MODEL OVERVIEW REPORT

Your Next-Generation Cloud Strategy Model, US Government Edition

September 22, 2025

By Devin Dickerson with Lauren Nelson, Lee Sustar, Tracy Woo, Naveen Chhabra, Bill Martorelli, Dario Maisto, Brent Ellis, Caroline Bonde, Kara Hartig

FORRESTER®

Summary

Federal cloud leaders must empower their organizations with modern cloud technologies to achieve high-performance mission-focused outcomes. More than a decade since the cloud-first mandate, most organizations are well on their journey. They strive to advance their cloud programs with secure and resilient platforms, mission-centric partners, and advanced internal practices. The Next-Generation Cloud Strategy Model, adapted for the US federal government, comprises seven key principles for success in each category, which leading organizations embrace. Organization leaders should weave them into the core of their cloud programs to accelerate modernization and enhance mission delivery.

Federal Organizations Must Evolve Their Cloud Strategy For The Future

In the early days of federal cloud adoption, migrating a single system was newsworthy. Today, the scale and sophistication are vastly different. We see the US Department of Defense's (DoD's) Platform One initiative enabling secure software development across services and organizations leveraging the Technology Modernization Fund to overhaul critical customer-facing services with cloud-native solutions. Leading organizations aren't just exploring the cloud; they are fully immersed, managing complex multicloud environments. With more than a decade of experience, organizations should rethink federal cloud strategy to address these advancements (see Figure 1). At a basic level, every organization needs to define the following:

- **A cloud-smart North Star to guide the journey.** Every cloud strategy needs guiding principles that inform real-time decisions. For the federal government, this is the cloud smart policy, which emphasizes security, procurement, and workforce. Your organization's North Star should reflect this national strategy, customized to your specific mission objectives. Even experienced federal leaders face challenges: They must sift through legacy systems, analyze acquisition options, decipher real policy barriers from perceived ones, and determine the best path forward that balances mission needs with budgetary realities under the planning, programming, budgeting, and execution process. Customize your cloud strategy for your business, as the DoD did with Cloud One.
- **A modern operating model.** Cloud is no longer a specialty infrastructure stack isolated from the rest of the enterprise; it's the standard. Any practice or operating model must be designed to serve its needs. Your operating model must define your customers (stakeholders, engagements, outcomes), value (value streams, offering, value proposition, value orchestration), capabilities (application, data, process, people, infrastructure), structure (definition of work, operating units, location, interactions, reporting lines), governance (decisions, accountability controls, transparency), and leadership (strategy, vision, culture, values, performance, motivation).
- **A documented strategy and roadmap.** Documenting your cloud strategy reinforces and communicates your mission-aligned goals. It establishes your organization's specific approach, such as a multicloud posture, a preference for platform as a service (PaaS) to abstract complexity, adherence to FedRAMP, and a timeline for achieving Zero Trust objectives. Your roadmap reinforces the strategy by showing its progression and key milestones.

- **An integrated cloud governance and resilience plan.** The cloud exists outside traditional network perimeters. Therefore, a robust governance plan is a critical first step. This begins with leveraging FedRAMP to ensure a secure baseline for all consumed services. Organizations then build on this with multiple accounts and landing zones to isolate controls and meet regulatory needs. Atop this foundation, organizations must implement a Zero Trust architecture (ZTA), as mandated by EO 14028. You must clearly define this plan from the start and evolve as the organization's cloud footprint matures.
- **An optimized and compliant tech stack.** The cloud ecosystem is rapidly evolving. A formal process must be in place to manage your organization's tech stack, which includes not only the major cloud platforms (e.g., Amazon Web Services, Azure, Google Cloud Platform) but also a vast array of enablement technologies for security, management (e.g., FinOps, infrastructure automation), and development. All components must be evaluated for FedRAMP authorization and alignment with your ZTA implementation. Navigate these decisions with The Forrester Tech Tide™: Cloud Governance And Enablement Technologies, Q4 2020, and Forrester's Essential Research For Selecting Cloud Technologies And Services.
- **A foundation to streamline innovation.** The cloud's most important value is as an innovation platform for the mission. By creating a foundation of secure landing zones, continuous integration/continuous delivery (CI/CD) pipelines, and preapproved services (a paved road), organizations can empower teams to experiment and deliver new capabilities rapidly without the friction of lengthy manual security and compliance reviews. If you're not using the cloud to accelerate the delivery of value to the warfighter or other customer, you're missing out on its most powerful proposition. If you're facing tough times and having difficulty fathoming an innovative culture, think about small innovations (i.e., lightning bugs, not lightning) focused on solving the problems at hand rather than grand efforts of brilliance.

Figure 1

Moving Past Yesterday's Cloud To The Next Generation Of Cloud

	Yesterday	Today and beyond
Scale	Eighty percent of the federal IT budget for operations and maintenance (O&M)	Strategic shift to large-scale multibillion-dollar enterprise cloud contracts (e.g., agency-specific IDIQs, GWACs); focus on reducing legacy O&M costs and using modernization funds (e.g., the TMF) to deliver mission value
Number of cloud(s)	Single cloud or accidental hybrid	Strategically multicloud; increasingly hybrid cloud or, in some cases, hybrid app
Type of cloud services	Largely infrastructure services	A mix of infrastructure, data, and development services
Scope	One department, or a handful of them, using cloud for isolated use cases	Major cloud migration/modernization efforts and central platform for innovation
Governance	Agency-specific security assessments, focus on perimeter defense, and governance that is managed through manual checklist-based authority-to-operate (ATO) processes for individual systems	Governance that starts with FedRAMP for provider authorization, with agencies then implementing a Zero Trust architecture as mandated by executive order, which is enabled by landing zones, FinOps for cost governance, and the ultimate goal of policy as code to achieve a continuous ATO
Resilience	Failure with same ability-zone (AZ) recovery	Multi-AZ recovery and resilience engineering

Set The Vision With The Next-Generation Government Cloud Strategy Model

Each organization's cloud strategy will be unique, but leading federal cloud programs share common characteristics. They demand technology platforms that are secure, innovative, and transparent. They seek to build true partnerships with industry, focused on trust, mission outcomes, and cocreation. And they are adopting modern internal practices to handle the speed and complexity of 21st-century government. This approach is the Next-Generation Cloud Strategy Model. The model has three sections (see Figure 2):

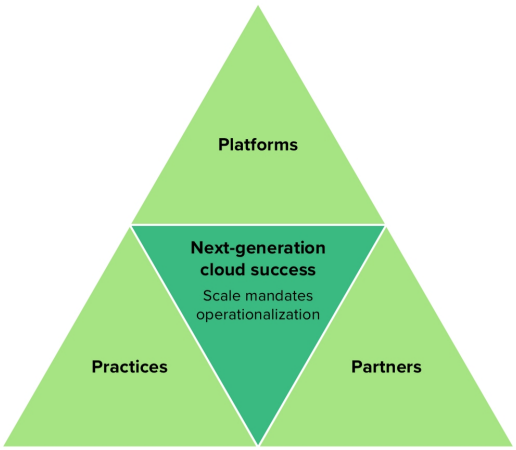
- **Platforms powered by continuous innovation.** Technology is at the heart of every cloud strategy. Leading organizations are raising their standards, expecting providers not only to be FedRAMP authorized but also to embrace modern product techniques, transparently share roadmaps, and actively address feedback from the federal community.
- **Partners dedicated to mission success.** Embracing the cloud requires a host of changes to policy, process, and workforce. Organizations rely on a collection of

partners — from global systems integrators (GSIs) to independent software vendors — to help them succeed. The modern federal partnership is shifting from transactional input-based contracts to flexible outcome-based relationships centered on achieving mission objectives.

- **Practices enabling the speed of mission.** To take full advantage of modern platforms, organizations must update their practices. This means organizing into platform teams, transforming system administrators into site reliability engineers (SREs), embracing DevSecOps, and baking security and resilience into every stage of the lifecycle through practices like policy as code.

Figure 2

The Next-Generation Cloud Strategy Model



Platforms	Partners	Practices
• Intelligence and automation • Abstracted complexity • Composable experiences • Platform teams • Diversified risk • Workload-affinity enablement • Modern cloud-native architectures	• Automation- and analytics-powered offerings • Platform-based elements • Advisory-led strategy • Responsiveness and flexibility • Transformation • Cocreation • Outcome- and experience-oriented goals	• Product-led strategy • Agile-plus-DevOps • SRE and platform engineering • FinOps and ITFM/TBM • Zero Trust and app security • Creative resilience • Policy as code

Platforms: Look Beyond FedRAMP

Technology powers modern government. But not all technology is equal. Leading organizations seek platforms that deliver value today and are positioned to deliver it far

into the future. They look beyond the FedRAMP authorization to how vendors operate, support their platforms, and enable extensibility. Don't settle for opaque release cycles or incomplete APIs. You must strategically organize your teams around platform management and embrace these seven key principles for platform success:

- **Intelligence and automation.** Every platform is growing more intelligent and automated, whether it's leaning on observability and AI for IT operations to understand the root of an incident or on genAI to assist developers. The cloud platforms are continually improving resource optimization, and the surrounding ecosystem is leveraging AI and automation to enhance the operator and developer experience, a critical force multiplier for a strained federal workforce.
- **Abstracted complexity.** As missions become more complex and the threat landscape intensifies, the underlying technology grows more complicated. Leading organizations don't try to remove this complexity; they seek to abstract it. They lean on technologies like PaaS (e.g., cloud.gov), multicloud container platforms (e.g., Platform One), and serverless development to shield developers from underlying infrastructure, allowing them to focus on mission code.
- **Composable experiences.** The future of government service delivery is composable, where services are built from modular, interchangeable, and reusable components. Organizations use multiple cloud platforms and a mix of native and marketplace services. The goal is to seamlessly integrate these components into a unified experience. Today, Kubernetes is a key enabler, but the long-term vision is a fully composable architecture built on APIs and microservices.
- **Platform teams.** Federal IT is reorganizing around major technology platforms rather than subject matter expertise. Advanced cloud practices have moved past a traditional cloud center of excellence to dedicated platform engineering teams. These teams build and maintain the internal tools, services, and automated pipelines that application teams use to deliver value securely and efficiently. In Forrester's Cloud Survey, 2025, 92% of public or private cloud decision-makers in US state or federal government said that their organization used centralized cloud platform teams paired with a cloud business office. For more information, see Charter A Corporate Cloud Platform Team and Navigating The New Terrain Of IT Platform Teams.
- **Diversified risk.** While standardizing on one cloud can seem simpler, a multicloud strategy is the federal standard for mitigating risk. This prevents vendor lock-in, enhances negotiating power, and provides resilience against provider outages. A sophisticated strategy involves being hyperaware of dependencies on any single service and its potential impact on the mission.

- **Workload affinity.** The ultimate vision is for applications to be designed without being tied to a specific location or platform, allowing them to move seamlessly between on-premises data centers, multiple clouds, and the tactical edge as mission requirements or costs change. Technologies like Kubernetes and WebAssembly (Wasm) are paving the way for this future, and leading organizations are embracing the platforms that will enable it. The vision is workload affinity, where an app is designed without being tied to a location or a specific platform and can move without significant rework required. Leading enterprises see this as the future and are embracing platforms that will likely enable it. New to Wasm? See Forrester's two-part video blog that digs into what it is and why it matters.
- **Modern cloud-native architectures.** The platforms you consume — and the systems you build — should have modern cloud-native architectures. As you modernize legacy systems, focus on rearchitecting them with service patterns that match mission needs. This ensures your systems can be continuously improved and adapted to evolving mission needs, moving beyond a lift-and-shift mindset.

Partners: Push Your Partners On Outcomes And Experience

Every organization relies on industry partners, but rigid compliance-focused contracts often strain these relationships. The modern approach pivots to helpful co-innovative partnerships focused on mission outcomes. Organizations expect more from their partners: dashboards to visualize results, automation to speed delivery, and flexibility in contract terms. There are eight key principles that leading organizations seek in their modern cloud partnerships:

- **Automation and analytics powered.** GSIs providing reusable templates is no longer enough. To win the business of leading organizations, service providers must find patterns in federal processes and automate repeatable work to create efficiency. Organizations should also expect powerful analytics to inform complex decisions, from cloud migration planning to FinOps.
- **Platform based.** Organizations want a digital experience to interact with their partners. The most prominent service providers are building their own platforms and capabilities — often custom built — to provide clients with transparent, modern support and to demonstrate the value of the partnership.
- **Advisory led.** Organizations rarely bring in a managed service provider late in the journey just to run operations. They want partners that have been with them from the start, helping navigate complex strategic questions around Cloud Smart, ZTA, and multicloud architecture. These partners must supplement their build/run capabilities with a strong professional services practice.

- **Responsive and flexible.** The old adversarial relationship between organizations and contractors doesn't work in a world of continuous change. Leading organizations expect their partners to be true advocates, acting with flexibility to meet evolving mission needs rather than rigidly adhering to the original text of a contract.
- **Transformative.** Today's environment demands continuous transformation, not discrete one-time modernization projects. Engagements with service providers must be structured to support this dynamic reality, enabling organizations to achieve and demonstrate value rapidly and continuously throughout their cloud journeys.
- **Cocreative.** Leading organizations identify partners that can cocreate solutions to drive the mission forward. This involves breaking down traditional top-down processes and working collaboratively with industry to jointly design and develop new services that are more responsive to the needs of customers and warfighters. To learn more about co-innovation partnerships, see Forrester's Get Started With Co-Innovation Partnerships.
- **Outcome and experience oriented.** The federal acquisition world is shifting from input-based contracts to outcome-based contracts. This model, which ties contractor payment to the achievement of measurable performance standards, incentivizes partners to focus on delivering mission value and creates accountability for results.
- **Enterprise focused.** The era of piecemeal technology procurement is ending, forcing a move beyond siloed one-off projects. Leading organizations are consolidating their purchasing power to shape massive enterprise-level agreements such as those under the US General Services Administration OneGov Vehicle designed for transformational impact. This strategy involves creating a competitive portfolio of vendors to maintain agility and negotiating for integrated value, including workforce training and security compliance, directly in the contract. The focus shifts from modernizing single systems to acquiring platforms that can transform entire mission portfolios.

Practices: Organize For Success In Platform Teams And Partner With Solution Architects

The cloud enables us to move at the speed of the mission, but organizations must equip their workforce and processes to handle that speed. This requires drastic changes to how we organize, work, and address security and compliance. There are seven key principles that leading organizations embrace in designing their cloud

operating model and practices:

- **Product-led teams.** Teams that are product led view software from end to end, from design to operation, with mission outcomes as their driving force. They are shifting from project-based thinking (where a team disbands after launch) to persistent teams that operate, maintain, and continuously refine a product or service.
- **Agile-plus-DevOps.** In the federal context, this is the practice of integrating development, security, and operations (DevSecOps) to deliver software faster and more securely. It acts as the lever that enables agile practices by lowering the cost and risk of software delivery through automation across the CI/CD pipeline, with the goal of achieving continuous authority to operate.
- **Site reliability engineering and platform engineering.** The traditional IT admin role is fading. Site reliability engineering has reshaped operations, requiring a product-oriented mindset and deep automation skills. SREs build and maintain the platforms that make developers successful. Organizations must build pathways to evolve their current IT workforce into these new roles. Getting to that state means that IT admins must evolve or retire, but the organizations they work for should build a path supporting that skill and mindset evolution. To learn more, see Forrester's How To Transition Your IT Admins To Become Site Reliability Engineers report.
- **FinOps-plus-IT financial management/technology business management.** As cloud budgets expand, organizations are building a FinOps practice to eliminate waste and maximize the value of every dollar spent. This is uniquely challenging in the federal government due to the multiyear planning, programming, budgeting, and execution process and the Anti-Deficiency Act. Federal FinOps focuses on forecasts, rigorous cost allocation through tagging, and optimization of spend through rightsizing and commitment-based discounts.
- **Zero Trust and app security.** Security is paramount. Building on a foundation of FedRAMP-authorized services, organizations focus their own efforts atop that foundation on a ZTA (i.e., redesigning perimeter-based security to secure from the data packet out) and application security (aka DevSecOps). To learn more, see Forrester's Getting Started With Zero Trust In The Cloud and Decoding Zero Trust reports.
- **Creative resilience.** Resilience underpins mission success and public trust. Cloud brings new risks, and developing resilience plans means adopting practices like chaos engineering and blameless postmortems. Resilience must become a core

value, addressed creatively through an empowering culture and exploratory practices. Developing cloud resilience plans means adopting practices like agile architecture, chaos engineering, blameless retrospectives, agile knowledge management, and more.

- **Policy as code.** As cloud environments grow, manual governance becomes untenable. With policy as code, security and compliance policies (for FedRAMP, the Defense Federal Acquisition Regulation Supplement, ZTA, etc.) are defined and enforced through machine-readable code. This automates compliance, embeds governance directly into the CI/CD pipeline, and dramatically reduces the risk of human error, enabling secure, agile governance at scale.

FORRESTER®

We help business and technology leaders use customer obsession to accelerate growth.

FORRESTER.COM

Obsessed With Customer Obsession

At Forrester, customer obsession is at the core of everything we do. We're on your side and by your side to help you become more customer obsessed.

Research

Accelerate your impact on the market with a proven path to growth.

- Customer and market dynamics
- Curated tools and frameworks
- Objective advice
- Hands-on guidance

Learn more.

Consulting

Implement modern strategies that align and empower teams.

- In-depth strategic projects
- Webinars, speeches, and workshops
- Custom content

Learn more.

Events

Develop fresh perspectives, draw inspiration from leaders, and network with peers.

- Thought leadership, frameworks, and models
- One-on-ones with peers and analysts
- In-person and virtual experiences

Learn more.

Contact Us

Contact Forrester at www.forrester.com/contactus. For information on hard-copy or electronic reprints, please contact your Account Team or reprints@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.

Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA 02140 USA
Tel: +1 617-613-6000 | Fax: +1 617-613-5000 | forrester.com