

# Achieving FedRAMP Compliance with OpsMx Enterprise for Spinnaker





## What is FedRamp?

The Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program that promotes the adoption of secure cloud services across the federal government by providing a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. FedRAMP provides a cost-effective, risk-based approach for the adoption and use of cloud services by the federal government.

Before FedRAMP, vendors had to meet different security requirements for each federal agency. FedRAMP eliminates this duplication by providing a common security framework, making it possible for agencies and cloud service providers to reuse authorizations.

The FedRAMP program exists to verify the security and quality of cloud-managed products and services for use in government agencies. Without compliance, solution providers cannot contract with federal entities. Cloud Service Providers (CSP) that are FedRAMP authorized are listed in the FedRAMP Marketplace. This marketplace is the first place government agencies look when they want to source a new cloud-based solution. It's much easier and faster for an agency to use a product that's already authorized than to start the authorization process with a new vendor.

FedRAMP is mandatory for all Executive Agency cloud deployments and service models at the low, moderate, and high-risk impact levels. This pretty much includes all Executive departments and agencies in the U.S. Federal government.

## Challenges of FedRAMP Compliance with Software Delivery

Achieving FedRAMP compliance can be a long, complex process involving a great deal of documentation. The level of security required is mandated by law. There are many applicable laws and regulations, along with many standards and guidance documents. It's one of the most rigorous software-as-a-service certifications in the world.

One area that FedRAMP heavily scrutinizes is the software development lifecycle (SDLC), the process which develops and deploys the cloud products and services that federal agencies consume. Companies seeking FedRAMP certification quickly realize that their software delivery process and tools do not meet FedRAMP requirements.

## Governance and Security

FedRAMP is all about risk. It's a program that is designed to provide federal agencies with the information they need to make their own informed risk based decisions about whether to adopt cloud. Governance and security are at the core of FedRAMP, yet many CSP's do not have the governance infrastructure and security controls in place to provide the internal controls necessary to comply with FedRAMP. Examples include:

- *End-to-end observability and traceability of the software delivery process.*
- *A governance infrastructure that is automated and continuous.*
- *A security program that includes policies, procedures, best practices, and enforcement of things such as role-based access controls, authentication, and infrastructure hardening.*

Providing continuous and automated governance and security capabilities is an absolute requirement because any manual interventions would provide unacceptable lead times with poor quality and higher risk.

## Deployment Velocity

Highly manual release and deployment processes will not meet FedRamp requirements. Deployment automation and Continuous Delivery processes will be required to achieve the deployment velocity needed to support FedRAMP requirements. FedRAMP prescribes specific timelines to deploy things like security patches and software fixes.

Documentation is another challenge in a company's quest for FedRAMP compliance, as the regulations require full and complete records of all policies and procedures related to configuration change management or service deployment. Achieving that level of granular documentation using existing manual framework would be incredibly complex and not satisfy the requirements of government regulators.

## Achieving Compliance with OpsMx Enterprise for Spinnaker

To overcome the challenges of FedRAMP, OpsMx Enterprise for Spinnaker (OES) provides two specific benefits as it related to FedRAMP compliance: 1) OES provides a secure, agile deployment pipeline that enables cloud service providers (CSPs) the timeline and record-keeping capabilities demanded by FedRAMP. 2) Automating manually-intensive release and deployment processes to recapture valuable work hours, eliminate human error, and make the process more responsive to the needs of both regulators and crucial government clients.

OpsMx Enterprise for Spinnaker (OES) is an enterprise-ready intelligent software delivery platform that empowers enterprises to transform their software delivery by releasing faster with greater confidence and less risk. OES leverages OSS Spinnaker for its underlying multi-cloud orchestration functionality while adding simplicity, security, scale, and intelligence to the platform.

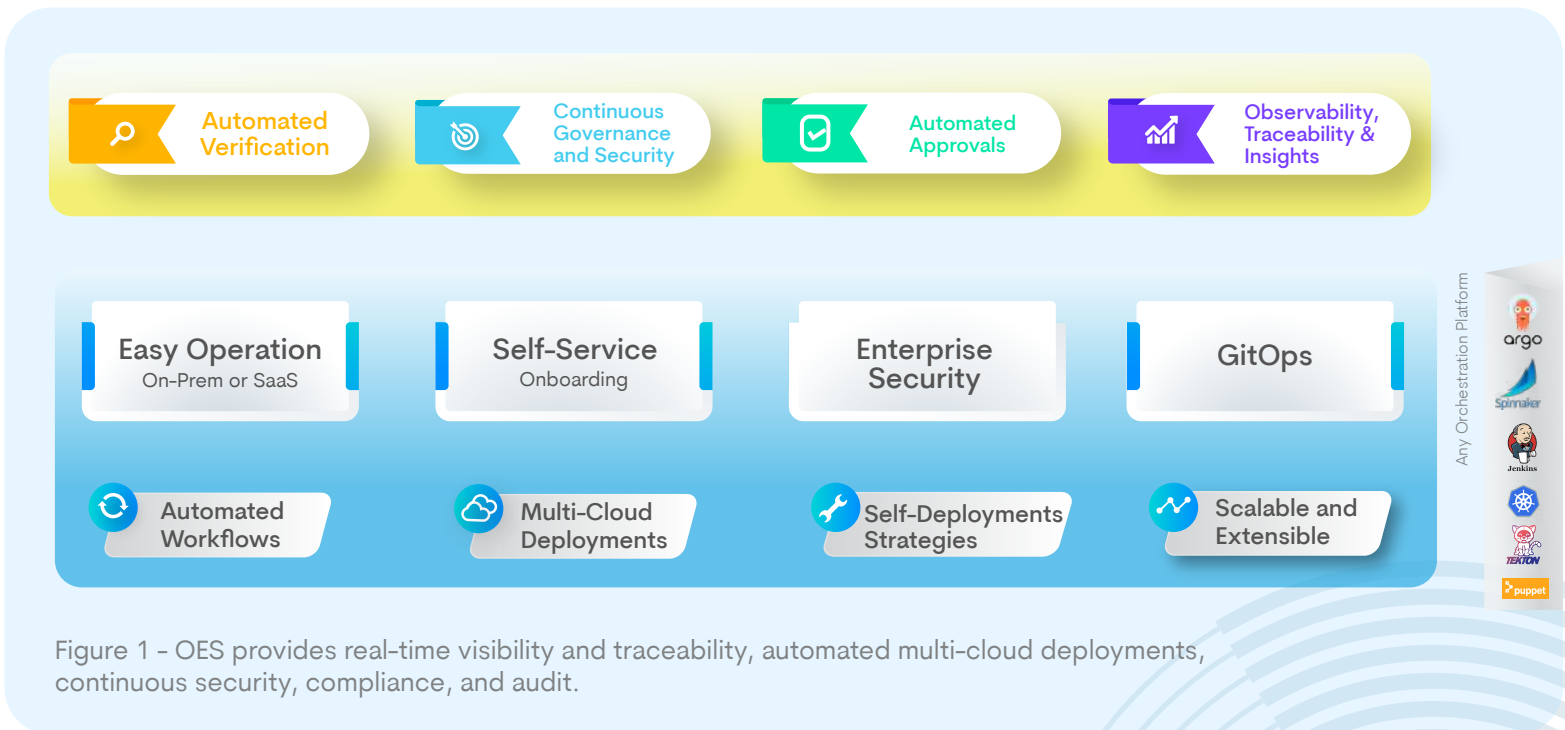



Figure 1 - OES provides real-time visibility and traceability, automated multi-cloud deployments, continuous security, compliance, and audit.

## Enterprise Security


OES mitigates security risk while increasing the software releases into production through integrating security best practices into all stages of deployment. Secure release pipelines, manage user authentication and role-based authorization, and ensure built-in protection across multiple teams, point tools, and infrastructure through hardened Spinnaker. OES supports:

- *Integrated Secrets Management - HashiCorp Vault, AWS KMS/ Key Store, or Azure Key Vault.*
- *Industry Standard Authentication - Restrict access to pipelines, projects, and accounts by hooking into the authentication systems that you are already using, such as OAuth, SAML, LDAP, X.509 certs, Google groups, Azure groups, or GitHub teams*
- *Role-Based Access Control (RBAC) - Manage the accessibility of resources and support privilege escalations for authorized access of users and groups through fine-grained control.*
- *Hardened and Certified Spinnaker with Secure APIs - Leverage secured internal service-to-service communication between the Spinnaker microservices and reduce risks.*
- *Integration with SAST, DAST, and other security tools - Gain comprehensive risk visibility and control over your CD pipeline through integration with logs, metrics, and APM tools as well as Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST), and Software Composition Analysis (SCA). Ensure readiness of Software Delivery.*

## Deployment Automation and Pipeline Management

 **Pipeline as code** - Pipeline management frequently involves changes, tracking, and controls (who/when/what). While Spinnaker natively saves pipelines as code, i.e., JSON format files, it lacks the additional support to provide tracking, approvals, etc. OES supports GitOps by seamlessly using GIT to Manage Pipeline/Template versions. OES automates and simplifies the creation of application delivery workflows with Pipeline-as-code. Pipelines are templated and provide the ability to insert fine-grain policy within the pipeline, with real-time visibility and diagnostics during the pipeline execution.


## Observability and Insight

 **Gain confidence** in releasing software by identifying defects in pipeline and application deployment through observability and deep insights. OES enables you to foster a high trust and collaborative culture through real-time observability of your complex deployments and their performance in different stages. Perform informed application approval or promotion between different deployment pipeline stages through real-time data about the release, including source code changes, build information, source code analysis, SAST/DAST tool analysis, risk verifications, and policy checks.




## Continuous GRC (Governance, Risk, and Compliance)


OES provides a continuous GRC framework by providing extensive features for policy and risk management, audit, and compliance.

 **Governance and Control** - this set of features allow you to create policies (in a declarative language) to set stringent guidelines for safe and detailed controls on the Spinnaker deployment pipeline. In addition, this feature gives you the freedom to set or declare specific policy rules or guidelines. E.g., Automated Testing should be completed before deployment, which is a rule which must be completed when creating a Spinnaker pipeline and policies.

OES Policy Management allows you to quickly declare policies and integrate with 3rd party policy managers for validations. Policy management also enables you to validate policies in runtime through 3rd party policy engines (like Open Policy Agent) using REST API. Moreover, security managers can quickly add, modify, delete policies in tune with business policy changes.

 **Verification and Risk Assessment** - This feature provides a release verification capability that provides DevOps engineers an automated real-time and actionable risk assessment of a new release deployed. The assessment verifies the latest version of the release, comparing it to the baseline or prior release after production rollout. The baseline can be deployed from a previous time or current production instance during rollout using canary or blue/green, or rolling update strategies. It leverages unsupervised and supervised machine learning and Artificial Intelligence (AI) techniques to analyze 1000's of metrics (infra and APM) and logs data to perform an in-depth analysis of architectural regressions, performance, scalability, and security violations new releases in a scalable way for enterprises.

Predictive Risk Assessment determines the risk of every update before deploying to production. Automatically analyze data from dynamic and static scans, functional tests, metrics, and logs to identify and highlight anomalies that should be considered before approval.

 **Compliance and Audit** - Ensuring compliance to industry standards and organizational policies while shipping your releases faster to production is an absolute requirement. You must be able to identify the who, what quickly, when, where, and how for your pipelines and applications through audit reports and traces. OES integrates with third-party tools within the DevOps toolchain to provide a comprehensive audit trail with searchable policy events.

With OES, you can ensure continuous compliance with FedRAMP while shipping your code, security patches, upgrades, applications to production quickly.





## About OpsMx

---

Founded with the vision of "delivering software without human intervention," OpsMx enables customers to transform and automate their software delivery process. OpsMx's intelligent software delivery platform is an ML-powered software delivery and verification platform that enables enterprises to accelerate their software delivery, reduce risk, decrease cost, and minimize manual effort. Follow us on [Twitter @Ops\\_Mx](#) and learn more at [www.opsmx.io](http://www.opsmx.io).