PROJECT HOSTS™
Security Compliant Clouds

WHITEPAPER

Building a FedRAMP Business Case

Raymond de Avila, Project Hosts, Growth & Strategy
Josh Krueger, CISO

Contents

Between a Rock and a Hard Place

Independent Software Vendors (ISVs) with cloud-based applications who want to serve the Federal Government often find themselves “between a rock and a hard place.”

The barrier to entry is real. Navigating the cybersecurity requirements to compete for opportunities can be daunting. In addition to meeting the rigor of the compliance standards, organizations must have a solid business case to justify the human capital and financial investment required to earn the right to compete and win federal business.

The Federal Imperative

The cybersecurity threat landscape is expanding at an unprecedented pace, driven by constantly evolving attack surfaces, advanced AI-powered exploits, and increasingly sophisticated adversaries.

As vulnerabilities multiply and regulatory frameworks adapt, compliance has become a strategic imperative. Organizations that proactively strengthen their security posture and meet evolving standards are better positioned to protect sensitive data, maintain trust, and stay ahead of emerging mandates, making compliance a continually growing and mission-critical discipline.

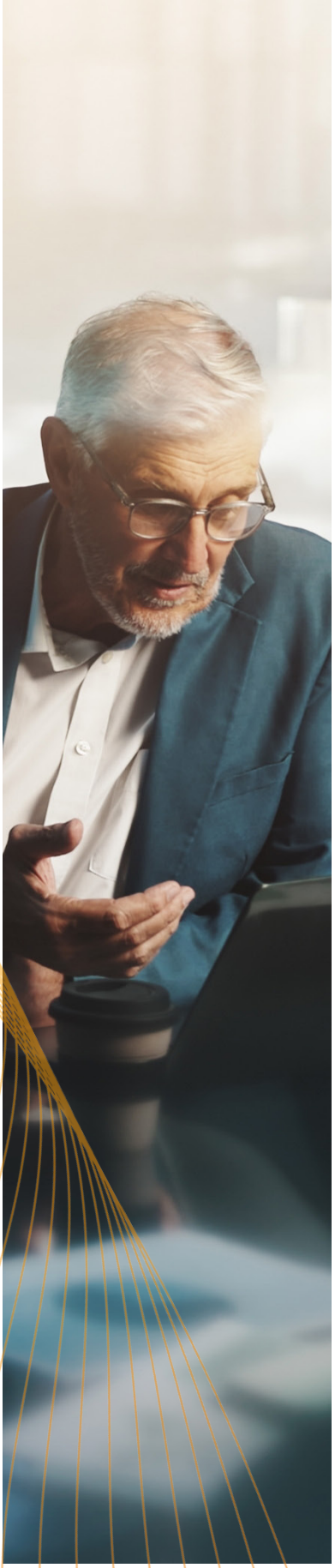
The U.S. government places a high priority on cloud security for ISVs who seek to serve federal agencies and the Department of Defense (DoD). Through a series of policies, mandates, and frameworks, the government has made clear that secure cloud adoption is essential to national security, operational readiness, and public trust.

58%

of breaches impacting the top 100 U.S. federal contractors are caused by third-party attack vectors.[1]

72%

of data breaches in 2025 involved data stored in the cloud.[2]



"If you were to do this on your own, you have to take on the costs associated with building your own compliant environment. And not only that, but we're reducing the stress of complying with cybersecurity regulations that, in many cases, fall outside of our client's core competencies."

- DAN RUSERT, VP OF BUSINESS DEVELOPMENT AT JAMIS

To deliver cloud services to federal agencies, ISVs must demonstrate a strong cybersecurity posture through programs such as:

Federal Risk & Authorization Management Program (FedRAMP)
Mandatory for any cloud service used by civilian federal agencies. ISVs must undergo rigorous third-party assessments against NIST SP 800-53 controls.

DoD Cloud Computing Security Requirements Guide (SRG)
Requires compliance with Impact Levels (IL2 - IL6) depending on data sensitivity.

Cybersecurity Maturity Model Certification (CMMC)
Required for defense contractors and ISVs handling Controlled Unclassified Information (CUI).

Determining the required level of compliance can be confusing. Simultaneously, it's essential to understand exactly which program applies and the compliance level required to select an efficient, cost-effective path forward.

As threats escalate and regulatory frameworks tighten, the burden naturally shifts to technology providers — particularly ISVs whose solutions provide the innovation to address mission requirements. Meeting federal expectations for cloud security is no longer optional; it demands deliberate investment in compliant infrastructure, continuous monitoring, and rigorous authorization processes such as FedRAMP and DoD Impact Level certifications.

For ISVs, this means allocating resources to innovation and delivering robust security to earn and maintain government trust.

Key Takeaways for Federal Agencies and ISVs

METRIC		WHAT IT MEANS
$4.75 MILLION	Cloud misconfiguration breaches cost $4.75M on average.[3]	Compliance gaps and poor security can have major financial consequences.
80%	80% of organizations have had a cloud security incident in the past year.[4]	Cloud threats are now **common,** not theoretical.
80%	80% of exposures are caused by identity and credential misconfigurations.[5]	Most issues are **preventable** with strong controls and visibility.
60%	Nearly 60% of federal contractor breaches are tied to vendors.[6]	**ISVs are a growing attack vector** and must be held to higher standards.

Cloud Security Is Non-Negotiable for ISVs

ISVs seeking federal opportunities are often required to demonstrate a significant level of compliance just to compete. Historically, the cost, rigor, and time needed to achieve that compliance have placed a heavy burden on these vendors — creating a classic "chicken-and-egg" dilemma: they must invest heavily to qualify, yet have no assurance of winning the business that would justify the investment.

Deciding to pursue the required cloud-security certifications involves two key steps. First, determine whether a strong business case justifies the investment. If so, the next step is to identify how to achieve compliance in the most efficient, reliable, and cost-effective way.

When developing that business case, several critical factors merit careful evaluation.

Building the Business Case

Key areas to explore when evaluating the opportunity include:

Market Assessment & Justification
Map out the total addressable market, conduct a competitive analysis, and create a clear go-to-market plan.

Solution Fit
Gain confidence that your offering meets agency mission objectives and differentiates from competitors, supported by stakeholder feedback.

Pipeline Visibility
Create a list of existing or potential opportunities, current federal relationships, and a concrete plan to develop new ones.

Agency Sponsorship
Build a focused list of agency prospects who may be able to sponsor your SaaS solution, and use early conversations to uncover their mission needs, procurement timelines, and interest in supporting your path to authorization.

Executive Commitment
Gain leadership alignment on costs, timing, and organizational impact.

Scope & Resources
Establish a realistic understanding of time, cost, expertise, and internal capacity to reach authorization.

From Business Case to Execution

Once you've validated the business case, the focus shifts to selecting a compliance strategy that aligns with your organization's culture, timeline, and budget. Leaders at Microsoft and AWS note that ISVs often encounter high costs, extended timelines, resource strain, and rigid, one-size-fits-all solutions — making the choice of program critical. Multiple pathways can lead to authorization, and the best route depends on where you are in your compliance journey.

Determining the Required Compliance Level

To achieve an Authority to Operate (ATO), organizations must determine the right level of compliance for their solution and chart a clear path to full authorization. Some choose to pursue FedRAMP compliance, others opt for FedRAMP equivalency, and some work directly toward an agency-sponsored ATO. ISVs don't need to do everything at once — many take a phased approach that lets them start the process, demonstrate progress, and build momentum while steadily moving toward full compliance.

Understanding FedRAMP Pathways

Before exploring which agency determines requirements, it's helpful to understand the terminology often used in the marketplace:

FedRAMP Compliance
A designation for cloud services that have implemented the baseline FedRAMP security controls (NIST SP 800-53) but have not been formally authorized by a federal agency. Providers may complete readiness or internal assessments, but no ATO is issued.

FedRAMP Equivalency
A designation the DoD uses for cloud services that meet FedRAMP baseline security requirements through an alternate assessment process. This status is valid for DoD use but is not automatically recognized by civilian agencies.

FedRAMP Authorization
A designation granted when a cloud service offering achieves a formal, agency-sponsored ATO under FedRAMP. Authorization requires third-party assessment and PMO validation and enables reciprocity and listing on the FedRAMP Marketplace.

The next step is understanding how different government bodies — from civilian agencies to the Department of Defense — determine the required compliance level for a given application.

Federal Agencies

For any cloud-based application the U.S. government or DoD plans to use, the sponsoring agency — through its Authorizing Official (AO) or designated representative — sets the required compliance level. This decision covers both the applicable framework and the security impact level. The AO's evaluation considers factors such as data sensitivity, mission criticality, and the potential impact of a breach. To guide this determination, agencies reference standards like FIPS 199, which classifies systems as Low, Moderate, or High based on confidentiality, integrity, and availability requirements.

Civilian Agencies

For civilian agencies, the sponsoring agency's AO — working with the FedRAMP Program Management Office (PMO) — determines whether the application needs FedRAMP Low, Moderate, or High authorization.

DoD Agencies

For DoD use, the Authorizing Official within the DoD component (often coordinated through DISA, the Defense Information Systems Agency) specifies the Impact Level based on the DoD Cloud Computing SRG.

While vendors can propose a target level and prepare their environment, the agency's AO is the final authority. The government agency or DoD component that will use the system determines the required compliance level, not the cloud provider or the software vendor.

80% of exposures are caused by identity and credential misconfigurations.[5]

Charting the Right Path Forward

Determining the right path for your organization begins with a clear understanding of your business case and an honest assessment of where you are in the compliance journey. This can be broken down into three phases:

Exploring
When agency interest is emerging and you're weighing entry into the public sector, the focus should be on building a strong compliance narrative, establishing a presence in the FedRAMP Marketplace, and seeking expert guidance. At this stage, cost-efficient solutions that allow you to take the first step without overcommitting are key.

Pursuing
Once you've committed to serving the public sector, the goal is to advance steadily toward FedRAMP or DoD authorization. A phased strategy can help generate agency interest, build a qualified pipeline, and adapt as requirements evolve, allowing you to scale at your own pace while positioning for long-term success.

Charging
When compliance is non-negotiable and agency sponsorship is within reach, it's time to fully engage. With a mature business case and strong organizational commitment, partnering with a team experienced in FedRAMP and DoD certifications ensures efficiency and confidence. Whether extending on-premises solutions to the cloud or leveraging prior authorizations, careful evaluation of key criteria will smooth the path to authorization.

Determining Required Capabilities

Meeting federal compliance goals requires a clear understanding of the capabilities your organization must have in place. These capabilities serve as decision criteria to evaluate the different paths available and to ensure your investment in compliance delivers long-term value.

Business Considerations

Strong business alignment drives sustainable compliance success.

KEY CAPABILITIES	DESCRIPTION
STAKEHOLDER ALIGNMENT	Secure executive sponsorship and cross-functional engagement across IT, Security, Legal, Finance, and Operations. Everyone must move in the same direction.
BUSINESS CASE & ROI	Define the market opportunity, revenue potential, and cost offsets to justify both initial and ongoing investment.
PRICING STRATEGY	Adopt a transparent model to ensure authorization and continuous monitoring costs remain predictable.
TIMELINE & MILESTONES	Build a realistic schedule with clear checkpoints for assessment, remediation, and authorization — including contingencies for delays.
INTERNAL RESOURCES & EXPERTISE	Identify skill gaps early. Use a clear RACI model to define roles between internal teams and external compliance partners.
FEDRAMP MARKETPLACE STRATEGY	Develop a plan to achieve your own FedRAMP Marketplace listing so agencies can easily find and procure your solution.

Technical Considerations

Your architecture must enable—not constrain—compliance.

KEY CAPABILITIES	DESCRIPTION
HOSTING & ARCHITECTURE DECISIONS	Select the optimal cloud service provider(s) and environment (e.g., AWS GovCloud, Azure Government). Determine whether to deploy in a dedicated or multi-tenant boundary.
APPLICATION READINESS	Assess application design changes required for FedRAMP or DoD compliance (encryption, logging, IAM). Maintain flexibility to integrate third-party tools and avoid lock-in.
CONTINUOUS MONITORING & INCIDENT RESPONS	Establish processes for vulnerability management, event reporting, and incident response per FedRAMP requirements—allowing teams to stay focused on mission priorities.
SCALABILITY & PERFORMANCE	Build for growth. Ensure your compliant architecture can handle expanding workloads and agency demand without compromising compliance posture.

Compliance Considerations

Compliance is not a milestone—it's an operating discipline.

KEY CAPABILITIES	DESCRIPTION
REQUIRED AUTHORIZATION LEVEL	Identify the applicable baseline (FedRAMP Low/Moderate/High, DoD IL4/IL5/IL6) based on data sensitivity and Authorizing Official requirements.
COMPLIANCE BOUNDARY OWNERSHIP	Decide between a dedicated or shared boundary—each has trade-offs in control inheritance, cost, and autonomy.
AUDIT & DOCUMENTATION READINESS	Engage a provider who can manage documentation heavy-lifting, including the SSP, policies, and evidence collection for 3PAO assessments.
CONTINUOUS AUTHORIZATION	Plan for annual audits, continuous monitoring, and ongoing reporting to maintain your "Authorized" status.

Shared Boundary Risks

Organizations often underestimate the long-term impact of shared environments.

Control Exposure
Incidents in shared environments could jeopardize your authorization.

Loss of Autonomy
Provider policy or architecture changes may require disruptive adjustments.

Limited Flexibility
Restrictions may prevent infrastructure changes or adoption of new technologies.

Summary Insight

When evaluating your compliance approach, think beyond authorization. Your chosen capabilities should enable predictable costs and timelines, align business, technical, and compliance goals, and create a foundation for continuous growth in the public sector.

50%

Over 50% of audited federal cloud systems had insufficient continuous monitoring or outdated ATO documentation — GAO Report on Cloud Security in Federal Agencies (2023)[7]

Final Thoughts

By weighing business, technical, and compliance factors from the start, you can build a realistic roadmap that enables accurate budgeting, efficient resource allocation, and a FedRAMP strategy aligned with your organization's goals and risk tolerance.

Just as important is doing your due diligence: engage with current federal customers, verify references, and scrutinize pricing to ensure you're making true "apples-to-apples" comparisons.

Choose a compliance program that aligns with your business case — one that matches your team's responsibilities, budget, timeline, and culture. An approach tailored to your unique requirements will help you achieve compliance faster, control costs, and meet the federal government's demanding security standards.

Next Steps

Review these insights with your leadership team to assess your current stage in the compliance journey and define clear next steps. When you're ready to move forward, connect with Project Hosts — your trusted advisor in accelerating your path to ATO. From early strategy to full compliance, our proven programs, experienced team, and cloud compliance platform simplify the journey, reduce risk, and deliver results with the assurance of success.

Ready to simplify your compliance journey?

Connect with Project Hosts to learn how we support FedRAMP, DoD IL4 and IL5, and beyond.

(814) 325-9131 info@projecthosts.com

Sources
https://securityscorecard.com/research/defending-the-federal-supply-chain-a-cyber-security-assessment-of-the-top-100-u-s-government-contractors/
https://www.ibm.com/reports/data-breach
https://www.ibm.com/reports/data-breach
https://www.techmagic.co/blog/cloud-security-statistics
https://www.securitymagazine.com/articles/100630-misconfigurations-drive-80-of-security-exposures
https://securityscorecard.com/research/defending-the-federal-supply-chain-a-cyber-security-assessment-of-the-top-100-u-s-government-contractors/
https://www.gao.gov/products/gao-23-105482