ATARC

ATARC cATO Working Group

FEBRUARY 2026

Clarifying Cloud Foundations

PaaS vs. IaaS for Federal Modernization

Acknowledgements

David Raley, USMC
Nicholas Rappold, National Weather Service
Gordon Deng, Orbital Labs
Henry Sienkiewicz, Georgetown University

Executive Summary

This paper provides a clear and practical guide for federal stakeholders to distinguish Infrastructure-as-a-Service (IaaS) from Platform-as-a-Service (PaaS), evaluate trade-offs, and implement the right model for secure, sustainable modernization. Understanding these models is essential to aligning technology decisions with mission outcomes, risk tolerance, and workforce realities.

Federal agencies are under increasing pressure to modernize aging IT environments, yet persistent confusion between IaaS and PaaS continues to slow progress. These service models fundamentally shape how organizations balance control, security, cost, agility, and mission delivery. Selecting the wrong model, or misunderstanding the distinction, can introduce unnecessary complexity, prolong Authorization to Operate (ATO) timelines, duplicate compliance efforts, and delay mission outcomes.

IaaS is best suited for teams that build and maintain platforms - organizations with the skilled staff, funding, and operational maturity required to manage infrastructure, security controls, and compliance activities directly. PaaS, by contrast, is designed for mission owners who use platforms to deliver capabilities. By abstracting infrastructure and embedding security and compliance into the platform itself, PaaS reduces operational burden, lowers dependency on highly specialized technical staff, and enables teams to scale and deliver faster while staying focused on mission outcomes.

Today, federal organizations spend nearly **80% of their IT budgets** maintaining legacy systems, leaving limited capacity for innovation. Understanding where responsibility shifts from infrastructure management (IaaS) to capability delivery (PaaS) is critical to improving modernization, return on investment and operational readiness. Ultimately, the choice between IaaS and PaaS determines whether agencies devote their time and resources to patching servers or to delivering mission software at speed.

1. Introduction: The Federal Cloud Challenge

Federal IT has long relied on monolithic legacy systems and acquisition models rooted in waterfall development. These approaches result in years-long modernization cycles, brittle architectures, and a heavy operational burden on system administrators.

In addition, the traditional Authorization to Operate (ATO) and Risk Management Framework (RMF) processes are often manual and documentation heavy. This further exacerbates the challenge and impedes cloud adoption. The consequences are clear:

- Delayed delivery of mission capabilities
- Increased vulnerabilities from outdated technology
- Rising operations and maintenance (O&M) costs
- Difficulty attracting and retaining modern technical talent

The next wave of federal modernization will not be won simply by moving workloads to the cloud. Progress depends on adopting the right cloud service model—one that balances speed, security, and compliance while reducing operational overhead. PaaS and IaaS each play a role, but they deliver fundamentally different outcomes.

2. Understanding Cloud Service Layers

The **Shared Responsibility Model** remains the foundation for federal cloud understanding. It defines how security, compliance, and operational responsibilities are divided between cloud providers and agencies based on the service model in use.

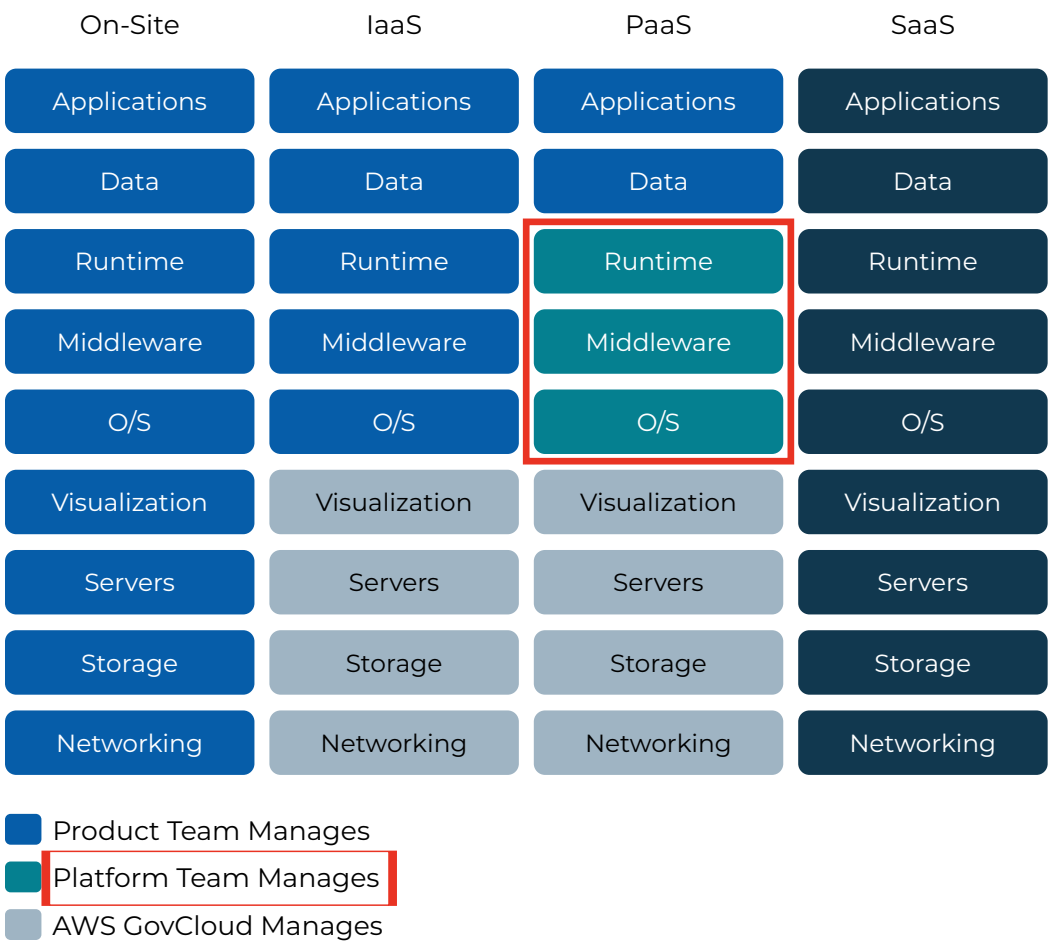
In **IaaS** environments, agencies manage much of the technology stack, from operating system patching and configuration to security controls and system monitoring. In **PaaS** environments, the provider manages everything beneath the application layer, enabling agencies to focus on software delivery rather than infrastructure operations.

IaaS provides projects with the **basic building blocks**, virtual servers, storage, and networking, but leaves **responsibility** for everything running on top of that infrastructure **with the agency**. This includes patching, configuring,

securing, and monitoring the systems that support applications. IaaS is useful when projects require full control, customization, or support for legacy applications, but it also demands more time, expertise, and resources spent managing technology rather than delivering mission capabilities.

PaaS provides a **fully managed, pre-secured environment** where teams can build and deploy applications without owning servers, infrastructure, or most compliance activities. The platform automatically handles security, scaling, patching, and operational tasks, allowing **mission owners to focus entirely on outcome delivery**. By shifting responsibility to the platform, PaaS accelerates modernization by letting teams focus on the mission, not the infrastructure behind it, while benefiting from provider support in planning, building, and compliance.

As agencies adopt higher-level cloud services, they gain greater opportunities to standardize environments, automate compliance, and accelerate mission delivery. This is why mature PaaS offerings often create transformative effects across federal environments.



3. Infrastructure-as-a-Service (IaaS)

Core Concept

IaaS provides virtualized compute, storage, and networking. Agencies control the operating system, middleware, configurations, and security hardening, and are responsible for maintaining and securing those components.

Typical Use Cases

- Hosting legacy workloads
- Highly customized architectures
- Applications requiring direct OS or kernel-level control

Examples

- Directly Provisioning AWS Services
- Provisioning Azure Virtual Machines

Ideal Fit

Agencies with strong systems engineering expertise and a desire to maintain deep control over infrastructure and compliance boundaries.

Benefits

- **High flexibility and more control**; agency managed compute resources
- **Supports legacy and custom architectures**
- **Elastic scaling capabilities**
- **Direct access to cloud provider services and support**
- **Can be cost-efficient when well optimized**

Risks

- **High management overhead** (patching, hardening, monitoring)
- **Requires significant in-house expertise**
- **More complex security responsibilities** across OS, network, and IAM
- **Cost creep** from under-managed resources
- **Potential to have longer security authorization processes** due to system-level authorization

IaaS aligns with traditional, control-heavy federal environments but often increases compliance friction and slows modernization.

4. Platform-as-a-Service (PaaS)

Core Concept

PaaS delivers an already managed environment for developing, deploying, and scaling applications without requiring agencies to manage underlying infrastructure. Modern PaaS offerings integrate security automation, DevSecOps, CI/CD pipelines, and built-in compliance inheritance, often at FedRAMP authorization Moderate or High. The platform has an existing ATO. The product team can then leverage the platform's ATO along with the cloud provider's FedRAMP authorization to pursue their accreditation.

Typical Use Cases

- Software factories
- Containerized workloads
- Continuous delivery environments
- Mission application development

Examples

- Operation StormBreaker
- Platform One - Party Bus
- Cloud Foundry
- Azure App Service

Ideal Fit

Agencies focused on delivering mission applications quickly and securely, without managing operating system patching, networking, or infrastructure scaling.

Benefits

- **Rapid deployment** with pre-configured environments
- **Significantly reduced operational burden**
- **Built-in high availability and resilience**
- **Consistent, standardized environments**
- **Often lower cost for steady workloads**

Risks

- **Reduced control** over underlying OS and configurations
- **Potential platform provided vendor-specific tool set lock in**
- **Autoscaling costs must be monitored**
- **Not suited for legacy applications** requiring custom OS or runtimes
- **Troubleshooting visibility may be limited**

When implemented as a true shared service, PaaS frees developers and mission teams to focus purely on delivering capabilities rather than maintaining infrastructure.

5. Why Confusion Persists

Despite years of cloud adoption, federal teams continue to struggle with distinguishing PaaS from IaaS due to:

- Overlapping and inconsistent terminology
- Cloud procurements written and evaluated like hardware contracts
- Cultural inertia within infrastructure-centric organizations
- RMF interpretations that prioritize documentation over automation
- Misalignment among IT, acquisition, cybersecurity, and mission owners

Shifting from control-oriented thinking to outcome-oriented modernization requires both cultural and procedural evolution across federal organizations.

6. Key Differences Between PaaS and IaaS

Dimension	IaaS	PaaS
Control	Agency manages OS, middleware, runtime, cloud account, and configurations	Platform provider manages everything below the application

Dimension	IaaS	PaaS
Speed	Months to years due to provisioning, configuration, and ATO	Minutes to hours through standardized, pre-authorized environments
Security & Compliance	Mission team managed, monitored and remediated	Platform team managed, monitored, and collaborative remediation with layers of inherited controls
Compliance Ownership	Mission team responsible for maintaining and updating controls	Platform team responsible for staying compliant as controls evolve
Cost Model	Infrastructure-driven O&M with variable optimization; increased fidelity and control	Value-based productivity; shared platform cost recovery
Best For	Infrastructure engineers and platform builders	Developers, mission owners, product teams
Workforce Impact	Requires larger, specialized technical staff; often higher reliance on contractors	Smaller teams; reduced need for highly specialized infrastructure expertise
Integration & Automation	Security automation limited to resources available to team mission owner; requires manual setup	Built-in automation, pipelines, and standardized guardrails

Bottom line

IaaS is ideal for organizations who prioritize architectural control, customizability, and have increased available resources. It offers maximum control, but demands ongoing investment in specialized expertise and operational resources.

PaaS is ideal for mission owners who prioritize capability delivery over infrastructure management; preferred for teams that prioritize speed to delivery. It provides a standardized, secure, and compliant environment that reduces operational burden and enables teams to focus on mission outcomes instead of infrastructure.

7. Case Study: Operation StormBreaker

Operation StormBreaker demonstrates what modern federal PaaS can achieve.

Problem

Legacy DoD systems experienced 12–18 month ATO timelines, heavily manual compliance processes, and slow deployment cycles.

Solution

StormBreaker implemented a PaaS model integrating DevSecOps pipelines, security automation, and RAISE certification. Compliance artifacts were generated and embedded directly into the platform rather than produced manually.

Impact

- Reduced deployment time from **18 months → 15 minutes**
- Enabled **ATO reciprocity** across multiple mission systems
- Reduced compliance workload by **~70%**
- Enabled repeatable infrastructure and application patterns
- Shifted teams from infrastructure maintenance to product delivery

Lesson

Modern **PaaS succeeds** when **compliance becomes codified**, not simply documented. **Automation unlocks both speed and rigor.**

8. Implications for Federal Stakeholders

Federal modernization requires adopting a shared-services mindset:

For CIOs

- Adopt a portfolio approach to determine which workloads belong in IaaS versus PaaS.
- Prioritize scalable platforms over one-off system deployments.

For CISOs

- Shift from static, artifact-based RMF to continuous, evidence-based security.
- Leverage inherited controls and reusable compliance packages.

For Acquisition Leaders

- Move toward outcome-based, sprint-based contracting aligned with PaaS delivery velocity.
- Avoid system-specific infrastructure procurements where a platform exists.

For Developers & Mission Owners

- Embrace platform standardization, automation, and shared controls.
- Focus time on capability delivery rather than reinventing platform components.

Agencies that lack deep technical capacity often benefit more from mature PaaS offerings, while those with strong engineering infrastructure may choose to maintain selective IaaS environments.

9. Recommendations

1. **Define mission-aligned criteria** for when PaaS or IaaS should be used across agency portfolios.
2. **Invest in reusable PaaS capabilities** that provide baked-in security, compliance, and automation.
3. **Adopt continuous authorization** models supported by real-time evidence and integrated DevSecOps tooling.

4. **Reduce redundant ATOs** by prioritizing inheritance and reciprocity through shared platforms.
5. **Accelerate contracting cycles** to match PaaS delivery cadence.
6. **Shift culture toward product teams** focused on continuous delivery and mission outcomes.
7. **Determine resources available, trade-offs, and acceptable risk** profile to your mission objectives.

10. Conclusion

Federal digital modernization depends not just on cloud adoption but on choosing the right platform model. IaaS empowers infrastructure innovators; PaaS empowers mission owners.

Understanding this distinction allows agencies to:

- Reduce unnecessary O&M costs
- Improve security through automation
- Speed delivery of mission capabilities
- Create sustainable modernization pathways

The call to action is clear:
Invest in platforms that unify security, compliance, and delivery. When these move together, modernization follows.