Seven key lessons for a successful zero-trust transformation in government

The changing security landscape

Like their private sector counterparts, government agencies are grappling with a fundamental change in how employees expect to work. The shift to a remote and hybrid workforce has created a need to expand the security perimeter, allowing access from anywhere and often with any device. Increasingly, the partners, contractors, and suppliers in the organization's technology ecosystem demand the same access, and maintaining that freedom is critical to fast collaboration and timely delivery.

This is exactly what a **zero-trust architecture (ZTA)** was designed for. Traditional perimeter-based security models are insufficient in this context, where the perimeter is not well defined. This shift has introduced new vulnerabilities, making agencies more susceptible to data breaches, ransomware, and cybersecurity attacks. To mitigate these risks, agencies must move toward ZTA, where trust is never assumed and identity is continually verified.

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.

The seven essential lessons

We regularly identify recurring challenges and the ways leaders effectively overcome them through our support of commercial and federal clients in planning and executing their zero trust (ZT) journeys. While there are many lessons we've learned along the way, there are seven that stand out as essential for any government organization looking to begin its ZT journey.

1 ZT is a transformation, not an implementation

Perhaps the biggest misconception we often see is that ZT is a technology problem and can therefore be solved by technology alone.

A well-designed, engineered, and organizationally aware ZTA is the mechanism for incorporating ZT principles into an organization. However, looking at the ZT journey solely as a technical implementation often overshadows its transformative nature and limits its value to end users and the business. 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. 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.

2 Remember your people

Bandwidth constraints often pose significant challenges to technology projects and initiatives; however, the aggressive timelines, extensive target capabilities, and high expectations for implementing a ZTA can magnify these issues. This can make ZT efforts feel cumbersome and draining, especially when considering the length of the journey.

Agency leaders and ZT champions must remember that every ZT capability and project requires someone to implement a tool, alter configurations, re-engineer processes, collect data, and/or take actions. Unfortunately, in today's understaffed security, architecture, and operations teams, this means relatively small pools of personnel disproportionately feel the burden of implementing ZT. It is important, therefore, for these ZT implementers to understand why ZT is being adopted, how the framework will be leveraged, and what tools will be used along the journey.

To do this, it is important to socialize the various initiatives and how they impact the organization, enable your teams to plan proactively, and coordinate initiatives to help remove strain from stakeholders. If a ZTA is successfully deployed but the organization loses talent due to burnout, or other security activities such as patching, configuration hardening, or vulnerability management suffer, then ZT provided no net security value. Remember your people and bring them along on the ZT journey; share the vision, give the context, and enable your people to be a part of the transformation.

3 Establish a PMO

The ZT journey encompasses a multitude of new capabilities and initiatives spanning different cybersecurity domains. A cohesive ZTA requires the individual initiatives to align, integrate, and work synergistically in order to streamline this journey, eliminate silos, and realize value.

This requires establishing a single, centralized organizing entity or program management office (PMO) to champion a unified approach from start to finish. This entity serves to articulate and drive a common ZT vision and strategy, sequence and synchronize the individual capability implementations, and coordinate activities at the organizational level across individual business units, including IT, human resources, finance, and operations. This central PMO would then oversee and coordinate a network of individual PMOs or liaisons/leads that would manage efforts within each of the seven ZT pillars:

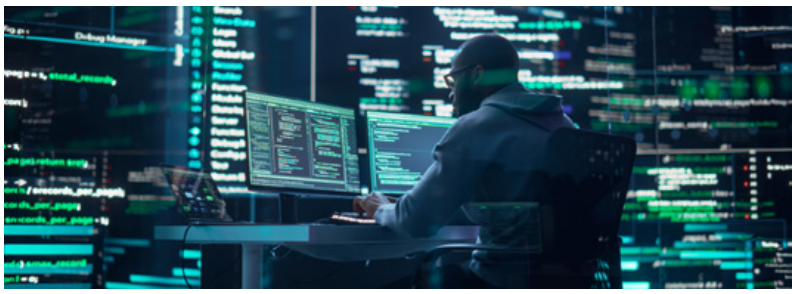
- Securing users, both employees and constituents
- Securing devices, from user phones and laptops to Internet of Things devices
- Safeguarding applications and workloads
- Protecting data, including encryption and controlled access
- Network and environment, including physical segmentation and granular access controls
- Automation and orchestration, such as automated policy enforcement
- Visibility and analytics, including artificial intelligence to improve threat detection.

The lack of a PMO structure like this can undermine efficiency, strain stakeholders, and extend implementation timelines.

4 Build thoughtful and flexible governance

Governance decisions made in one ZT pillar inevitably impact other areas within the organization, given ZT's wide reach across an organization. It's crucial to establish governance that holds an organization accountable while minimizing operational hindrances. Individual ZT pillars or project leads often develop tactical governance frameworks that focus on a specific technology's implementation, operation, and maintenance, ensuring stakeholders are guided throughout the adoption. However, this leads to discrepancies and variations of how ZT is governed across pillars.

Instead, governance should primarily flow from the ZT PMO down, while also accommodating specific exemptions flowing from the ZT pillars and project teams upward. This dual flow caters to the individual needs of various projects but also maintains an overarching set of right and left limits for ZT policy and doctrine. The ZT PMO should foster cross-collaboration among ZT pillars to construct a wholistic governance framework for the ZT program. Integrating ZT into an organization's change management processes helps ensure compliance with ZT policies and procedures, while also mitigating the common problem of only considering security as an afterthought. Governance must be rigid enough to enforce standardization, alignment, and integration but flexible enough to prevent stifling individual capability implementations.



5 Empower and engage stakeholders

Stakeholders frequently resist change due to concerns around resource constraints, system impacts, and conflicting priorities. Empowering and engaging stakeholders throughout the entire ZT journey is crucial. Stakeholders need to understand the vision and their place in it. Building a ZT strategic communications plan and messaging campaign enables stakeholders to understand the organization's rationale for ZT adoption, how it contributes to the mission, and how it will be achieved.

Strategic communications should be leveraged prior to initiating projects to socialize goals, identify impact to stakeholders, and understand expected timelines. Messaging campaigns proactively address common concerns, establish regular communication channels, and engage stakeholders throughout the ZT journey. The more employees and stakeholders clearly understand the vision, benefits, and impact to day-to-day operations, the more resistance and doubt give way to engagement and action, and ultimately a successful ZT project.

6 Collect the data…once

In today's data-driven business landscape, stakeholders are inundated with continuous, overlapping, and uncoordinated data requests. This can result in wasted resources and alienated stakeholders as leaders expend valuable resources addressing data requests versus executing priority initiatives. Stakeholders often find themselves spending significant time gathering bespoke data for various ZT projects and stakeholders without understanding the context behind the data requests. These redundant or duplicative data requests not only burden project stakeholders but also the system administrators, operators, engineers, and "hands on keyboard" personnel necessary to deploy ZT capabilities.

Instead of each ZT project or capability amassing a slightly different version of the data set, use your PMO. The ZT PMO should collect, clean, and disseminate ZT data in a way that can be consumed by the individual project teams. If there are known data "sources of truth," then all the project teams should populate and enrich these central repositories with new data discovered during ZT implementations. This approach collects all necessary data in one go, enabling ZT project teams to focus on deploying capabilities and accelerating delivery timelines. Being proactive and structured in data collection allows for streamlined ZT project delivery, provides better data insights, and helps eliminate wasted effort.

7 Build the foundation

Leverage existing tools first, where fit, and procure additional tools as necessary to enable a cost-effective ZT journey. Organizations often gravitate to procuring a new technology first before evaluating how existing technologies may be adjusted to provide similar security. Even worse, sometimes technologies are procured in a vacuum without sufficient consideration for organizational risk and context.

Prior to acquisitions and procurements, an effective ZT journey starts with refining current processes, leveraging existing technologies, and defining the requirements of additional ZT tooling to be procured. In advance of executing a ZT roadmap, organizations must maintain a mature asset inventory, configuration/vulnerability management program, patching program, and incident response capability. Understanding what's in your environment and operating a mature security program is a fundamental necessity in today's cybersecurity landscape; moving towards a mature security posture cannot wait on a fully deployed ZTA. Organizations effective at these security basics will transition to a ZTA and reap the benefits of ZT faster and cheaper. Harness current tool and process capabilities to harden networks and build a solid day-to-day security program. With this foundation in place, undertake the ZT journey with assurance today's security will hold while a longer-term ZTA is deployed.

Experience that matters

Through our years of experience helping numerous federal and commercial clients reimagine, redesign, and reengineer their IT architectures and security capabilities, we know that ZT transformation is a more complex and involved journey than implementing a technology—it's far from over when the technology is installed. Indeed, because the world continues to evolve, the journey rarely ends.

For example, we helped a large US Department of Defense (DoD) client accelerate its ZT journey, not only with technology implementation, but also with the strategic communications, data analytics, and stakeholder management necessary to complete the broader transformation. Despite the project's complexity and aggressive timelines, KPMG was able to deliver, relying on our time-tested methodologies and innovative and collaborative approach. We continue to support the client with advice, targeted recommendations, and updated processes based on feedback and lessons learned as it seeks to continually improve its security posture.

How KPMG can help

With more than 9,300 cybersecurity professionals, KPMG is well equipped to help you understand and manage your cybersecurity threat landscape, with services and methodologies designed for your organization's unique risk tolerance, mission, stakeholder dynamics, security culture, and regulatory environment.

Our incident responders can help conduct forensic analysis and provide timely threat intelligence. Our cybersecurity professionals can help build data-driven threat profiles to help prioritize resources and deployments of security controls. And our security engineers and cloud architects, in conjunction with our more than 30 technology alliance partners, can help you transform your infrastructure to address the increasing complexity of today's network environments; the growing expectations of leaders, employees, and constituents; and the expanding and constantly evolving cybersecurity threat landscape.

KPMG has worked with federal, state, and local governments for more than a century. We have significant experience implementing ZT in both the private and public sectors. We bring that experience and our well-honed methodologies to every engagement, helping you to navigate the complexities, nuances, and transformative nature of a broad ZT journey—and deliver results that matter.

About KPMG

KPMG has worked with federal, state, and local governments for more than a century, so we know how agencies work. 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.

Contacts

Tony Hubbard
Principal, Government Cyber Security Leader
KPMG LLP
202-486-4945
thubbard@kpmg.com

Tyler A. Carlin
Director, Advisory
KPMG LLP
571-243-5655
tcarlin@kpmg.com

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

---

read.kpmg.us/modgov

KPMG