Falling behind on zero trust?

Five things you can do to help get back on track

Why modern government is important

Government agencies in the US must modernize in order to keep up with changing user needs, regulations, and health and public safety requirements. Leaders of modern governments rethink business processes and service delivery models to more effectively achieve their mission. This article is one of a series that features how modernizing affects the government workforce and the user experience, improves security and public trust, and accelerates the digital journey. KPMG team members offer insights intended to help guide governments in their modernization efforts to encompass all processes, technologies, policies, and the workforce so each works together to create connected, powered, and trusted organizations.

Coming to grips with the complexity of zero-trust security

As fiscal year 2027 (FY27) draws ever closer, many government agencies are struggling to comply with the federal directive requiring all government agencies to adopt a zero-trust (ZT) security approach and architecture. By the end of 2024, the Department of Defense, for example, reported it had completed just 14 percent of its target ZT activities.[1] That's a lot of ground to make up in a short amount of time.

The principles behind ZT are deceptively simple: Treat both internal and external networks as insecure. Assume that if attackers are not already on the network, then they will be eventually. Continually verify the identity of every person, device, or system requesting access to a network resource, and ensure they're given least privileged access to it. But as agencies are discovering, the engineering and architectural decisions and technology implementations required to achieve the ZT principles are anything but simple.

Inadequate funding, duplicative efforts, limited implementation expertise, competing priorities, nonaligned stakeholders, weak governance, and poor coordination are hampering ZT progress to varying degrees across many government agencies. Despite these obstacles, progress is being made, but the friction is negatively impacting cost, timelines, and long-term capabilities, including warfighting readiness. Adversaries will not wait for federal networks to be ready.

Much of the friction stems from the way agencies have historically approached IT implementations, prioritizing just a few for delivery each year. As a result, many have treated ZT as a portfolio of independent technology implementations run by different stakeholder groups with separate contracting teams operating under disconnected governing directives.

However, ZT isn't a technology implementation—it's an organizational transformation. If it were an implementation, then it would be far simpler to comply with the ZT mandate—specify what software is required, install it, and check the box "done." But as a transformation, delivering a fully implemented ZT architecture (ZTA) within the next few years requires deploying far more capabilities each year than agencies are accustomed to and doing so in an integrated, aligned, and appropriately sequenced manner.

To meet the FY27 ZT mandate, government organizations must appreciate the magnitude of this transformation. While new technology is required, in our experience, it's rarely the technology that's the complicated part, even in government environments, with their tangled web of aging legacy systems, cloud-based solutions, and cybersecurity and compliance challenges. It's almost always the organization that's the real challenge—the "business" side.

[1] C. Todd Lopez, "Zero trust architecture could prevent adversary data theft, protect war fighters," US Department of Defense, February 26, 2025

Start by asking the right questions

It may be tempting for agency leaders to address the FY27 ZT mandate and any schedule slippages by requesting deadlines move to the right or by re-evaluating which technologies are truly required to be ZT *compliant*. Given there are no definitive assessment criteria for an acceptable ZTA, and deadlines are regularly rebaselined or shifted, these may be viable approaches.

However, a better approach is to avoid getting lost in the requirements and scale of ZT, and instead perform an honest evaluation of the organization's current technologies, processes, and network designs. Then, identify the specific ZT targets at the agency level based on mission, funding, existing technology stacks, workforce skill sets, and strategic goals. Start by answering the question: *What does ZT look like for my organization and specific mission?* Not every ZT capability requires a tool acquisition, for example, so think carefully about which tools are necessary, provide the best security return on investment, and integrate well within your organization's existing tech stack.

The questions demanding answers don't stop there. How will the journey to ZT be tracked? How will you know when you've reached a sufficient enterprise ZTA? How will you track or verify that the requisite ZT components have been incorporated into the different processes and systems throughout the organization?

Stakeholders at all levels of the organization will have their own questions. What is the plan or strategy to achieve ZT? What will be guided from the top of the organization and what will be left up to stakeholders to figure out? What existing technologies can be leveraged? What new technologies will be acquired at the enterprise level, and what must be acquired at the department level or by application owners? Failing to fully communicate what's expected of stakeholders will leave them with more questions than answers.

ZTA is more an evolution of security architecture than a wholesale replacement, and so it's likely that stakeholders throughout the enterprise have already implemented solutions or processes that align with top-down ZT mandates. However, without a clear plan and communication of expectations and responsibilities from the top, it may be difficult or impossible to know what can be leveraged or repurposed. Many application owners, for example, likely have already implemented a Security Information and Event Management (SIEM) solution, analyzing log data to automatically detect anomalous access or security issues. But is the solution they've implemented acceptable? How must it integrate with the broader enterprise architecture? Is a centralized solution available that could be used instead, which would eliminate the extra licensing costs of such localized implementations? What is a ZT-worthy SIEM solution?

It's not only the IT teams who will have questions. Auditors, for example, must now understand what they're measuring, and the organization must understand what they're being measured against, not only from a security perspective but also from a financial perspective. How do you measure ZT return on investment? How do you score or assess a ZT architecture?

There are no "right" answers to any of these questions. The path to ZT will vary organization to organization. There's tremendous flexibility in ZT and the way a ZT architecture is achieved, including what solutions and processes can or should be used. There are many decisions that must be made throughout the organization to deliver on ZT, but it's difficult to make decisions and evaluate options inside a vacuum of information. The key is to start by asking thoughtful ZT questions that account for your organization's mission, context, and operational requirements.

Five essentials for getting—and keeping—ZT efforts on track

Beyond improved security, ZT is also a business/mission enabler, breaking down siloes and facilitating secure and seamless collaboration across different networks, platforms, applications, and data stores. The network perimeters may be gone, but in a properly deployed ZTA, so, too, are the constraints they may have imposed. Resources may now be scattered across on-premise, cloud, and hybrid environments, but the user experience to access them should be seamless. However, enabling such broad technology integration first requires broad stakeholder collaboration and thorough human-centered design.

Because it's a transformation, ZT ultimately can change the culture of an organization. It will change not only the way an organization approaches security, but also how it deploys new systems, applications, and technologies and how it architects the overall enterprise IT environment. As with any digital transformation, ZT requires informed technology and architecture decisions as well as robust change management, stakeholder engagement, organizational understanding, and integration between technology platforms and business units. It requires buy-in at all levels of the organization—including the administrators, application owners, and engineers with their hands on the keyboards executing and implementing the necessary tools and configurations.

So, how are you going to achieve this? We see five things you can do to help realize and sustain the benefits of ZT in the shortest possible timeframe.

1 Establish a strong central ZT program management entity

Given the magnitude of the organizational transformation, even the most well-crafted ZT strategy will fail without effective communication and broad cooperation and collaboration. Such a strong foundation is necessary not only to enable technical implementations, but also to catalyze the broader transformation and fully capitalize the value of ZT.

This is the job of a centralized ZT program management entity—a program management office (PMO) or functional management office, for example. This ZT management entity serves to:

- Articulate and drive a common ZT vision and strategy across the entire organization.
- Identify champions for each ZT pillar—user identities, device security, application and workload security, network security, automation, and analytics. It oversees and coordinates the individual PMOs or champions that would manage efforts across the ZTA.
- Identify dependencies, then sequence and synchronize the individual capability implementations (e.g., identity, credential, and access management [ICAM] and microsegmentation) and create standardized methodologies and project approaches for how the individual capabilities are deployed.
- Define metrics, goals, and objectives that provide an organization the big picture of the ZT journey instead of leaving those up to the individual project teams.
- Help ensure new technology acquisitions or tool selections are vetted within the context of the larger ZTA to avoid redundancies, incompatibilities, and excessive cost.
- Coordinate activities at the organizational level across individual business units, including IT, human resources, finance, and operations.
- Sustain capabilities with long-term support and resourcing identified, effectively integrating capabilities into change management, asset inventories, centralized logging, etc.

A central, authoritative structure is key to ZT success, and the lack of one can undermine efficiency, strain stakeholders, and extend implementation timelines.

2 Spend more time on design and dependency mapping

There's a tendency to rush to implementation, especially when falling behind on schedule and especially in government projects. It's not unusual, for example, for government contractors to be told they must deliver an implementation plan within 20 days of a project start. But the rush to implementation inevitably will shortchange the design and planning phase. With the number of moving parts that come with ZT, shortchanging the dependency analysis can lead to significant pain down the road.

For example, we've seen ZT technologies deployed in an environment set to be decommissioned soon thereafter. The inevitable migration and reconfiguration challenges could have been avoided had this dependency been identified and deployment scheduled based on the new environment's readiness.

Take the time to develop detailed dependency maps within an integrated master schedule that clearly delineates how each capability impacts others on the ZT roadmap. Prioritize capability deployments by their return on security investment, not just whether they have the funding but whether they can be successfully deployed based on all the projects' dependencies.

3 Less talk, more listening

There's a temptation for IT leaders to dictate how ZT efforts will be implemented within agencies or departments, especially if the organization head is not technically minded.

The result is that ZT can often feel like trying to force a square peg into a round hole because of a failure to account for the different dependencies of an organization—the different contexts and priorities around why an organization is operationally run the way it is. It's not unusual to spend hours in meetings trying to solve issues that should have never arisen in the first place if the organizational needs were better understood and accounted for in the initial design. Thoroughly understanding and evaluating the requirements for each ZT capability will pay dividends in the long run. Inevitably, changes and adjustments will be necessary, but the changes should be fine-tuned modifications rather than systemic, structural changes late in the ZT architecture deployment.

4 More agile, less waterfall

Given the size of government projects, there's often an assumption that a linear, sequential waterfall approach is the only way to execute. But once implementation has begun, the farther down the waterfall you go, the more difficult and costly changes can be given the dependencies at each step. The inertia of the sunk cost fallacy, too, can keep projects headed on their original course even when it becomes clear that a course correction is required. Everyone has a tendency to spend a little more time hoping it's going to work.

Given the complexity of ZT transformation, however, course corrections are almost guaranteed. You must be willing to stop and continually rethink and redesign ZT efforts early and at every step. Embracing agile methodologies—or at least the agile mindset—is essential for success.

5 Get the timing right

As you march onward with your ZT mandate, keep in mind that the leaders in the organizations you'll engage with all have day jobs—advancing the mission of their agency or department—and that ZT can easily be seen as a distraction from that mission. Your priorities and schedules may not mesh with theirs. But nearly every government organization will have peaks and ebbs in their schedules. Find the ebbs. Make this part of your dependency analysis. Operational tempo inevitably varies and ZT capability deployments can seek to leverage the lulls versus trying to force a new initiative when resourcing and manpower cannot sustain or support it.

How KPMG can help

ZT is much more than a compliance effort. It's essential to help ensure that government agencies—especially those with existential responsibilities—are able to consistently and reliably achieve their missions in a world where technology has become both an indispensable asset and a significant vulnerability.

We help government organizations achieve their ZT objectives with strategies, technologies, and organizational transformations that can improve the effectiveness of cybersecurity capabilities, reduce control complexity, and lower the costs of complying with regulatory mandates.

ZT program management – A successful ZT implementation demands an effective vision and strategy. We can help by analyzing gaps between your current and desired states, synchronizing capability implementations, coordinating activities across ZT pillars, and establishing a strategic communications approach with stakeholders. We can also help you perform advanced data collection to increase efficiency, reduce stakeholder strain, and accelerate implementation timelines.

ICAM transformation – We take a holistic approach to ICAM. We can help you automate manual processes, reduce user friction with just-in-time provisioning, centralize access decisions and authorization matrices with streamlined roles and attribute-based authorization, and leverage platform reporting capabilities to strengthen segregation of duties and access request policies.

ZT networking and architecture – Fine-grained network segmentation is a key component of a ZTA. We can help you bring the protection of a firewall to the application level to increase granularity of control, enhance network visibility, reduce the organizational attack surface, and improve control of east-west network traffic to reduce adversarial lateral movement on the network.

Why KPMG

KPMG LLP (KPMG) has worked with federal, state, and local governments for more than a century. We have over 1,500 dedicated cybersecurity professionals worldwide, and have been recognized by Forrester, IDC, and ALM Intelligence as a leading global organization of professional services in cybersecurity.[2,3,4]

We're a multidisciplinary organization with business, technology, data and AI, risk, audit, and change management professionals working together as one team. We combine our cybersecurity acumen, government operations experience, cross-sector and cross-disciplinary skills, and alliances with leading technology providers to deliver robust ZT solutions to address your organization's most pressing needs.

Because each organization is unique, we take a collaborative, client-centric approach. We'll work closely with you to understand your specific needs and tailor our solutions to meet them. We see our role as a trusted adviser, drawing upon our multidisciplinary skills and experiences to foster an exchange of ideas that challenge assumptions and spark innovation.

[2] ALM Intelligence Pacesetter Research, April 2022

[3] "IDC MarketScape: Worldwide Cybersecurity Risk Management Services 2023 Vendor Assessment," October 2023

[4] "The Forrester Wave, Cyber Risk Quantification, Q3," 2023

About KPMG

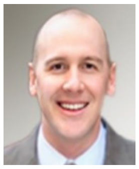
Our team understands the unique issues, pressures, and challenges you encounter in the journey to modernize. We draw on our government operations knowledge to offer methodologies tailored to help you overcome these challenges and work with you from beginning to end to deliver the results that matter.

The KPMG team starts with the business issue before we determine the solution because we understand the ultimate mission. When the way people work changes, our team brings the leading training practices to make sure your employees have the right knowledge and skills. We also help your people get value out of technology while also assisting with cloud, advanced analytics, intelligent automation, and cybersecurity. Our passion is to create value, inspire trust, and help government clients deliver better experiences to workers, citizens, and communities.

Contact

Talk to us about how we can help you implement a successful ZT program in your government organization.

Tyler A. Carlin
Director, Advisory
KPMG LLP
240-306-5097
tcarlin@kpmg.com



Nate Deshong
Director, Advisory
KPMG LLP
843-327-6641
ndeshong@kpmg.com

Al Yeasin
Director, Advisory
KPMG LLP
703-380-3774
ayeasin@kpmg.com

read.kpmg.us/modgov

KPMG

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

Learn about us: in **kpmg.com**

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.