IT infrastructure in mid-sized cities and counties:

Moving toward resilience and sustainability

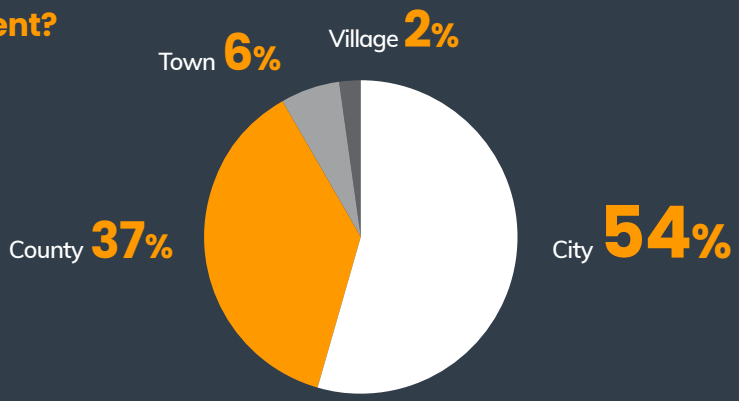
Introduction

In May 2022, the Center for Digital Government (CDG) conducted a national survey of 127 leaders from mid-sized counties and cities, defined as counties with a population between 50,000 and 1 million people and cities with a population between 25,000 and 500,000. The goal was to gain insight into IT infrastructure, especially cloud infrastructure, in local government and identify common trends related to infrastructure requirements, challenges, and plans for the future. Overall findings indicate mid-sized jurisdictions are firmly grounded in the requirements for a robust IT infrastructure and are incorporating cloud-based solutions to help them address key business and technology challenges on the path to a more resilient, sustainable IT infrastructure.

Respondent demographics

What is your branch of government?

The Center for Digital Government surveyed 127 local government leaders from mid-sized cities and counties in May 2022 on the topic of infrastructure modernization. The following data shows respondents' demographics by the branch of government they work in and the function of their agency or department.



What is the function of your agency or department?

- 44% Information technology/telecommunications
- 9% Administration/operations/general services/purchasing
- 8% Finance/taxation/budgeting
- 8% Public works/transportation/infrastructure/utility/planning
- 6% Elected official/ legislative
- 6% Economic development/workplace development
- 5% Health and human services
- 4% Courts/corrections/justice
- 3% Law enforcement
- 2% Human resources/benefits/personnel
- 1% Environment/energy
- 1% Fire/emergency services
- 1% Education/library services
- 2% Other

Key Findings:

Security infrastructure, connectivity, and disaster recovery are top necessities for a robust IT infrastructure.

Respondents ranked security infrastructure, sufficient bandwidth/connectivity, and disaster recovery infrastructure as the three most necessary components for a robust IT infrastructure, with security infrastructure significantly outranking all other options.

- **Security infrastructure.** The rise in phishing and ransomware attacks — combined with increasingly distributed environments, the shift to remote work, and digital constituent services — keeps security top of mind. Respondents recognize traditional defenses focused on "guarding the castle" are no longer sufficient. When asked about the most important components of a security strategy, the top two responses — employee awareness training (59%) and identity and access management (56%) — focused on users themselves.

- **Sufficient bandwidth.** Connectivity is the backbone of IT operations. To support new use cases; deliver ample bandwidth for edge computing, automation, and other bandwidth-intensive operations; and ensure users and devices can access resources wherever they are, organizations need an infrastructure that supports a range of connectivity options. Nearly 50% of respondents are making investments in at least one area to improve networking and content delivery. The most commonly cited investments in this area include hybrid connectivity (25%), public-private partnerships (24%), application networking (20%), edge networking (16%), private 5G networks (9%), and satellites (7%).

- **Disaster recovery.** Disaster recovery has always been essential to recover from outages quickly and minimize data loss associated with incidents. In recent years, its role in ransomware prevention and recovery has been increasingly highlighted. If organizations can ensure (via immutable backups and/or synchronous replication) data will not be compromised or held hostage by a ransomware attack, cybercriminals have less motivation to attempt extortion.

What components are most necessary for a robust IT infrastructure for mid-sized governments? Please select up to 5.

There's rarely enough funding, staffing, or time when it comes to modernizing IT infrastructure.

Funding (69%), staffing (65%), and time (53%) are challenges for a majority of respondents. Nearly 75% of respondents reported that either staffing or expertise/skill sets are a challenge.

Although recent funding from the Infrastructure Investment and Jobs Act (IIJA) and other sources has been a boon to many, not all agencies can make use of those monies.

"There are very big disparities in terms of funding capabilities across agencies," says Omar Sandoval, director of government programs for CDG. "When we talk about licensing seats, not all agencies are created equal. For example, a special district typically does not receive anywhere near as much tax funding as it does from its services and collection of fees."

Even organizations that can leverage one-time funding must determine how they will pay for ongoing operational expenses. Funding questions may also exist about how to move to cloud procurement models that don't fit into a traditional capital expenditure budget structure.

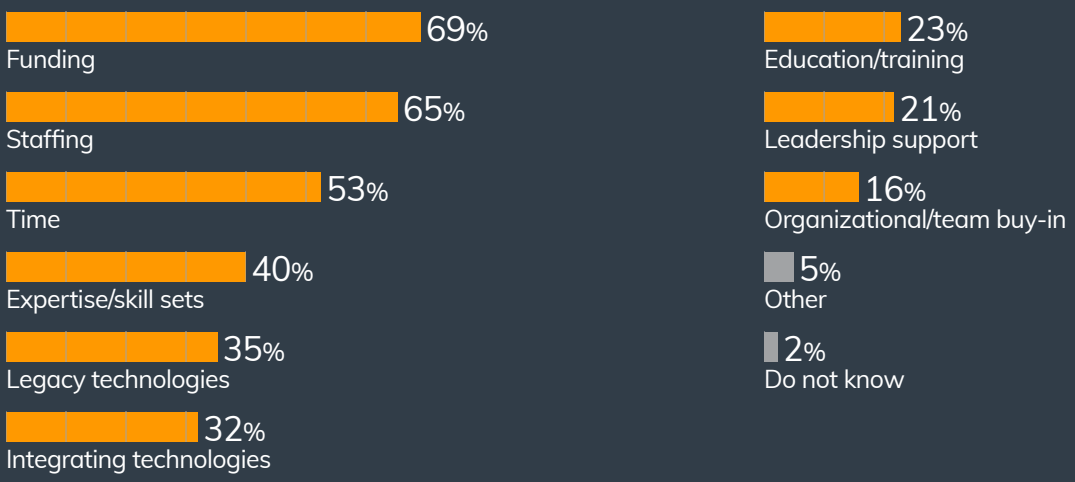
Staffing limitations and complexity are also barriers to modernization. It takes a very different skill set to manage the cloud versus an on-premises server, for example. In addition, about a third of organizations that responded to the CDG survey are concerned about the task of migrating and integrating legacy technologies and workloads. Agencies don't always have the skill sets to implement these solutions on their own, and they may not want to spend money on hiring for those skills.

"Most legacy solutions weren't built to be digital-friendly," says CDG Vice President Brian Cohen. "When governments take steps to make their systems more user-friendly and accessible for constituents, they are most likely creating new infrastructure and security challenges. These same organizations are constantly putting out fires and finding it hard to get ahead when legacy systems and technical debt don't allow them."

In the drive to address urgent infrastructure issues, lengthy procurement times and other obstacles can slow modernization efforts. To ensure compliance and competitiveness in procurements, government organizations must pass through a series of checks and balances that can take months. In addition, leadership changes can delay or derail initiatives, thereby creating further technical debt and interfering with modernization goals.

"The urgent issues that came up in this survey most often cannot wait," Cohen says. "Security concerns should not linger while governments work through the steps necessary to ensure a competitive procurement process or include the expense as a strategic investment in its funding plan."

What are the top challenges you face in modernizing your IT infrastructure?
Please select up to 5.



Security infrastructure, user devices, and cloud data storage are the top planned upgrades.

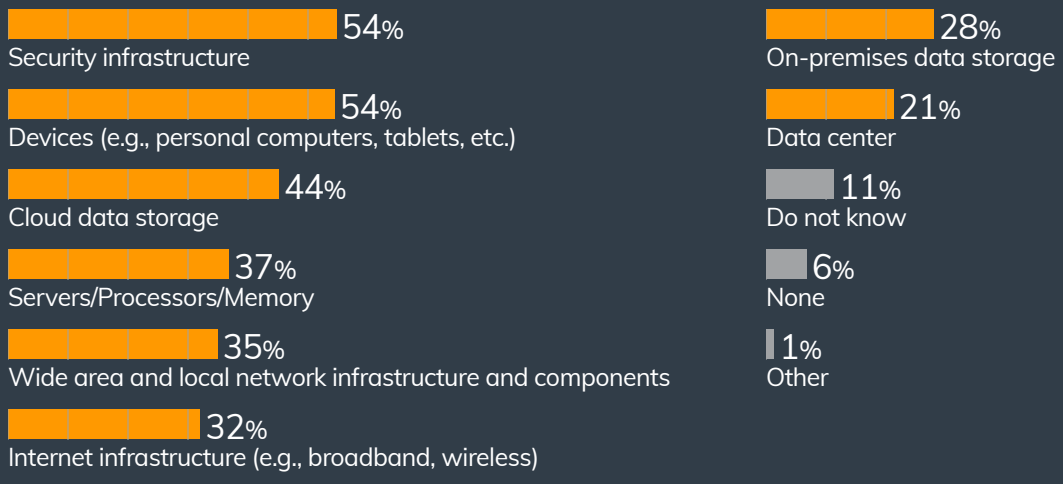
Respondents were most likely to report their jurisdictions are planning to upgrade security infrastructure (54%), user devices (54%), and cloud data storage (44%).

IIJA cybersecurity grants make this an especially good time to consider security infrastructure upgrades — especially for rural areas and smaller towns and cities. For example, the Rural and Municipal Utility Advanced Cybersecurity Grant and Technical Assistance Program gives priority to "eligible entities that have limited cybersecurity resources, own assets critical to the reliability of the bulk-power system, or own defense-critical electric infrastructure (as defined in the Federal Power Act)."[1]

While personal computers, tablets, and mobile devices aren't always considered part of IT infrastructure, they have become essential to remote work, field work, and other operations. The devices of even a few years ago may not have the security features and compute power needed for advanced collaboration and other tasks. Planned upgrades to cloud data storage (44%) and servers, processors, and memory (37%) also reflect a growing need for more storage and processing power as organizations manipulate high volumes of data and embrace machine learning (ML), automation, edge computing, data sharing, and other advanced processes.

While personal computers, tablets, and mobile devices aren't always considered part of IT infrastructure, they have become essential to remote work, field work, and other operations.

What IT infrastructure is your jurisdiction planning to upgrade in the next 12 to 24 months? Please select all that apply.



Cloud infrastructure investments are a preferred path to meet data storage/backup, security infrastructure, and other modernization goals.

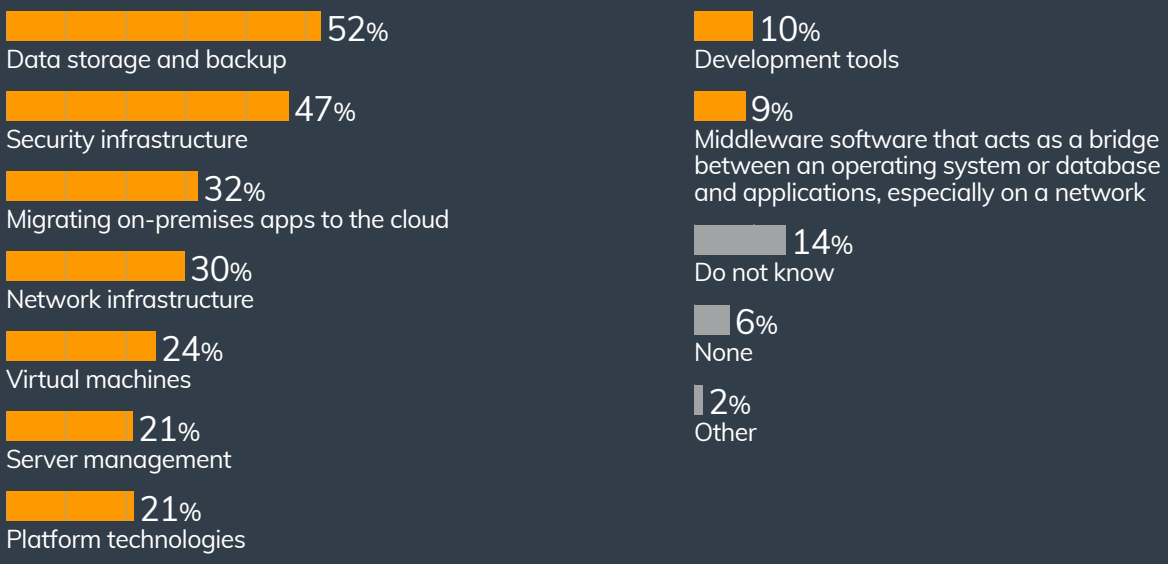
About half of respondents reported their jurisdiction is investing in cloud data storage and backup (52%) and cloud security infrastructure (47%).

Using the cloud for storage and backup provides a number of advantages. With a cloud solution, cities and counties can rapidly provision different types of storage and flexibly scale storage capacity as needs fluctuate. Cloud data lakes provide low-cost storage for structured and unstructured data, and they enable organizations to leverage data from multiple sources for data analytics, automation, and other processes. Cloud-based immutable backups help mitigate the risk of (and damage from) ransomware attacks and other breaches by creating an air gap so bad actors can't access, alter, or delete backups.

Using the cloud for security infrastructure protects data at scale from distributed denial of service (DDoS) and other massive attacks. The high number and wide distribution of data centers in a vendor's cloud infrastructure allows for failover to other sites if needed and enables both synchronous and asynchronous replication, which is necessary for rapid, low-data-loss disaster recovery. Finally, leading cloud vendors have invested more money into tools, best practices, and highly skilled cybersecurity teams to protect their cloud infrastructure and solutions than most cities and counties can afford on their own.

Using the cloud for security infrastructure **protects data at scale** from distributed denial of service (DDoS) and other massive attacks.

Is your jurisdiction investing in any of the following types of cloud infrastructure? Please select all that apply.



Disaster recovery is by far the biggest driver for moving IT infrastructure to the cloud. In many ways, it's representative of cloud's multiple benefits.

Two-thirds of respondents said disaster recovery/business continuity is a top driver for moving infrastructure to the cloud. Cost savings/ROI (47%) and improved cybersecurity (45%) are also top drivers.

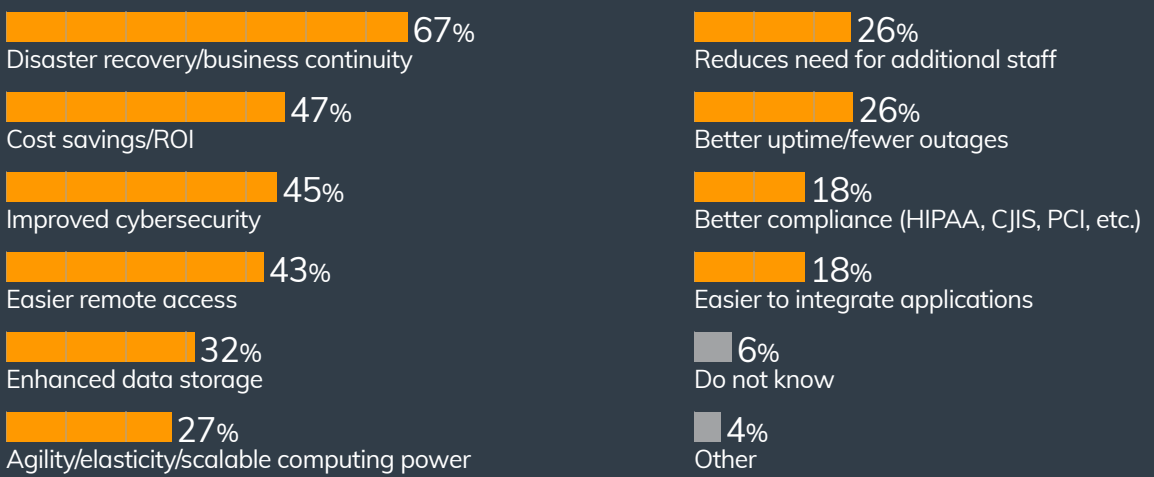
Natural disasters, power outages, and accidental cable cuts have always been disaster recovery/business continuity (DR/BC) concerns. Now government agencies also have to contend with the threat of cyberattacks and civil unrest that can bring down their mission-critical systems.

DR/BC capabilities help maintain the availability of vital services and help ensure minimal data is lost in the event of a disaster. Maintaining these capabilities on-premises is very costly and complex. Short recovery times and minimal data loss require architectures with multiple highly scalable data centers. Besides building and equipment costs for each data center, organizations must also pay for staffing, connectivity, maintenance, ongoing upgrades and modernization, and other operating expenses. Deployments can take years.

When organizations move to the cloud, they automatically get a DR solution and a BC plan by virtue of being in the vendor's cloud environment. This reduces capital and operating costs — and the workload on IT staff — substantially. Taking advantage of the cloud provider's BC plans may also allow organizations to meet auditing or other requirements for a BC plan.

When organizations move to the cloud, they automatically get a DR solution and a BC plan by virtue of being in the vendor's cloud environment.

What are the biggest drivers of moving IT infrastructure to the cloud?
Please select up to 5.



Procurement contracts provide essential details for evaluating cloud infrastructure providers and the components they offer.

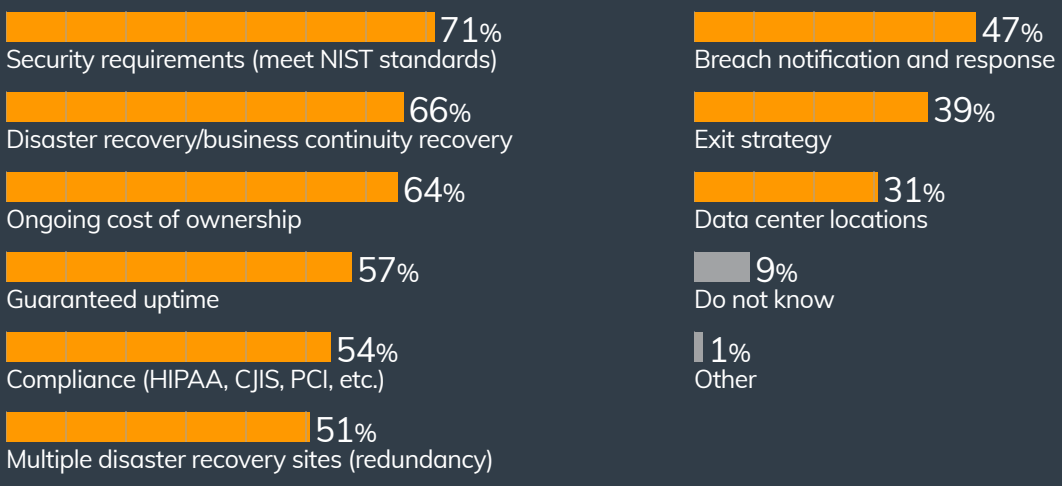
When it comes to structuring procurement contracts for cloud-based infrastructure, 71% of respondents said it's important for a contract to address security requirements, while 66% cited disaster recovery/business continuity and 64% said ongoing cost of ownership.

Respondents also noted that asking for service-level agreements (SLAs) and historic performance on guaranteed uptime (57% of respondents), as well as details about the number of disaster recovery sites (51%) and data center locations (31%) should be part of any conversation on disaster recovery/business continuity. Similarly, regulatory compliance (54%) and breach notification/response (47%) ties into discussions about security requirements and should be on every procurement checklist.

Finally, while cloud solutions greatly reduce the operational cost of owning infrastructure, organizations are wise to investigate ongoing cloud-related costs associated with networking/connectivity to the cloud, security, and management. Doing so will be important for making a strong business case, budgeting for the future, and avoiding unwanted surprises down the road.

While cloud solutions greatly reduce the operational cost of owning infrastructure, organizations are wise to investigate ongoing cloud-related costs associated with networking/connectivity to the cloud, security, and management.

What components of a procurement contract must be addressed when buying cloud-based IT infrastructure? Please select all that apply.



Going further and faster with less risk

Components alone are not enough for successful modernization. A mature, robust infrastructure requires governance and best practices, regularly rehearsed DR plans, automation and machine learning to help detect suspicious behavior and enable intelligent resource allocation, appropriate staffing and maintenance, and more. Working with the right cloud partner helps pull all these details and disciplines together, ensuring mid-sized jurisdictions have the modern, robust infrastructure they need to take advantage of new opportunities and respond to change more agilely, resiliently, and cost-effectively.

This piece was written and produced by the Center for Digital Government Content Studio, with information and input from AWS.

1. https://www.natlawreview.com/article/infrastructure-investment-and-jobs-act-invests-heavily-cybersecurity

Produced by: CENTER FOR DIGITAL GOVERNMENT

The Center for Digital Government, a division of e.Republic, is a national research and advisory institute on information technology policies and best practices in state and local government. Through its diverse and dynamic programs and services, the Center provides public and private sector leaders with decision support, knowledge and opportunities to help them effectively incorporate new technologies in the 21st century. **www.centerdigitalgov.com.**

Sponsored by: aws

Amazon Web Services (AWS) Worldwide Public Sector helps government, education, and nonprofit customers deploy cloud services to reduce costs, drive efficiencies, and increase innovation. State and local government transportation agencies are leveraging AWS to improve the safety and performance of transportation networks. Whether your focus is on agency modernization, resiliency, or cost savings, AWS has dedicated teams to help you pave the way for innovation and, ultimately, make the world a better place through technology. **aws.amazon.com/stateandlocal/transportation/**

ADOBESTOCK