

**Authorizing Cloud Programs:**

**Remediating the Challenges and Accelerating Adoption**

White Paper

**Introduction**

Federal agencies spend an extraordinary amount of time and effort authorizing cloud programs within the Risk Management Framework (RMF) process. For most federal agencies, obtaining an Authorization to Operate (ATO) can take up to 9-12 months or longer.

The established requirement for the RMF is a direct result of the Federal Information Security Management Act (FISMA) of 2002. For federal agencies to maintain their compliance with FISMA, they must follow the RMF guidelines put forth in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: a Security Life Cycle Approach*.

The ever-growing list of security control requirements from the NIST RMF continues to hinder operational initiatives. In its current form, authorization officials are running significantly behind on approvals, and security teams cannot keep pace with implementing the necessary controls. In order for Federal agencies to navigate and remediate these issues, they need to better understand the current challenges they face and how to effectively accelerate the ATO process through innovative, secure, and cost-efficient next generational tools and technologies.

**Table of Contents**

[**ATO Challenges 4**](#_Toc520274148)

[Lack of Understanding ‒ The Shared Responsibility Model 4](#_Toc520274149)

[Lack of Understanding of FedRAMP Packages 4](#_Toc520274150)

[Lack of Automation in Managing Controls 5](#_Toc520274151)

[Overly Manual FISMA Accreditation Processes 5](#_Toc520274152)

[Lack of Continuous Monitoring & Compliance –True “Service Availability” 6](#_Toc520274153)

[**ATO Acceleration 7**](#_Toc520274154)

[Inheriting FedRAMP Controls 7](#_Toc520274155)

[Applying Automation 7](#_Toc520274156)

[ATO Acceleration Playbook 8](#_Toc520274157)

[Continuous Monitoring and Compliance 8](#_Toc520274158)

[Organization Change for IA Professionals 8](#_Toc520274159)

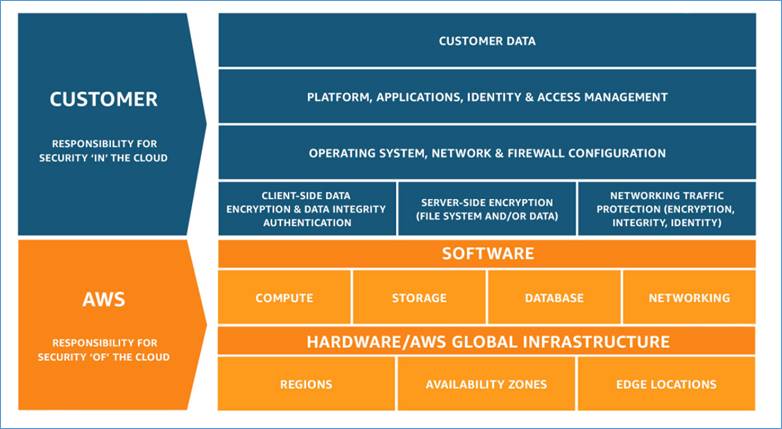
# ATO Challenges

## Lack of Understanding ‒ The Shared Responsibility Model

As agencies decide if moving to the public cloud is the right decision, they often wonder if the public cloud will offer the same level of security as their current on-premises infrastructure.

Cloud Service Providers (CSPs) have gone to great lengths to secure their infrastructure, utilizing world-class security tools and employing in-house security teams with deep expertise. Most importantly, CSP’s use a **shared responsibility model** for providing defense-in-depth security.

Amazon Web Services’ (AWS) Shared Responsibility Model (Figure 1) provides the best example.



*Figure 1* *AWS’ Shared Responsibility Model* <https://aws.amazon.com/compliance/shared-responsibility-model/>)

In the model, AWS is responsible for “S*ecurity of the Cloud*,” and the customer is responsible for “*Security in the Cloud*”. This means that AWS is responsible for protecting the infrastructure that runs all of the services offered in the AWS Cloud. The infrastructure includes the hardware, software, networking, and facilities that run AWS Cloud services. The customer’s responsibility is determined by the specific AWS Cloud services selected.

As outlined below, the shared responsibility model also extends to security controls.

**Inherited Controls**: Controls which a customer fully inherits from AWS, including:

* *Physical and Environmental controls* – documentation of a cloud offering’s security requirements, providing the framework to capture the system environment, system responsibilities, and the current status of the baseline controls required for the cloud offering.

**Shared Controls:** Controls that apply to both the infrastructure layer and customer layers, but in completely separate contexts or perspectives. In a shared control, AWS provides the requirements for the infrastructure and the customer must provide their own control implementation within their use of AWS services. Examples include:

* *Patch Management* – AWS is responsible for patching and fixing flaws within the infrastructure, but customers are responsible for patching their guest operating systems (OS) and applications.
* *Configuration Management* – AWS maintains the configuration of its infrastructure devices, but a customer is responsible for configuring their own guest operating systems, databases, and applications.
* *Awareness & Training* –AWS trains AWS employees, but a customer must train their own employees.

**Customer Specific:** Controls that are solely the responsibility of the customer based on the application they are deploying within AWS services. Examples include:

• *Service and Communications Protection or Zone*

*Security* – a customer routes or zones data

within specific security environments.

As part of the shared responsibility model, Amazon protects the underlying cloud infrastructure from vulnerabilities, intrusions, fraud, and abuse, and provides its customers with necessary security capabilities that can be configured as needed. What’s more, CSP’s like AWS and Azure continue to make significant investments in the security of their services, leading some IT leaders to argue the public cloud may actually be *more secure* than what can be achieved on premises. Customer’s deploying in the public cloud can take advantage of the shared responsibility model and accelerate more secure deployment of IT assets.

## Lack of Understanding of FedRAMP Packages

The federal government has been under a “Cloud First” mandate since 2010. More than seven years later, agencies still struggle to make cloud their first priority for IT services and infrastructure.

One of the key initiatives intended to help speed this process is The Federal Risk and Authorization Management Program (FedRAMP), a government-wide program that provides a standardized approach to security assessment for cloud-based resources. Launched with the best of intentions, FedRAMP quickly presented a number of the same kinds of roadblocks to deployment that FISMA and other federal compliance standards have imposed. Instead of facilitating moving to the cloud, FedRAMP itself became something of a barrier to entry.

The FedRAMP program has recently been streamlined to address these concerns. Still, confusion remains about the specifics required of cloud service providers that want to make their offerings available to the federal market. In particular, many CSPs aren’t familiar with the complex package of documentation they must submit for FedRAMP compliance. The complete package can run from hundreds to well over a thousand pages of documents, including:

* **System Security Plan (SSP)**: The SSP is the multi-part documentation of a cloud offering’s security requirements, providing the framework to capture the system environment, system responsibilities, and the current status of the baseline controls required for the cloud offering.
* **Controls Implementation Summary (CIS)**: This outlines the FedRAMP security control responsibilities of CSPs and customer agencies. It provides a summary of all required controls and enhancements across the system as well as implementation responsibility and status of the controls.
* **Security Assessment Plan (SAP)**: The SAP is developed by a third-party assessment organization (3PAO) to document the methodology it will use to test the controls implementation of the cloud offering. It identifies the assets within the scope of the assessment and also provides a roadmap and methodology for execution of the tests.
* **Security Assessment Report (SAR)**: This is an assessment prepared by the 3PAO containing information about vulnerabilities, threats, and risks discovered during the testing process and guidance for CSPs in mitigating them.
* **Plan of Action and Milestones (POA&M)**: A document prepared by the CSP to identify, assess, prioritize, and monitor the progress of its efforts to correct and mitigate any security weaknesses in its cloud offering as revealed by the SAR.

Other elements of the package include the FIPS-199 categorization, a privacy impact assessment, incident response plan, penetration test report, and a host of supporting evidentiary artifacts.

CSPs also need to know that many of these are living documents that must be kept up-to-date as part of FedRAMP’s continuous monitoring requirements.

## Lack of Automation in Managing Controls

A common challenge that all organizations face is regulatory and policy compliance. In government agencies and highly regulated industries, compliance with a recognized framework of controls is mandatory. Additionally, all organizations have internal policy compliance requirements such as audits, business continuity, and disaster recovery.

Cybersecurity professionals across all industries are tasked with continuously evaluating and monitoring their information systems against the required set of security controls provided by these regulations.

In the federal space, agencies must adhere to the National Institute of Standards and Technology’s (NIST) library of security controls and frameworks. For example, NIST SP 53-800, *Security and Privacy Controls for Federal Information Systems and Organizations*, is a catalog of security controls that is implemented via several federal security frameworks, including the NIST Risk Management Framework, the NIST Cybersecurity Framework, and FedRAMP.

Since its initial release, the number of security controls in SP 800-53 has climbed from less than three hundred to nearly a thousand, making it nearly impossible to manually manage compliance with them.

In addition, CSPs modify their offerings over time in response to customer requests and market demand. This natural inclination to improve a product can lead to system changes that might take the offering out of compliance—a situation known as configuration drift.

Compounding the risk of configuration drift is the fact that the controls themselves are occasionally updated. Each time there is an update to SP 800-53, for example, the system test plan must be updated to reflect those changes, which can be significant from one revision to the next. The upcoming new version of 800-53 (Rev 5) will add two new control families and result in a total of 1,000 to 1,050 controls.

A further complication for cloud offerings is the shared responsibility model of security. As observed earlier in this paper, the cloud host provides security *of* the cloud, whereas the CSP is responsible for the security of their offerings *in* the cloud. This makes it imperative that the CSP be aware of the controls under its management and be able to ensure compliance with them even when making improvements to their offerings.

Without automated and continuous controls management, a cloud offering is in constant jeopardy of falling out of compliance with the security controls it must follow in order to be used by federal agencies and other regulated organizations.

## Overly Manual FISMA Accreditation Processes

FISMA requires federal agencies to develop, document, and implement programs to provide security for the information and systems that support them. Additionally, FISMA directs agencies to implement a large range of security controls, guidelines, and frameworks developed by NIST. Agencies must successfully apply these standards for each system in order to receive an authorization to operate (ATO) that allows the system to be put into operation.

FISMA’s original certification and accreditation (C&A) process was extremely report-heavy and labor-intensive, resulting in the production of expensive multi-part documents running to thousands of pages in scores of volumes. Systems only needed to be recertified every three years, so that even a minor change to a system early on would immediately render its ATO effectively meaningless, with no recertification on the horizon.

FISMA was amended by The Federal Information Security Modernization Act of 2014 in an effort to address these concerns. Its changes resulted in less overall reporting, greater focus on managing risk, and a greater emphasis on continuous monitoring to assure the ongoing authorization and accreditation (A&A) of a system.

Nevertheless, the current A&A process for achieving ATO is still daunting. Driven by the NIST Risk Management Framework (and by FedRAMP for cloud-based systems), it is a comprehensive evaluation of an information system’s security policies, technical and non-technical security components, controls documentation, and vulnerabilities. It details the extent to which a system complies with federal mandates for security as well as the agency’s own unique guidelines. Its continuous monitoring provision requires the agency to detect and document any change in the security posture of the system to enable decision-making based on current information.

Many agencies still labor with manual tools and processes to do this work, using documents, spreadsheets, and email to manage the compliance posture of every system. Relying on manual processes to achieve and maintain their systems’ ATOs is very time-consuming, error-prone, and paper-intensive. It can take months or even years to gain approval, delaying the standup of critical systems and jeopardizing an agency’s mission as a consequence.

## Lack of Continuous Monitoring & Compliance –True “Service Availability”

FISMA’s continuous monitoring requirements in NIST SP 800-137 are intended to provide ongoing awareness of information security, vulnerabilities, and threats to better defend one’s organization. The requirements include the use of automated tools to perform periodic risk assessments, test security procedures, and detect and respond to security incidents. The intent is to de-emphasize compliance as a documentation and reporting exercise, and to accurately assess the likelihood of one’s organization in getting breached.

Continuous monitoring does not replace the security authorization requirement for federal information systems but it can transform a static security control assessment process into a dynamic process that enables an organization to track its security state in near real time.

Federal agencies’ migration to the cloud, however, has made continuous monitoring much more challenging. Cloud environments are inherently more volatile than physical environments because cloud infrastructure is driven by application programming interfaces (APIs), meaning it can be easily created and destroyed with a handful of commands. Hundreds or even thousands of servers can be brought up and down within a span of minutes or hours.

Cloud environments are typically more complex than physical environments because there are more components such as microservices, serverless functions, and containers. The practice of identifying the impact of a component as high, moderate or low becomes more difficult when the number of components increases like this.

Additionally, cloud environments provide new ways of making environment changes. Physical environments are typically located in discrete data centers or server rooms with locked down access. Anyone entering a data center must sign in and one’s activity is recorded by multiple cameras. Cloud environments, by comparison, can be changed by anyone with the right permissions and access to the cloud provider console. It is common for developers to have full access to production environments in the cloud and make changes during the development process.

# The net result is that cloud environments are more volatile than physical environments with far more components, and possessing more ways in which the environments can change. Automated tools exist to track changes in cloud environments but the tools typically do not have context to assess the security impact of these changes. For example, changing a permission in a storage bucket may be harmless or may open the storage bucket to the world. Also, there is no way to revert changes in cloud environments to a known good state or baseline configuration

# ATO Acceleration

## Inheriting FedRAMP Controls

Once a CSP has received their FedRAMP Authorization, Software as a Service (SaaS) or Platform as a Service (PaaS) providers can inherit controls from the authorized infrastructure. If you look back at the AWS Shared Responsibility Model ([Figure 1](#figure)), AWS is responsible for “*Security of the Cloud*”, and the customer is responsible for “*Security in the Cloud*”.  The CSP will be responsible Physical and Environmental controls, which will be inherited by the SaaS or PaaS. One of the benefits using a FedRAMP approved CSP is that it eliminates redundant validation of compliance for those inherited controls. Additionally, AWS’s Shared Security Model allows CSPs to easily distinguish which controls they are able to inherit from AWS. With this inheritance it is easier to build a FedRAMP compliant cloud service offering.

The CSP’s FedRAMP SSP provides the all controls to include the inherited and shared for which the SaaS or PaaS would be inheriting that control. As part of the FedRAMP process, FedRAMP allows the stacking of authorization packages like building blocks to assistance with the inheritance.

In this process, the SSP for each system must only describe the implementation of that specific system (for example, SaaS service providers would not detail any implementation details of the leveraging infrastructure provider within the SaaS service SSP). This eliminates redundancy across authorization packages and keeps authorizations delineated by system.

Leveraging the CSP’s FedRAMP compliant services like AWS, along with the proper implementation of those services and tools, enables inheritance of a sizable portion of the required security controls. The less controls your organization is responsible for means less time and money required to achieve and maintain FedRAMP compliance.

## Applying Automation

Automation has a critical role to play when operationalizing the processes for achieving a FedRAMP ATO. Emerging tools can help organizations embrace the FedRAMP process without spending heavily to meet compliance requirements. This will help reduce barriers to meeting the requirements of the FedRAMP framework and continue a sea change in securing the data and infrastructure of increasingly interconnected organizations.

Automation provides at least *two tangible benefits*: 1) Detecting violations in cloud environments and creating a streamlined workflow for collecting validation data needed to demonstrate achievement of security objectives and 2) Presenting the body of evidence (BoE) that demonstrates a standard of due care.

Fugue, the cloud infrastructure automation and security company, identifies security and compliance violations in cloud infrastructure and ensures they are never repeated. Fugue scans cloud environments and detects violations to security controls such as turning off encryption or disabling multifactor authentication. Fugue creates reports of these violations and sends them to other monitoring and reporting tools via REST API-based integration.

**Xacta**®, the security compliance and risk management solution suite from Telos Corporation, is purpose-built to operationalize the NIST family of IT security controls and to automate and streamline the NIST frameworks for cybersecurity and risk management. Serving some of the world’s most security-conscious organizations, Xacta’s capabilities have:

* **Reduced ATO process times to weeks versus many months.**
* **Eliminated 4 to 6 weeks of manual effort per project when compliance regulations changed**
* **Avoided months of manual effort in identifying, inheriting, and managing controls**

A key part of Xacta’s compliance-automation capabilities for cloud offerings is its ability to inherit controls from the cloud host’s infrastructure. This continuous controls inheritance capability streamlines and simplifies the risk assurance and compliance reporting of cloud-based systems and workloads.

Think about the effort required to document control implementation, create test procedures, and manually validate every control for each service. Xacta’s continuous controls inheritance saves tremendous time and effort by eliminating these manual and redundant steps in cloud compliance reporting.

Process automation is key to the efficient deployment of FedRAMP. Xacta’s ability to inherit security controls, collect and manage the right data, and maintain a supporting body of evidence to prove compliance changes FedRAMP from being a barrier to entry into a powerful regimen for assuring cybersecurity and enabling IT risk management for cloud-based systems.

## ATO Acceleration Playbook

The current timeline for obtaining an ATO does not typically align to the mission needs of agencies, due to the overall complexity and manually intensive steps to address and implement controls and meet the requirements of the RMF process. Because of this, agencies are often discouraged.

For example, during the RMF process, a significant amount of time and effort is spent on the implementation phase. All of the required security controls must be implemented and documented. An information system that has been categorized as a Moderate impact will typically have hundreds of controls that must be met. As a result, organizations will create page after page of documentation describing how they have implemented the required controls that have been levied on them.

There are a number of things that can be done to help agencies accelerate the ATO process. The degree of acceleration may vary depending on the size, scope, and complexity of the system; however, it is possible to greatly decrease the time and effort spent on the ATO process for even larger, more complex systems. This acceleration is made possible through applications and systems that are deployed into a cloud environments like Amazon Web Services (AWS) or Microsoft Azure.

There are multiple steps that need to be taken in order to accelerate the ATO process:

1. **Controls Inheritance**: Inherit as many authorized controls as possible from the CSPs (IaaS, PaaS, SaaS), as well as other organization services provided to the system/application that will reduce the number of required controls for validation. The less controls the system/application is responsible for means the less time and money required to achieve and maintain authorization.
2. **Security Automation**: Automate the fundamental structure of the organization’s cloud account with reliable coded security and governance in a CSP environment. Implement security tools that can assist with assessment of controls.
3. **Reusable Architecture**: Include a set of pre-approved architectures, technology stacks, and control implementation descriptions.
4. **Simplicity:** For complex frameworks like RMF and FedRAMP there should be a workflow-based system to guide the user through the process in a logical and methodical manner (like TurboTax). This can have the added benefit of reducing dependency on security/IA personnel who are expensive and hard to find.

Additionally, as part of the ATO acceleration process, agencies will need to take advantage of controls inheritance. This requires implementation of a Governance, Risk, and Compliance Management, and Compliance (GRC) tool similar to **Xacta 360®** to allow for the mapping and reduction of necessary controls.

Within the GRC, agencies must build provider projects and/or take advantage of existing projects that have already gone through the A&A process (similar to a type or generic accreditation). These projects can be used to provide controls inheritance to new projects (applications/systems) through either common or shared controls.

The provider projects built into the GRC that would be inheritable by the receiving projects would be the General Security Services (GSS) that organizations provide to their customers. Other provider projects would be the Cloud Service Providers (CSP) like AWS or Azure and additional services provided by the CSP. This maps to the [AWS Responsibility Model](#figure).

AWS is currently working with Telos, who provides Xacta 360 for the mapping of *at least 25 AWS Services as provider projects*. Xacta 360 helps customers using AWS as a CSP to accelerate ATO activities within various AWS environments like C2S, SC2S, GovCloud, and commercial regions (for FedRAMP low).

## Continuous Monitoring and Compliance

Continuous monitoring is an important element in FedRAMP. Early efforts at enforcing agency compliance with security controls for on-premises systems overlooked the need for ongoing security assurance, resulting in a static point-in-time approach to security that left federal systems vulnerable over time.

FedRAMP includes an ongoing assessment and authorization program to account for intended and unintended changes to a system and its environment once it has received a FedRAMP authorization. This continuous monitoring element of FedRAMP helps to maintain the authorization of cloud offerings on a rolling basis.

However, effective continuous monitoring requires ongoing interaction among the cloud service provider, the agency, and the 3PAO. Supporting that work requires detailed updates to the documents within the security authorization package as well as supplemental reports that provide evidence of system changes and how those changes are being reconciled with the system’s security posture.

Xacta’s continuous monitoring capabilities are ideally suited to this requirement. They empower organizations to correlate scan results from multiple security products into a single view and map them to the relevant FedRAMP controls for security and risk management. Xacta’s integration with the cloud host’s APIs also supports scanning, testing, and monitoring to continuously validate the security compliance of cloud-based resources.

Xacta then produces updated documents for the FedRAMP security authorization package including updates to the plan of action and milestones (POA&M). These documents provide sound evidence that FedRAMP baseline security controls continue to safeguard the system as originally envisioned. With Xacta, the goal of a “continuous ATO” is within reach for agencies that use cloud-based resources.

## Organization Change for IA Professionals

## Changing an organization’s culture is one of the most difficult leadership challenges. That is because an organization’s culture comprises an interlocking set of goals, roles, processes, values, communications practices, attitudes and assumptions.

## Highly regulated enterprises frequently deploy rigid controls to protect the company from the risk of security threats and vulnerabilities. Many of these controls are implemented with a series of cybersecurity processes, often manual, that drastically slow down the speed by which services are designed, developed, and deployed.

## The deployment of application services should be coupled with processes that are integrated with security and operational needs. What’s more, these processes should be flexible and scalable enough to accelerate the authorization and delivery of services to meet evolving mission-critical needs.

When agencies adopt cloud-based services, they need to take full advantage of security controls inheritance that CSPs like AWS offer. For example, AWS provides dedicated Access Control tools like as Identity and Access Management (IAM) and CloudTrail that enable agencies to securely control access to AWS services and resources while managing governance and operational auditing. These type of security controls are specifically designed to assist with speeding the authorization process while standardizing the processes by which system owners remain complaint. The design of CSP security controls inheritance tools allows for greater security and lowering of the overall cost of operations, and accelerating the authorization process for RMF or FedRAMP.



**For more information visit** [**http://www.unisys.com/federal**](https://www.unisys.com/industries/government/unisys-federal)

**© 2018 Unisys Corporation. All rights reserved.**

Unisys and other Unisys product and service names mentioned herein, as well as their respective logos, are trademarks or registered

trademarks of Unisys Corporation. All other trademarks referenced herein are the property of their respective owners.