains available. The data that remains secure.

That is how public trust is built and maintained.

Hitachi Vantara

Hitachi Vantara is transforming the way data fuels innovation. A wholly owned subsidiary of Hitachi, Ltd., we're the data foundation the world's leading innovators rely on. Through data storage, infrastructure systems, cloud management and digital expertise, we build the foundation for sustainable business growth.

Learn More →