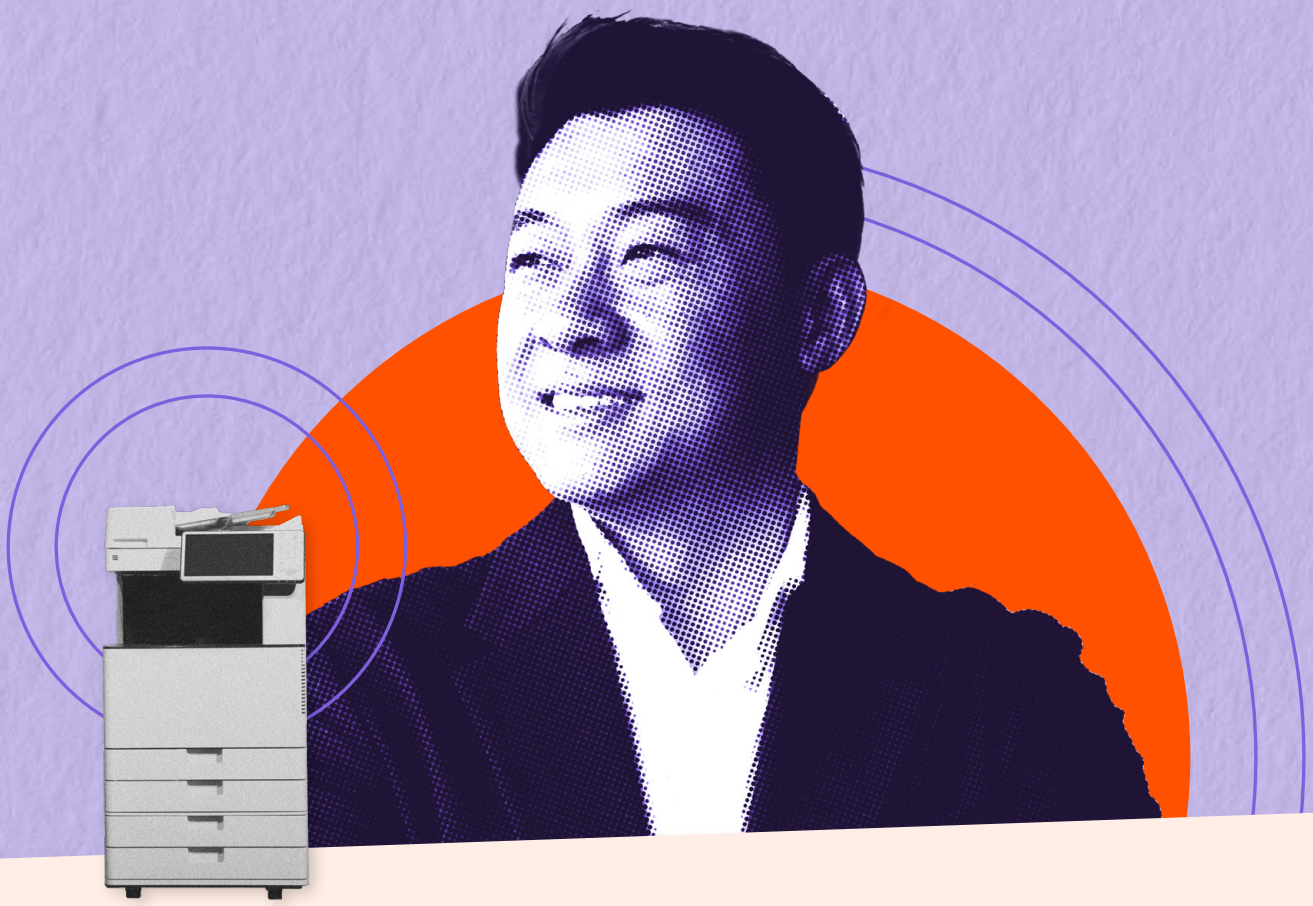
PrinterLogic®

FedRAMP™



# FEDRAMP® HIGH AUTHORIZATION

What It Means for Government and Regulated-Industry CIO and CTOs

# TABLE OF CONTENTS

## EXECUTIVE SUMMARY

In January 2026, Vasion achieved FedRAMP® High Authorization—the cloud-native intelligent print automation platform built for the demands of U.S. federal agencies and the strictest regulatory environments in the private sector. This authorization was earned through assessment against 421 security controls by an accredited Third Party Assessment Organization (3PAO), covering the highest impact level in the FedRAMP framework.

For federal agencies, FedRAMP High Authorization is the clearest possible signal: Vasion platform has been independently validated to protect Controlled Unclassified Information (CUI), law enforcement data, Protected Health Information (PHI), and mission-critical national security systems.

Similarly, for highly regulated commercial industries—healthcare, financial services, defense contracting, and critical infrastructure—FedRAMP High represents a security and compliance posture most enterprise vendors cannot match.

This whitepaper explains what FedRAMP High Authorization means, why it matters, and how Vasion authorization specifically addresses the security, modernization mandates, procurement, and compliance challenges that could be holding your agency back.

| 421 | 109 | 0 | 3+ |
|---|---|---|---|
| Security controls assessed at FedRAMP® High | Existing government customer ATOs | Print-related customer breaches | Months security review time saved for agency ISSOs |

SECTION 1

# UNDERSTANDING FEDRAMP®; THE GOLD STANDARD FOR CLOUD SECURITY

## WHAT FEDRAMP ACTUALLY IS

The Federal Risk and Authorization Management Program (FedRAMP®) is a U.S. government-wide framework that standardizes security assessment, authorization, and continuous monitoring for cloud products and services used by federal agencies. Established under the Federal Information Security Modernization Act (FISMA) and codified in OMB memo M-11-11, FedRAMP operationalizes NIST 800-53 rev.5, the authoritative security and privacy controls catalog for federal information systems, into a repeatable, auditable, and reusable authorization process.

FedRAMP has three impact levels, each tied to the severity of harm that could result from a security incident:

| Impact Level | Data Types Covered | Security Controls Required |
|---|---|---|
| Low | Public, non-sensitive information | 125 controls |
| Moderate | CUI, general agency operations | 325 controls |
| High | National security, PHI, law enforcement, CUI | 421 controls |

FedRAMP® High is not simply “more controls”: it’s a fundamentally different tier of security assurance. It applies to systems where a breach could result in loss of life, compromise of national security, or catastrophic harm to mission-critical operations. The assessment process involves a 3PAO-conducted security test of the vendor’s entire cloud environment, reviewed by the FedRAMP® Program Management Office (PMO), and ongoing continuous monitoring with monthly vulnerability scans and annual assessments.

## THE AUTHORIZATION HIERARCHY: FEDRAMP AUTHORIZED VS. IN PROCESS

The FedRAMP® Marketplace lists vendors at various stages. Here’s the breakdown of each phase:

- **FedRAMP Authorized:** The vendor has completed the full assessment, received a government Authority to Operate (ATO), and is listed on the FedRAMP® Marketplace. This is the only status that legally satisfies FISMA and agency ATO requirements.
- **FedRAMP In Process:** The vendor is undergoing assessment but has not yet received authorization. Agencies may not reuse an in-process vendor’s security package.
- **FedRAMP Ready:** The vendor has passed a Readiness Assessment but has not undergone the full authorization process. Not a substitute for Authorized status.

### ALREADY AUTHORIZED

Vasion (Vasion Automate Fed) carries full FedRAMP® High Authorization—not In Process, not Ready. Our authorization package is available on the FedRAMP Marketplace and can be used by any federal agency to issue their own ATO, dramatically shortening the procurement timeline.

### WHY HIGH AUTHORIZATION IS INCREASINGLY THE FEDERAL STANDARD

Historically, FedRAMP Moderate was the de facto standard for most federal cloud deployments. That is changing rapidly. Three converging forces are driving agencies toward High:

- **Executive Order 14028 (Improving the Nation's Cybersecurity, 2021):** Requires agencies to adopt Zero Trust Architecture (ZTA) and prioritize cloud solutions with demonstrably stronger security postures. FedRAMP® High Authorization directly supports ZTA adoption.
- **OMB Memo M-22-09 (Zero Trust Strategy, 2022):** Mandates that agencies meet specific Zero Trust milestones. Agencies using FedRAMP® High-authorized solutions are better positioned to satisfy these milestones without additional security engineering.
- **Expanding CUI and PHI workloads in the cloud:** As agencies move sensitive data (e.g., health records, law enforcement files, intelligence-adjacent information,) to cloud environments, Moderate authorization is frequently insufficient. High becomes mandatory.

SECTION 2

## WHAT VASION FEDRAMP® HIGH AUTHORIZATION MEANS

### THE ATO REUSE ADVANTAGE

For federal agency information security officers (ISSOs) and the CIO/CTOs who direct them, the most immediate and tangible benefit of Vasion's FedRAMP High Authorization is ATO reuse. Rather than conducting an independent security assessment of Vasion platform—a process that typically consumes 6 to 12 months of security engineering time and significant budget—agencies can reuse Vasion's existing authorization package.

This isn't a shortcut. It's the intended design of FedRAMP. The program was created specifically to allow the federal government to "authorize once, use many", meaning one rigorous assessment benefits every agency that subsequently adopts the same cloud service. Vasion 3PAO-validated security package covers 421 controls.

Your ISSO reviews our package, conducts a lighter-weight agency-specific assessment for any controls not inherited, and issues an ATO. Internal review timelines shrink by three months on average.

> "Working with Vasion on this large-scale deployment gave us confidence that the platform could meet the security and operational demands of a major military command. The scale and reliability has been exceptional."
>
> **— Tony Jimenez, CEO, MicroTech — supporting the largest Vasion Automate Fed deployment in the U.S. Army (NETCOM)**

## MANDATORY COMPLIANCE COVERAGE IN A SINGLE AUTHORIZATION

Vasion Automate Fed's FedRAMP High Authorization satisfies or directly supports compliance with the following mandates in a single vendor relationship:

- **FISMA:** Federal agencies are required by law to protect federal information and information systems. FedRAMP authorization is the recognized mechanism for cloud services to satisfy FISMA requirements.
- **NIST 800-53 rev.5:** 421 assessed controls are mapped to the current revision of NIST's security and privacy controls standard—the foundational framework for all federal information systems.
- **FAR and DFARS:** The Federal Acquisition Regulation and Defense Federal Acquisition Regulation Supplement require contractors handling CUI to meet specific security standards. FedRAMP High authorization satisfies these procurement requirements.
- **CMMC (Cybersecurity Maturity Model Certification):** Defense contractors must demonstrate cybersecurity maturity to bid on and hold DoD contracts. FedRAMP® High posture maps strongly to CMMC Level 2 and Level 3 requirements.
- **Zero Trust Architecture (M-22-09):** Vasion supports ZTA principles including identity-based access, least-privilege, micro-segmentation of print workloads, and continuous verification—directly aligned with the DoD Zero Trust Strategy's 2027 target deadline.
- **FIPS 140-2/140-3:** All data in transit and at rest in Vasion Automate Fed uses FIPS-validated encryption modules, satisfying the Federal Information Processing Standards required for federal deployments.
- **Cloud Smart Strategy (OMB):** The federal cloud modernization strategy prioritizes security, savings, and speed. The Vasion cloud-native architecture—with no on-premises servers required—directly supports Cloud Smart objectives.

## CONTINUOUS MONITORING REDUCES THE BURDEN

Unlike point-in-time security reviews, FedRAMP requires continuous monitoring: monthly vulnerability scans, real-time security event reporting to the FedRAMP PMO, and annual 3PAO-conducted assessments. The Vasion authorization includes an active continuous monitoring program. Agencies inherit this evidence stream—reducing the ongoing security management burden on agency security teams.

## PRINT AND OUTPUT MANAGEMENT: THE OVERLOOKED ATTACK SURFACE

Print infrastructure is one of the most neglected security domains in federal agencies. A 2025 Quocirca study found that 83% of organizations expect their spend on security to increase in 2026 as they look to protect against print-related breaches and about 56% of organizations experienced a print-related data breach in the prior year. In the federal context, unsecured print environments create specific risks:

- Documents printed to shared printers and left uncollected could expose CUI to unauthorized personnel.
- Legacy on-premises print servers running outdated operating systems create persistent, unpatched vulnerability points on agency networks.
- Print job data transmitted over unsecured protocols can be intercepted (particularly relevant in multi-tenant government facilities.)
- Physical print audit trails are often nonexistent, making investigation of data loss events nearly impossible.

### TOP 3 PRINT SECURITY CHALLENGES

**1 28%**
Securing print in a remote/home environment

**2 28%**
Protecting sensitive or confidential documents from being printed

**3 25%**
Understanding the types of threats and vulnerabilities of print infrastructure

### PRINT SECURITY SPEND IS INCREASING

**83%**
of organizations expect their print security spend to increase in the coming 12 months

*Quocirca Print Security Landscape 2025 Study

## VASION ADDRESSES ALL OF THESE RISK VECTORS WITHIN ITS FEDRAMP HIGH-AUTHORIZED ENVIRONMENT:

- **Secure Release Printing:** Print jobs are held in the cloud and released only when the authorized user authenticates at the device using CAC/PIV card, PIN, or mobile app. Documents never sit unattended in output trays.
- **Serverless Architecture:** Vasion Automate Fed eliminates on-premises print servers entirely. Without a print server, there's no local server to patch, compromise, or use as a lateral movement vector.
- **Full Audit Trail:** Every print event is logged with user identity, device, document metadata, and timestamp—providing the evidentiary trail required for FISMA audits and insider threat investigations.
- **Encryption End to End:** All print data is encrypted in transit (TLS 1.2+) and at rest (AES-256) using FIPS 140-2-validated modules.

## PROCUREMENT ADVANTAGES

Beyond security, Vasion FedRAMP High Authorization creates measurable procurement advantages:

- **GSA Schedule Availability:** Vasion is available via GSA Schedule contract vehicles, allowing agencies to leverage existing contract mechanisms without a full open competition. This is particularly valuable for budget spending timeline pressures.

*Quocirca Print Security Landscape 2025 study: https://quocirca.com/quocirca-print-security-landscape-2025/

- **FedRAMP Marketplace Listing:** Vasion is officially listed on the FedRAMP® Marketplace. Contracting officers can confirm authorization status instantly, reducing procurement risk and satisfying acquisition review requirements.
- **FAR Part 12 Compliance:** As a commercial item with FedRAMP authorization, Vasion Automate Fed can be procured under simplified acquisition procedures where applicable.
- **Rapid Deployment:** Cloud-native serverless architecture means agencies can deploy Vasion Automate Fed in weeks not the 12-to-36-month acquisition and implementation cycles typical of legacy print management systems.

SECTION 3

# FEDRAMP® HIGH AS A TRUST SIGNAL FOR REGULATED INDUSTRIES

## WHY COMMERCIAL ORGANIZATIONS SHOULD CARE ABOUT A FEDERAL PROGRAM

FedRAMP was designed for federal agencies, but its benefits extend well beyond government walls. For technology leaders in healthcare, financial services, defense contracting, insurance, energy, and other highly regulated industries, FedRAMP High Authorization has become one of the most credible, independently verified security signals available in the enterprise software market.

The reason is straightforward: FedRAMP's 421-control assessment is more rigorous than the security questionnaire-based due diligence most commercial organizations conduct on their vendors. When a vendor carries FedRAMP High Authorization, you have third-party evidence, not a self-attestation, that their cloud environment meets the security standards the U.S. federal government trusts for its most sensitive data.

## REGULATORY ALIGNMENT FOR HIGHLY REGULATED INDUSTRIES

FedRAMP High Authorization provides direct alignment to regulatory frameworks:

| Industry Regulation | FedRAMP® High Alignment | Relevant Vasion Controls |
|---|---|---|
| **HIPAA / HITECH** | NIST 800-53 rev.5 maps directly to HIPAA Security Rule safeguards and PHI workloads require High-equivalent controls | Encryption, access control, audit logging, incident response |
| **PCI-DSS v4.0** | FedRAMP High encryption, access control, and monitoring controls satisfy or exceed PCI-DSS requirements in overlapping domains | FIPS encryption, multi-factor authentication, continuous monitoring |
| **SOX (IT Controls)** | Audit logging, change management, and access control requirements under SOX IT General Controls map to FedRAMP access and audit control families | Full print audit trail, role-based access, change management |

| Industry Regulation | FedRAMP® High Alignment | Relevant Vasion Controls |
|---|---|---|
| **CMMC Level 2/3** | Defense contractors must meet NIST 800-171 and 800-172 requirements, FedRAMP High's 421 controls encompass and exceed these frameworks | All NIST 800-53 control families at High baseline |
| **NYDFS Cybersecurity Regulation** | New York's financial services cybersecurity rule requires encryption, access controls, and audit trails—all present in the Vasion FedRAMP High authorization | Encryption, MFA, incident response, audit logging |
| **NERC CIP (Energy)** | Critical infrastructure protection standards for the energy sector align with FedRAMP High's access control and incident response requirements | Secure access, monitoring, physical/ logical separation |

## THE VENDOR RISK MANAGEMENT ARGUMENT

Enterprise vendor risk management programs typically require security questionnaires, SOC 2 Type 2 reports, and periodic security assessments. FedRAMP High Authorization significantly streamlines this process:

- **Pre-assessed:** Vasion security posture has been assessed by an independent 3PAO against 421 controls. You don't need to conduct your own technical security assessment. You can rely on the federal government's assessment, backed by continuous monitoring evidence.
- **Evidence-based:** Rather than vendor-completed questionnaires, FedRAMP provides audit-ready evidence packages. Your vendor risk and compliance team can review authorization documentation directly.
- **Continuously monitored:** Security is not static. FedRAMP requires ongoing vulnerability management, monthly reporting, and annual reassessment. Vasion authorization reflects a future-ready security posture, not just a point-in-time snapshot from a past audit.

## FOR BOARD-LEVEL RISK CONVERSATIONS

FedRAMP High Authorization provides a defensible, third-party-validated basis for technology procurement decisions. When a breach occurs in your industry and boards ask *"what due diligence did we conduct on our vendors?"* FedRAMP High Authorization is one of the strongest answers available.

## HEALTHCARE: PHI, HIPAA, AND THE PRINT RISK YOU MAY NOT HAVE PRICED

Healthcare organizations handle Protected Health Information (PHI) across some of the most distributed, heterogeneous IT environments in any industry. Print infrastructure in clinical settings (lab results, discharge summaries, prescriptions, imaging reports) creates persistent PHI exposure risk that most healthcare teams have not fully quantified.

HIPAA's Security Rule requires covered entities to implement technical safeguards protecting electronic PHI. Print output is frequently outside the scope of formal HIPAA technical safeguard programs, yet clinical printers handle PHI constantly. Vasion provides:

- **Secure Release Printing** ensures PHI print jobs are released only to the authenticated clinician and never left in output trays accessible to unauthorized personnel.
- **Full audit logging** of every print event provides the evidentiary trail required for HIPAA breach investigations and OCR audits.
- **Serverless architecture** eliminates on-premises print servers as a PHI breach vector.
- **Encryption end-to-end** satisfies HIPAA's encryption addressable implementation specification at a standard exceeding most healthcare IT environments.

### FINANCIAL SERVICES: REGULATORY SCRUTINY AND OPERATIONAL RESILIENCE

Financial services leaders face an increasingly aggressive regulatory environment: NYDFS cybersecurity regulations, SEC cybersecurity disclosure rules, DORA in European operations, and heightened OCC examination standards. Document output in financial services—account statements, loan documents, compliance filings, trading confirmations—carries significant regulatory and reputational risk if compromised.

Vasion FedRAMP® High Authorization provides financial services organizations with a vendor whose cloud security posture has been independently validated, meeting most financial regulators requirements. The continuous monitoring requirement ensures that security doesn't degrade between your annual vendor reviews—a critical consideration in an environment where threat actors actively target financial infrastructure.

SECTION 4

## THE FULL VASION SECURITY POSTURE

### AUTHORIZATION AND CERTIFICATIONS

Vasion FedRAMP High Authorization is Vasion most comprehensive security credential, but it exists within a broader security posture:

- **FedRAMP® High Authorized (January 2026):** 421 security controls assessed by an accredited 3PAO. The highest impact level in the FedRAMP framework.
- **SOC 2 Type 2:** Annual independent assessment of Vasion security, availability, processing integrity, confidentiality, and privacy controls. Type 2 covers a minimum 12-month observation period, not a point-in-time snapshot.
- **ISO 27001:2022:** International standard for information security management systems (ISMS). This certification covers the current 2022 revision with updated controls for cloud environments and supply chain security.
- **ISO 42001 (AI Management):** As Vasion incorporates AI-powered capabilities into its automation platform, ISO 42001 certification demonstrates responsible AI management—increasingly relevant as regulators examine AI governance in enterprise software.

- **DoD IL4 (In Process):** Impact Level 4 authorization for Department of Defense workloads handling CUI. Vasion is currently pursuing IL4, which will expand availability to DoD programs with more sensitive data classification requirements.
- **Zero Trust Architecture:** Vasion Automate Fed's architecture implements ZTA principles: no implicit trust, continuous verification of identity and device posture, least-privilege access, and micro-segmentation of print workloads. Fully aligned with DoD Zero Trust Reference Architecture and M-22-09 milestones.

## ENTERPRISE INTEGRATION WITHOUT SECURITY COMPROMISE

A common concern for technology leaders evaluating new cloud platforms is integration complexity, specifically whether a FedRAMP-compliant environment can connect to existing enterprise systems without creating security gaps. Vasion Automate Fed is designed for enterprise integration:

### NOT ALL FEDRAMP® AUTHORIZATIONS ARE CREATED EQUAL

The FedRAMP Marketplace lists all authorized vendors transparently. Teams evaluating print and output management solutions should verify the authorization level (High vs. Moderate) and confirm active authorization status of any vendor under consideration. Some print management vendors currently hold FedRAMP Moderate authorization only, which is insufficient for high-impact data workloads. While others lack true cloud-native architecture despite marketing language.

- **Active Directory:** User authentication and group policy management through existing agency or enterprise identity infrastructure. CAC/PIV card support for federal environments.
- **SIEM Integration:** Print event logs and security alerts can be exported to agency or enterprise Security Information and Event Management platforms for centralized threat monitoring.
- **ERP, EHR, and Line-of-Business Systems:** Vasion connects to SAP, Epic, Oracle, and other enterprise platforms through secure API integrations—all within the FedRAMP authorization boundary.
- **Cloud Platform Compatibility:** Compatible with agency and enterprise cloud environments including AWS GovCloud, Microsoft Azure Government, and Google Cloud Government—all of which maintain their own FedRAMP High authorizations.

SECTION 5

# IMPLEMENTATION CONSIDERATIONS

## DEPLOYMENT TIMELINE AND APPROACH

One of the persistent frustrations federal and regulated-industry leaders face with enterprise software is the gap between vendor sales promises and deployment reality. Vasion Automate Fed's cloud-native, serverless architecture fundamentally changes the deployment equation:

- **No print servers to provision:** Eliminating on-premises infrastructure removes the most time-consuming element of traditional print management deployments. There are no servers to size, procure, rack, patch, or maintain.
- **Lightweight endpoint deployment:** The Vasion client is deployed to end-user workstations and devices through standard software distribution tools (SCCM, Intune, JAMF) with no custom scripts or manual installation required.
- **Network printer enrollment:** Existing network printers are enrolled through the Vasion cloud management console. Most standard enterprise printer models are supported without additional drivers or hardware.
- **Typical deployment timeline:** Agencies and organizations with standard enterprise environments can deploy Vasion in 4 to 8 weeks. Larger, more complex environments with specialized security configurations typically complete in 8 to 16 weeks.

## CHANGE MANAGEMENT AND TRAINING

FedRAMP®-compliant platforms introduce new authentication requirements, like Secure Release Printing via CAC/PIV or PIN, for example, that differ from the "print and forget" behavior patterns most employees are accustomed to. The Vasion implementation team supports:

- End-user training materials for federal agency and enterprise environments.
- Administrator training covering policy configuration, device management, and audit log review.
- ISSO documentation for security staff who will manage the ATO inheritance process.
- Ongoing support through the Vasion federal support team.

## QUESTIONS YOU SHOULD ASK ANY PRINT VENDOR

Whether evaluating Vasion, or any other cloud platform, for sensitive-data environments, you should demand clear answers to:

- **FedRAMP Authorization Level:** Is the vendor Authorized (not In Process or Ready), and at what impact level? Verify directly on the FedRAMP Marketplace, don't rely on vendor materials.
- **Continuous Monitoring Evidence:** Can the vendor provide current continuous monitoring reports, including vulnerability scan results and Plan of Action and Milestones (POA&M) status?

- **3PAO Identity:** Which accredited 3PAO conducted the assessment? Is the assessment current (within the past 12 months)?
- **Authorization Boundary:** What is explicitly included in and excluded from the FedRAMP authorization boundary? Ensure the specific product and deployment configuration you intend to use is within scope.
- **ATO Package Access:** Can the vendor provide their System Security Plan (SSP), Security Assessment Report (SAR), and Plan of Action and Milestones (POA&M) for your ISSO's review?

CONCLUSION

## AUTHORIZATION AS STRATEGIC ADVANTAGE

FedRAMP® High Authorization is the result of one of the most rigorous cloud security assessments available in the U.S. market, including 421 controls, independent 3PAO testing, continuous monitoring, and ongoing federal government oversight. For federal agencies, it's the legally recognized path to ATO reuse, mandate compliance, and procurement efficiency. For highly-regulated industries, it's a third-party validated trust signal that no vendor questionnaire replicates.

Vasion achieved FedRAMP High Authorization in January 2026 because federal agencies, and the highly regulated enterprises that support them, deserve print and output management solutions that meet the same security standards as their most sensitive cloud platforms. With 109 government ATOs already in place, a perfect security record across all customer deployments, and a cloud-native serverless architecture that eliminates the attack surface of legacy print servers, Vasion is positioned to be the print and output management platform of record for the most security-conscious organizations in the world.

We invite IT teams and technology leaders to review the Vasion FedRAMP Marketplace listing, request our ATO package, or speak with our federal specialists about how Vasion Automate Fed fits your specific compliance requirements and deployment environment.

### GET STARTED *TODAY*

Federal Agencies

**REQUEST YOUR ATO PACKAGE**

Explains that the ISSO needs the SSP, SAR, and POA&M to begin ATO reuse, with a checklist of what they'll receive (full authorization package, 3PAO assessment summary, continuous monitoring evidence, ISSO onboarding guide, GSA contract vehicle reference)

Complete The Ato Package Request Form

Regulated Organizations

**TALK TO OUR SALES TEAM**

Addresses healthcare, financial services, defense contracting, and critical infrastructure audiences directly, with a checklist of what the conversation will cover (regulatory alignment, vendor risk documentation, deployment timeline, security posture docs, pricing)

Contact Vasion Sales Team

APPENDIX

# GLOSSARY OF KEY TERMS

**3PAO (Third Party Assessment Organization):** An independent organization accredited by FedRAMP to conduct security assessments of cloud service providers seeking authorization.

**ATO (Authority to Operate):** The formal approval issued by a federal agency authorizing use of an information system for a specific period. FedRAMP authorization enables ATO reuse across agencies.

**CMMC (Cybersecurity Maturity Model Certification):** A DoD framework requiring defense contractors to demonstrate cybersecurity practices at defined maturity levels (Level 1 through Level 3.)

**CUI (Controlled Unclassified Information):** Government-created or government-owned information that requires safeguarding per law, regulation, or policy, but is not classified. CUI workloads often require FedRAMP High.

**DFARS (Defense Federal Acquisition Regulation Supplement):** Regulations supplementing FAR for DoD procurement, including cybersecurity requirements for contractors handling CUI.

**FAR (Federal Acquisition Regulation):** The primary regulation governing federal government procurement. FedRAMP authorization is increasingly referenced in FAR acquisition requirements for cloud services.

**FIPS (Federal Information Processing Standards):** Standards developed by NIST for use in computer systems by non-military government agencies and contractors. FIPS 140-2/140-3 govern cryptographic module standards.

**FISMA (Federal Information Security Modernization Act):** Federal law requiring agencies to develop, document, and implement information security programs. FedRAMP authorization is the recognized mechanism for satisfying FISMA requirements for cloud services.

**FedRAMP® Marketplace:** The official government catalog at marketplace.fedramp.gov listing all FedRAMP®-authorized cloud services, their authorization status, and authorization level.

**IL4 (Impact Level 4):** A DoD-specific classification for workloads containing CUI and mission-critical data, requiring enhanced security beyond standard FedRAMP High in some cases.

**ISSO (Information System Security Officer):** The individual responsible for the day-to-day security operations of an information system within a federal agency.

**NIST 800-53 rev.5:** NIST Special Publication 800-53, Revision 5—the current authoritative catalog of security and privacy controls for federal information systems, upon which FedRAMP controls are based.

**PHI (Protected Health Information):** Individually identifiable health information protected under HIPAA. PHI workloads typically require FedRAMP High or equivalent controls.

**POA&M (Plan of Action and Milestones):** A corrective action plan documenting known vulnerabilities and the timeline for remediation. Required under FedRAMP continuous monitoring.

**SSP (System Security Plan):** A document describing the security controls in place or planned for an information system. The SSP is a core component of the FedRAMP authorization package available to agencies for ATO reuse.

**ZTA/ZTNA (Zero Trust Architecture / Zero Trust Network Architecture):** A security model based on the principle of “never trust, always verify”, requiring continuous authentication and authorization for all users and devices, regardless of network location. Mandated for federal agencies by M-22-09.

## ABOUT VASION

Vasion is the intelligent print automation platform making digital transformation attainable for all by eliminating print servers, consolidating print environments, and digitizing workflows. We’re redefining modern output management with the world’s most advanced and secure cloud-native platform, turning what’s been IT’s longest-standing headache, print, into a strategic advantage. More than 13,500 global customers, including hundreds of the world’s leading enterprises, rely on Vasion to modernize and unlock AI-ready environments. With Vasion, digital transformation works for everyone.