



2026 County CIO Insights

Counties are balancing resilience, modernization, and service delivery amid fiscal and operational constraints, with Enterprise Resource Planning (ERP) modernization emerging as a practical lever to improve staff experience and provide more actionable information.

July 2026

Table of contents

Table of contents	1
Executive summary	3
Capacity constraints across all themes	5
AI adoption is progressing, but readiness gaps are holding counties back	8
Maintenance-heavy environments continue to limit innovation	10
Security is a priority, but gaps persist across capabilities	12
Digital experience and advanced capabilities remain underdeveloped	14
County IT leadership has broad accountability, limited capacity	16
Implementation playbook for county CIOs	18
Conclusion	19

Foreword

The County CIO and IT Executive Survey, issued in December 2025, shows that county technology organizations are being asked to do more with less: maintain essential systems, secure expanding digital footprints, support modernization, and improve the constituent experience while relying heavily on local funding and relatively small teams.

County technology leaders are no longer simply maintaining systems and supporting departments. They are being asked to expand organizational capacity by helping staff work more effectively, improving constituent service, strengthening continuity and resilience, and enabling better decisions in an environment where time, funding, and talent remain constrained. That is the lens through which this report should be read.

The survey findings suggest that counties are making practical progress, particularly in foundational cybersecurity, operational support, and core digital capabilities. At the same time, progress is less consistent in areas such as advanced digital experience, formal program measurement, emerging technology enablement, and enterprise-wide governance maturity. The picture is not one of inaction; it is one of steady effort within real fiscal, staffing, and operational constraints.

What makes the findings especially significant is what they suggest about the future of county government: counties are being asked to expand organizational capacity, not just maintain systems.

Executive summary

County technology leaders are entering a phase where the challenge is no longer establishing IT's relevance but converting strategic alignment into sustained modernization and measurable capacity. Findings from our 2026 County CIO Survey indicate that county IT organizations are broadly aligned to county goals: roughly 62% report that IT strategy is completely or well aligned, and top priorities center on cybersecurity and compliance, mission alignment, and cost-effective operations.

At the same time, many counties are pursuing that mandate within constrained operating models and limited budget flexibility. Nearly half of respondents report having 10 or fewer full-time staff supporting county IT infrastructure, and roughly 91% say internal IT services are delivered primarily through a CIO or IT director model. Approximately 82% of counties rely heavily on local revenue sources such as county fees and property taxes, while grants and state appropriations play a smaller role. At the same time, county operating environments vary significantly by population served, tax base, service complexity, and organizational scale, so modernization paths will not look the same for smaller, mid-sized, and larger counties. Together, these dynamics create broad spans of responsibility, limited room for specialization, and a need to make prioritization central to county IT strategy.

Cybersecurity stands out as the leading strategic priority. About 63% rank enhancing cybersecurity posture and compliance among their top priorities, ahead of aligning IT to mission value and delivering cost-effective operations. Many counties appear to have made meaningful progress on foundational controls, but more advanced capabilities, such as citizen digital identity, program measurement, enterprise governance, and integrated resilience planning, remain less common. Modernization is also moving gradually: more than half of respondents in the 2026 County CIO survey say less than 10% of their IT budget is dedicated to innovation rather than maintenance, and two-thirds report environments that are at least 75% on premises. Counties are modernizing, but often from a position shaped by older systems, fiscal pressure, and operational risk sensitivity.

The findings point to a broader future-state challenge for county government. Counties are not managing separate agendas in artificial intelligence (AI), cybersecurity, ERP, digital experience, and governance. In practice, these are interconnected levers for creating capacity. AI can reduce manual work requirements and improve knowledge access. ERP modernization can improve staff productivity and provide more actionable information. Cybersecurity and continuity planning can strengthen resilience. Digital improvements can make

service delivery more effective. Governance can help counties direct resources toward the leading-value outcomes. **This report highlights six major themes emerging from the survey:**

- AI adoption is progressing, but readiness gaps are holding counties back from adopting AI.
- Main challenges to modernization are structural, not cultural.
- Maintenance-heavy environments continue to limit innovation.
- Security is strong at the core, but gaps persist across advanced capabilities.
- Digital experience and advanced capabilities remain underdeveloped.
- County IT leadership has broad accountability, and limited capacity.

The prevalent throughline across all six themes is capacity. Counties are being asked to do more with limited staff, funding, and time. The core question is not whether county leaders understand the modernization agenda. It is whether they can use modernization to create enough organizational capacity to meet rising expectations over the next several years.

Capacity constraints across all themes

Smaller counties are more likely to face acute specialization gaps and heavier reliance on generalist staff or external providers. Mid-sized counties often face scaling challenges as service expectations rise faster than team capacity. Larger counties may have greater internal depth, but also more complex environments, broader service portfolios, and more demanding governance needs.

Staffing Pressures

Staffing constraints sit underneath nearly every issue in this report. County respondents cite staff proficiency availability at 70%, salary cost at 60%, and career advancement opportunities at 55% among their top staffing concerns, with benefits and remote work also being contributing factors. In short, counties are trying to modernize and defend increasingly complex environments while competing for talent with tighter compensation flexibility.

This has two implications. First, county IT strategy must increasingly emphasize simplification, automation, and shared capability models. Second, operations should not be separated from modernization planning. If counties want stronger digital experience, better analytics, broader AI adoption, or more mature cyber operations, they should align talent models and operating approaches to complement human expertise and enable those outcomes.

Operating Capacity Constraints

Operating constraints can shape modernization as much as technology ambition. About 48% of surveyed counties have 10 or fewer full-time staff supporting county IT, roughly 82% rely primarily on local revenue sources, 53% dedicate less than 10% of the IT budget to innovation, and two-thirds operate environments that are at least 75% on premises. In practical terms, modernization competes with the day-to-day demands of maintaining essential systems, managing risk, and sustaining service levels.

Counties need modernization strategies that create capacity as they go by reducing maintenance burden, simplifying infrastructure, improving staff productivity, and lowering delivery risk

This has two implications. First, the central challenge is execution, not intent: 45% cite budget limitations as a barrier to modernization, while only 14% point to lack of executive support or sponsorship. Counties do not need more vision statements; they need modernization paths that are affordable, defensible, and tied to visible value. Second, counties need modernization strategies that create capacity as they go by reducing maintenance burden, simplifying infrastructure, improving staff productivity, and lowering delivery risk.

These constraints do not only limit project delivery. They shape the operating model itself. In many countries, the modernization challenge is less about selecting the right technology than it is about creating enough delivery capacity, governance discipline, and workforce adaptability to make modernization stick. That is why leading organizations are moving away from isolated technical upgrades and toward cross-functional operating models, measurable business outcomes, and more adaptive approaches to work design and change adoption.



AI adoption is progressing, but readiness gaps are holding counties back

Counties are beginning to adopt AI tools, but not at full speed. Among reported responses, 34% are already using generative AI, 23% plan to adopt it within 12 months, and 29% report no current plans. The direction is clear, but adoption remains uneven.

That caution is understandable. Counties are pursuing AI in environments where innovation funding is limited, digital maturity is uneven, and governance capabilities are still developing. Security and compliance remain the top strategic priority for 63% of county IT leaders, and generative AI security controls are already part of the broader cybersecurity agenda.

Readiness for AI will also vary by county size. Smaller counties may need to start with narrower, lower-risk use cases and rely more on shared guidance, external support, or consortium-based approaches, while larger counties may be better positioned to formalize governance and scale adoption across functions.

Counties should avoid treating AI as a bolt-on tool layered onto unchanged processes. The more important opportunity is to redesign selected workflows so AI can reduce repetitive administrative work, improves knowledge access, and shorten response cycles for internal service teams. In that sense, AI is not just an automation technology. It is a potential force multiplier for lean county workforces.

That does not require immediate large-scale deployment. For many counties, the practical path is targeted internal use: policy and knowledge retrieval, draft communications, service-desk support, summarization, workflow triage, and other low-risk administrative tasks. Over time, counties can expand from tool access to governed human-machine collaboration, provided that privacy, security, transparency, and human review remain explicit design principles.

The opportunity, however, is broader than experimentation with a new technology category. Over the next several years, AI has the potential to become a practical capacity lever for counties, particularly in operational efficiency, knowledge support, automation, internal service delivery, and constituent service. In constrained environments, that matters. Counties

that use AI responsibly may be better positioned to reduce administrative burden, improve staff access to information, and enhance workforce capacity, helping frontline employees focus on more public service responsibilities instead of administrative tasks.

The larger question is not simply whether counties adopt AI. It is whether they can adopt it in ways that strengthen workforce effectiveness, service delivery, and public trust. Counties that move too quickly may create avoidable governance, privacy, or security risks. Counties that delay entirely may preserve short-term risk control, but they may also widen gaps in productivity and service quality relative to their peers. The goal is not rapid adoption for its own sake. It is disciplined adoption tied to measurable value.

Illustrative example: A county with an existing lean administrative workforce may start with low-risk internal use cases such as knowledge retrieval, drafting routine communications, summarizing policies, or supporting help-desk workflows. The value is removing routine tasks for staff, allowing them to focus on strategic priorities.

Action Insights

- Start with low-risk AI use cases tied to internal productivity and staff enablement.
- Establish governance guardrails before scaling adoption.
- Link AI investment decisions to tangible value in staff effectiveness, constituent service, and risk reduction.
- Treat AI readiness as a combination of data, security, process, talent, and change readiness.
- Consider consortium-based or shared models where appropriate to help manage cost and build capacity on a scale.
- Create a secure internal AI sandbox for low-risk experimentation and workforce learning.
- Start workflow redesign before scaling AI, rather than automating existing friction.
- Use AI to augment scarce staff capacity, not to remove human accountability.
- Publish clear internal and public guidance on AI use, transparency, privacy, and human review.

Maintenance-heavy environments continue to limit innovation

County IT environments remain heavily weighted toward keeping the lights on. About 53% of respondents say less than 10% of their IT budget is allocated to innovation rather than maintenance. That is a clear signal that many counties are still devoting the bulk of available resources to sustaining existing operations.

Infrastructure profiles tell a similar story. Two-thirds of respondents report environments in which at least 75% of IT infrastructure is on premises, suggesting a continued reliance on legacy or locally managed environments rather than broad-based cloud or colocation models. This does not necessarily mean counties are resistant to change; rather, many are modernizing while managing security, staffing, budget, and operational constraints tied to existing environments.

The cost-efficiency strategies counties favor tend to be pragmatic and operationally grounded. The leading approaches cited are infrastructure consolidation at 55% and automation tools at 48%, followed by IT service management frameworks, generative AI (genAI) tools, and cloud migration at about one-third each. These are disciplined attempts to create room for modernization by reducing operational drag.

For many counties, modernization is less about making a single large-scale platform shift and more about deciding which systems should remain on premises, which should move to the cloud, and which may be well suited for hybrid or colocation models based on cost, risk, performance, and mission needs.

Counties should also distinguish between modernization that changes the cost structure and modernization that simply refreshes technology. Strong candidates for investment are likely those that remove recurring manual work, reduce platform sprawl, improve data consistency, and lower the ongoing effort required to operate core services. That is why platform simplification, selective ERP modernization, and targeted automation can matter more than broad technology replacement programs in constrained environments.

ERP modernization should be viewed through this same lens. For many counties, ERP can improve standardization, auditability, controls, data consistency, and visibility across finance, HR, procurement, and operations. Those benefits, however, are not automatic. In the near term, standardized workflows may feel slower or more administratively intensive than legacy manual practices, particularly for smaller departments, unless implementation is paired with process redesign, role clarity, training, and reporting enablement. ERP modernization should therefore be framed as a capacity-building opportunity over time, not as an immediate efficiency gain in each process.

Illustrative example: A county modernizing ERP may reduce duplicate data entry, shorten reporting cycles, improve visibility into finance and workforce data, and lower reliance on spreadsheets or workarounds. In a lean operating model, those gains can improve productivity and decision-making.

Action Insights

- Free up funding for innovation by targeting maintenance cost drivers first.
- Prioritize modernization efforts that reduce platform complexity and administrative burden.
- Treat ERP modernization as a business process, data, and operating-model change effort, not only a finance or IT upgrade.
- Treat cloud as a portfolio decision by evaluating workloads individually rather than assuming every system should follow the same path.
- Use automation where it directly improves service consistency, staff productivity, or risk reduction.
- Use a formal prioritization model that scores investments by capacity created, implementation risk, and operating burden reduced.
- Track business-value metrics such as staff hours saved, reporting-cycle reduction, backlog reduction, and service turnaround improvement.

Security is a priority, but gaps persist across capabilities

Security and compliance are top strategic priorities for county IT leaders, but the survey suggests capability maturity remains uneven. Roughly 63% of respondents rank enhancing cybersecurity posture and compliance among their highest priorities. While 92% report some form of advanced authentication, other core capabilities appear less consistently prioritized or deployed, indicating that many counties are still building beyond baseline protections. That maturity gap is likely most acute in smaller counties, where limited scale makes it harder to sustain specialized capabilities such as continuous monitoring, incident response depth, vendor-risk oversight, and recovery planning without shared or external support.

As counties adopt more digital workflows, cloud services, connected vendors, and AI-enabled tools, cyber risk becomes more operational and more systemic. The question is no longer only whether a county can prevent compromise, it is whether the county can detect disruption early, isolate failures, continue essential services, and recover quickly across departments. In practice, this points to an argument for a resilience model that connects identity, vendor oversight, continuity planning, incident response, data governance, and manual fallback procedures.

For smaller counties in particular, mature resilience may depend less on building every capability in-house and more on using shared services, managed detection and response, and standardized vendor controls to create coverage they cannot staff directly.

Part of the county cybersecurity agenda for 2026 is especially telling. Disaster recovery and business continuity stand out as the top priority at roughly 62%. Identity and access management follows at about 41%, with multifactor authentication near 38%. Other notable initiatives include data privacy and information sharing, training and awareness, business alignment, risk assessments, governance, regulatory compliance, cloud security, incident response, and genAI security controls.

Taken together, these responses suggest that counties are moving beyond a narrow controls-based view of cybersecurity and toward a broader resilience agenda, but many have not yet built the integrated operating model needed to support that shift. Fewer counties report capabilities such as security operations centers and network operations centers, vendor security compliance, and consistent data governance, while citizen digital identity remains rare. That pattern suggests many counties have pockets of control in place, but not yet the monitoring, coordination, and governance needed for mature cyber resilience.

The incident profile reinforces that gap. Common cybersecurity incidents over the past 12 months included viruses, malware, and financial fraud affecting local government entities. These results suggest that baseline controls alone, are not enough. Counties may need stronger detection, response, recovery, continuity, and governance capabilities to move from reactive protection to organizational resilience.

The message here is not simply to improve security controls. It is to help counties build resilience: the ability to continue operating, recover quickly, and sustain public services under stress. Cybersecurity, continuity planning, governance, and risk management should therefore be treated as part of the same county resilience agenda.

Illustrative example: A county investing in continuity planning, incident response playbooks, vendor risk management, and cross-functional governance is not only improving cyber posture. It is improving the county's ability to maintain essential operations during disruption

Action Insights

- Connect security efforts more consistently across identity, infrastructure, vendors, data, and continuity planning.
- Strengthen recovery and continuity planning across the enterprise, not only within IT.
- Expand focus from internal authentication to broader resilience, including citizen-facing identity and service continuity.
- Measure how well security and resilience programs are working, not just whether activities were completed.
- Prioritize governance models that integrate cybersecurity, risk management, and operational continuity.
- Treat business continuity exercises as enterprise drills, not IT-only tests.
- Add manual override and service-continuity planning for critical public operations.
- Standardize vendor cyber assessment requirements.
- Consider MDR / SOC-as-a-service where internal scale is limited.

Digital experience and advanced capabilities remain underdeveloped

While counties have invested in infrastructure and core cybersecurity, constituent-facing digital experience is still maturing. No respondents report delivering fully enhanced, personalized, and effective constituent experiences, and only 25% describe their digital platforms as advanced, integrated, scalable, and user-friendly.

Many counties remain in the middle. About 57.5% describe their digital environments as developing, with some advanced features but not full integration or scale, while 17.5% remain in earlier-stage models with basic online services and limited functionality. That suggests counties have laid some groundwork, but many still lack the architectural, product, and governance capabilities needed to deliver consistently modern constituent experiences.

The same pattern appears in training and specialized services. Training is common, reported by 86% of respondents, but only 21% say they have program measurement and reporting in place. Likewise, technical infrastructure security is nearly universal, but more advanced capabilities, including emerging technology programs, investigations, and forensics, are less common. This is the classic sign of uneven maturity: strong activity at the operational layer, weaker capability at the measurement, integration, and innovation layers.

Modern digital experience is not only about better resident interaction. It is also about simplifying processes, improving access to data, and increasing efficiency. In that sense, digital modernization and ERP modernization are closely linked. Both can reduce manual effort, improve service consistency, and create capacity across the organization.

Counties should view digital experience not as a front-end design issue, but as an operating-model issue. When staff are consumed by maintenance and manual work, constituent experience inevitably stalls. Better digital services usually require the same underlying capabilities that improve internal operations: cleaner workflows, stronger data practices, clearer ownership, better measurement, and more reusable platforms.

This is also where human-centered change matters. Organizations adapt more effectively when change is personalized, supported by feedback loops, and tied to day-to-day work rather than imposed as a one-time program. For counties, that means pairing digital modernization with practical training, role clarity, usage measurement, and feedback mechanisms that show where adoption is working and where friction remains.

Action Insights

- Improve staff and constituent experience through targeted modernization of core platforms, including ERP, licensing and permitting, and bill payment, with a focus on reducing manual workload and improving staff productivity as well as service quality.
- Add measurement disciplines to training, security, and service programs.
- Build governance capabilities that connect operational delivery to business outcomes.
- Invest selectively in advanced capabilities that close sizable service, resilience, or workforce-capacity gaps.
- Tie every digital modernization effort to adoption, usage, and service-quality metrics.
- Build continuous feedback loops into training and rollout plans.
- Focus initial investment on high-friction services such as permitting, payments, case management, and internal service requests.

County IT leadership has broad accountability, and limited capacity

County IT leaders manage broad portfolios with relatively small teams. Nearly half of respondents operate with 10 or fewer full-time staff supporting county IT, and only about 39% report staff of 20 or more. The operating model is also highly centralized, with the CIO or IT director functioning as the overwhelming primary mechanism for delivering internal IT services and support.

This matters because centralized accountability without commensurate scale tends to push organizations toward generalist operating models. In practice, that can help preserve responsiveness and clarity of ownership, but it can also make it harder to build depth in specialized domains such as advanced cybersecurity operations, enterprise data governance, digital product management, ERP modernization, and AI enablement.

Funding structure adds to this challenge. The implications differ by county size. In smaller counties, the challenge is often basic scale and access to specialized talent. In mid-sized counties, it is balancing growing complexity without equivalent staffing growth. In larger counties, it is coordinating across more systems, departments, and governance layers. Counties rely predominantly on local sources, especially fees and property taxes, while grant funding, chargebacks, federal pass-throughs, and state appropriations play supporting roles. As a result, leaders often have to balance resilience, modernization, workforce considerations, and service improvement within a defined operating environment.

The future implication is clear: county IT leadership is expanding from technology oversight into enterprise capacity leadership. CIOs are increasingly expected to help counties build resilience, improve staff productivity, enable better decision-making, modernize the service experience, and guide responsible adoption of technologies such as AI. That is a larger mandate than traditional infrastructure management, and it raises the importance of governance, prioritization, and selective investment.

County CIOs are also inheriting a workforce design challenge. Lean teams cannot keep scaling through headcount alone. They will need a blend of simplification, automation, shared services, external

collaborations, and more intentional human-machine collaboration. That shift requires more than tool deployment. It requires redesigning work, clarifying where human judgment matters most, and giving staff safe ways to experiment with new tools and practices.

More broadly, county IT leaders may need to organize less around narrow technical silos and more around cross-functional capabilities or service domains. In settings where specialized headcount is limited, cross-functional delivery models can improve responsiveness, strengthen business alignment, and reduce the handoff friction that slows modernization efforts today

Action Insights

- Align IT strategy explicitly to county mission outcomes and service delivery, not just technical priorities.
- Prioritize a small number of enterprise capabilities where shared services can create scale.
- Build operating models that reduce dependence on a few key individuals.
- Focus modernization investments on areas that can create measurable organizational capacity.
- Use grant and external funding opportunistically, but do not anchor core operations to them.
- Reorganize around priority capabilities or service domains where possible.
- Use job-to-capability redesign workshops to identify repeatable work suitable for automation.
- Dedicate a fixed share of modernization funding to training and change adoption.
- Build ‘digital playground’ environments for safe experimentation and workforce learning.

Implementation playbook for county CIOs

Counties do not need modernization for modernization's sake. They need a disciplined portfolio of investments that reduces administrative drag, lowers technical risk, and releases scarce human capacity.

- Prioritize for capacity creation
- Score investments by hours saved, risk reduced, service improved, and maintenance load removed.
- Modernize operating models, not only systems
- Use cross-functional teams, workflow redesign, and shared capabilities.
- Govern AI and cyber security together
- Treat privacy, vendor risk, resilience, and AI controls as one governance agenda.
- Build workforce adaptability deliberately
- Use training, sandboxes, feedback loops, and role redesign to support adoption

Conclusion

For many counties, the path forward is not sweeping transformation. It is disciplined modernization that creates capacity as it goes. The counties well positioned for the next several years will likely be the ones that reduce maintenance drag, redesign work where AI can safely augment people, strengthen resilience across both technology and operations, and measure modernization by the capacity it creates for staff and service delivery. In that sense, the county CIO's mandate is expanding from running technology to helping the county build a more adaptive, resilient, and effective operating model.



This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. In the United States, Deloitte refers to one or more of the US member firms of DTTL, their related entities that operate using the "Deloitte" name in the United States and their respective affiliates. Certain services may not be available to attest clients under the rules and regulations of public accounting. Please see www.deloitte.com/about to learn more about our global network of member firms.