UNITRENDS
A Kaseya COMPANY

CHECKLIST

Unitrends State & Local Government BCDR Checklist

Local governments' approach to IT has been greatly influenced by smart city initiatives and digital transformation. While such undertakings offer opportunities for innovation and growth, they also present challenges in meeting uptime demands and protecting a rapidly growing data set. Local governments must meet strict requirements regarding reliability, security, uptime and compliance.

The transformation to smart cities requires a significant digital effort. Sensors, data collection and analytics are being implemented to manage a number of services, right from tax payments, water and power delivery permits to traffic management, construction and everything in between.

Amid these initiatives, protecting sensitive citizen information and maintaining the integrity of government systems is just as vital as keeping critical services and applications available around the clock. According to IBM's Cost of a Data Breach Report 2024[i], the global average cost of a data breach has surged to $4.88 million, marking a 10% increase over last year and setting a record high. That's why a comprehensive business continuity and disaster recovery (BCDR) strategy is a critical part of your cybersecurity strategy. With the right BCDR plan in place, your organization can remain operational during disruptions, recover quickly from incidents and protect the integrity of sensitive data and public services at all times.

This checklist is broken down into five categories to help you understand the different options that exist in the market today. With hundreds of vendors and technologies emerging in storage, infrastructure, data management and continuity, there's a broad range of strategies to consider as you determine the right BCDR solution for your organization.

[i] https://www.ibm.com/reports/data-breach

> ***Someone operating with far too much power deleted thousands of files from a share inadvertently and did so permanently. I was able to recover them all in minutes — 2.5 minutes to be exact — from the time the user told me the path to the share. All the files were fully restored. With Unitrends Backup doing its thing every night, I just don't worry about it anymore.***
>
> JOHN PIERCY
> Senior IT Architect, City of Lynchburg, VA.

1. Protection for all workloads

	CAPABILITY	DESCRIPTION
☐	Fewer Point Products.	A multi-vendor protection strategy increases IT complexity, risk and cost. Reducing the number of point solutions means managing fewer licenses and service agreements, and cuts management and technician time.
☐	Purpose-Built Appliance.	A purpose-built, turnkey data protection appliance combines pre-integrated hardware, software and cloud technologies into a single, cohesive solution. This unified approach simplifies deployment, streamlines management and reduces the complexity often associated with multivendor setups.
☐	Comprehensive Protection Across Every Workload	A unified data protection platform reduces reliance on multiple point products by delivering modular capabilities tailored to specific environments — from data center infrastructure to Software-as-a-Service (SaaS) applications and remote endpoints. This platform approach enables IT teams to align recovery objectives with the criticality of each workload, ensuring service level agreement (SLA)-driven protection across the board. With a single user interface and consistent design, teams benefit from a shorter learning curve, faster adoption and greater operational efficiency, no matter where the data lives.
☐	Policy-Based Management	Admins should be able to choose how backups are scheduled, either by entering a specific schedule or by using intelligent, policy-based scheduling technology.
☐	Data Reduction	Data reduction (deduplication, compression) reduces the overall size of files and eliminates redundancy among stored blocks, making movement, management and storage more efficient.
☐	Global Deduplication	As stated above, considering solutions that offer global deduplication across the entire backup volume will enable more efficient storage utilization than job-based duplication, which reduces blocks on a per-job basis. Since the probability of having duplicate data on VMs with the same OS is relatively high, per-job deduplication misses out on efficiency unless you put all VMs into a single backup.
☐	RESTful-API	A RESTful API can easily integrate with other applications.
☐	Support for Hyperscale Clouds	Today's solution should easily integrate with hyperscale clouds, such as AWS or Azure, to protect IaaS workloads, store backups for long-term retention requirements and enable disaster recovery.
☐	Disaster Recovery-as-a-Service (DRaaS)	DRaaS provides assisted, rapid recovery of critical systems and applications in the cloud, ensuring your operations can resume with minimal interruption. Whether restoring an entire site or a single mission-critical workload, this cloud-based solution delivers the speed and flexibility needed to meet today's uptime demands. When evaluating providers, look for those that offer contractually guaranteed recovery time objectives (RTOs) to ensure your recovery timelines are met with confidence.

2. Avoiding downtime and data loss

	CAPABILITY	DESCRIPTION
☐	Flexible Recovery Options	Your solution should be flexible in how you can recover assets as well as where you can recover the data to. Look for solutions that support a wide range of recovery modes, including instant virtualization, physical-to-virtual (P2V), virtual-to-virtual (V2V), virtual-to-physical (V2P) and replicas.
☐	Instant Recovery From Local Disasters	If a server, VM or data center rack goes offline or fails, your appliance should be able to orchestrate failover to bring applications back up from your most recent backup with a near-zero RTO.
☐	Bare Metal Recovery	Bare metal restores enable application recovery across servers from different vendors and hardware configurations.
☐	Data Loss Prediction	Utilize intelligent tools that simulate different disasters and outage scenarios to determine what types of and how much data would be lost in a downtime event so you can refine your strategy and ensure RPOs are being met.
☐	Application Downtime Prediction	Leverage deep application testing to identify, simulate and test the multiple steps required to recover complex applications to ensure RTOs and uptime SLAs are being met.
☐	Automated DR Testing and DR Failover	Regular testing is essential to ensure your disaster recovery (DR) plan will actually work when it's needed. Automated DR testing allows you to validate recovery processes without disrupting production systems, helping uncover gaps before they become critical issues. In the event of an outage, automated failover enables rapid, seamless transition to backup systems, minimizing downtime and ensuring business continuity with little to no manual intervention.

> ***What stands out to me is that I don't have to babysit the system. Unitrends has been so easy to administer, and I'm never worried the backups aren't going to run — the consistency of Unitrends has been great.***
>
> JASON REITZ
> Systems Administrator, City of Fort Lupton, CO.

3. Safeguarding data from ransomware, cyberthreats and other security considerations

	CAPABILITY	DESCRIPTION
☐	AES Encryption	AES encryption secures data privacy both at-rest and in-flight. In addition to data backups, office email should be secured and any Personally Identifiable Information (PII) sent via email should be encrypted. Any removeable storage devices (HDDs, USB drives) should be encrypted. Staff should be trained adequately in encryption procedures.
☐	Ransomware Prevention	Consider a solution written in hardened Linux. Ransomware targets Windows applications and common utilities (i.e., VSS writers) due to their popularity and the fact that Windows is an open architecture.
☐	Threat Detection	Your solution should use machine learning to detect in near real-time an active infection. Advanced algorithms establishes a baseline of heuristics, such as change rate prediction, data entropy and randomness, to identify anomalies in data that antivirus and Firewalls don't catch. Automatic notifications alert admins, enabling them to take immediate action to slow the spread and speed recovery efforts.
☐	Anti-Phishing Defense	Empower employees to defend against phishing and account takeover attacks. Solutions that provide visual cues (i.e., banner notification) alert employees to external senders, spoofed and/or imitated users and enable them to quarantine suspicious emails, which helps to automate workflows and feedback loops to streamline IT review.
☐	Physical Security	Computers and servers should be in secured, locked locations. An alarm system should be in place for after-hours security as well as continuous visual security for office systems.
☐	Multifactor authentication	Enforcing MFA across the entire organization helps secure access to all applications, systems and the backup environment. By requiring an additional layer of verification, MFA significantly reduces the risk of unauthorized access and strengthens your overall security posture.

4. Regulatory compliance

	CAPABILITY	DESCRIPTION
☐	Role-Based Access Control	When dealing with highly proprietary data, not all backup and recovery users may require access. A solution that limits the scope and capabilities of admins and other users ensures that backup schedules and/or recoveries are only performed by authorized personnel.
☐	Long-Term Data Retention	Depending on your state, you may be required to retain records (such as tax records) for several years. Your solution needs to be able to accommodate long-term data retention, whether locally, to a cloud location, or a secondary target (i.e., NAS device or tapes).
☐	Immutable Audit Logs	Immutable logs and routine monitoring ensure that the data being handled by your backup and recovery systems is being appropriately handled and accessed by staff.
☐	Internal Anomalous Monitoring & Detection	Secure servers, data and network with an AI-augmented solution that identifies threats such as misconfigurations, unauthorized logins, new devices being added to the network, gaps in backups and admin rights being granted that firewall and antivirus can't detect.
☐	SLA Testing & Reporting	Recovery assurance reporting enables automated testing and documentation of recoveries against RTOs and recovery point objectives (RPOs). This not only builds confidence in your ability to recover but also provides clear, auditable proof of compliance with internal policies and regulatory requirements.

5. Support for non-savvy users

	CAPABILITY	DESCRIPTION
☐	Intuitive User Interface (UI)	A modern, simple UI should be a priority. Operating your backup system should be possible without the need to frequently consult a manual or guide. Substitutes and managers can quickly and seamlessly stand in when primary admins are unavailable.
☐	File Recovery	Government IT often supports unsophisticated users prone to mistakes who may click dangerous links or delete files. Your solution should make it intuitive and easy to find and restore individual files from backups with only a few clicks. Indexed search capabilities and self-service recovery (with role-based access control) enable quick recovery, and in some cases may not require IT intervention.
☐	Purpose-Built SaaS Protection	Native data protection tools for SaaS applications such as Microsoft 365, Google Workspace and Salesforce often can't meet the RTO and RPO required today. A purpose-built solution protects cloud-based applications to minimize loss of data and productivity with granular, point-in-time recovery.

Having cloud backups in addition to the onsite appliance is a huge help. We like having that quick restore ability locally, but having data replicated offsite as well, the assurance that we have with Unitrends is that no matter what the situation, we feel that we will always be able to get to our data.

JAY WALLER
Information Technology Manager, Town of Mount Pleasant, SC

Unitrends has a long history of helping IT professionals engaged with state and local governments protect their assets. Townships, cities, police departments and others across the world leverage Unitrends' portfolio of turnkey, cloud-empowered backup appliances to provide continuity across all workloads. Agile and customizable, Unitrends offers unmatched flexibility to help meet an organization's needs of today and tomorrow. Unitrends provides unparalleled protection for physical, virtual and cloud-based systems augmented with AI and automated, application-level recovery testing so you know that you can recover systems, data and applications with 100% confidence.

ARE YOU READY TO SEE HOW UNITRENDS CAN HELP YOUR ORGANIZATION?

GET STARTED TODAY!

ABOUT UNITRENDS

Unitrends makes efficient, reliable backup and recovery as effortless and hassle-free as possible. We combine deep expertise gained over 30 years of focusing on backup and recovery with next-generation backup appliances and cloud purpose-built to make data protection simpler, more automated and more resilient than any other solution in the industry.

UNITRENDS
A Kaseya COMPANY

05302025