Achieving Cloud Application ATOs with Oracle

FedRAMP ATOs

All government applications must be granted an Authority To Operate (ATO) before being placed into production status. As defined by NIST, an ATO represents the official management decision given by a senior organization official to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security and privacy controls – NIST SP 800-37 / NIST SP 800-53A Rev 4. The ATO is granted by the agency Authorizing Official (usually the agency CIO or delegated official) and every agency has their own ATO process. For traditional on premise applications, agencies follow the processes outlined in the Federal Information Security Management Act (FISMA) documentation. For cloud applications (including those applications running on IaaS or PaaS), the process is defined by the Federal Risk Authorization and Management Program (FedRAMP). FedRAMP enables agencies to accelerate the adoption of cloud computing by creating transparent standards and processes for security authorizations and allowing agencies to leverage security authorizations on a government-wide scale.

Using Oracle's FedRAMP High P-ATO

All of the **Oracle IaaS and PaaS services available[1] in the Oracle Gov Cloud** have FedRAMP High Authorization. The full list of Oracle Cloud Services (including SaaS) are listed on the **FedRAMP Marketplace**. Oracle has undergone the rigorous process of achieving a Provisional Authority to Operate (P-ATO) at the High impact level from the FedRAMP Joint Authorization Board (JAB) for the listed IaaS and PaaS services available in the Oracle Gov Cloud. It is a "Provisional" ATO because only the agency itself has the authority to issue a final ATO for systems that the agency uses or operates. Each new application will have its own controls that must be documented and approved along with Oracle's FedRAMP controls for that application to get an ATO.

Mandatory for all Federal Civilian Executive Agency cloud deployments, FedRAMP eliminates duplicative efforts by providing a common security framework where agencies review their security requirements against a standardized baseline. A Cloud Service Provider (CSP) goes through the authorization process once, and after achieving an authorization for their Cloud Service Offering (CSO), the security package can be reused by any federal agency. Oracle's security package for Oracle Gov Cloud can be reused to reduce an agency's administrative burden and shorten the ATO process by "inheriting" IaaS and PaaS P-ATO High Impact authorizations performed by the 3rd Party Assessment Organization (3PAO) on behalf of Oracle.

[1] Upon request, certain services that have completed third party assessment and are awaiting final authorization may be allowed.

5 Steps to Achieving a FedRAMP ATO with Oracle

At a high level, an agency ATO process with Oracle has 5 steps:

1) FedRAMP approvers can request Oracle's audited security documentation package that was issued to Oracle by the JAB by using the **Package Access Request Form** found on the FedRAMP marketplace using Package ID FR1900048743.

   The FedRAMP approver that can sign a Package Access Request Form is considered to be either the agency's Chief Information Security Officer (CISO), Authorizing Official (AO), Authorizing Official Designated Representative (AODR) or Designated Approving Authority (DAA). DAAs, must have authority to grant an Authority to Operate (ATO) for an information system.

2) Oracle sets up a Virtual Reading Room with secure access to the documentation package for the FedRAMP Approvers. (This documentation is extremely sensitive and is not allowed to be copied or distributed in any other way.)

3) FedRAMP approvers reach out to the Oracle Compliance Team or the FedRAMP Program Office with any questions they have.

4) FedRAMP approvers review and document the additional security controls that apply for their specific application—beyond the FedRAMP controls provided by Oracle.

5) The agency reviews the combined authorization package with the FedRAMP and agency controls combined. If these meet their security requirements, the agency issues an ATO. Templates are available on **fedramp.gov**.

Any group requiring an ATO for a cloud application should also speak with their agency's security compliance specialist for details about the FedRAMP ATO process at their agency.

Current information about Oracle's FedRAMP Cloud Solutions is available at Oracle.com/FedRAMP

Connect with us

Call +**1.800.ORACLE1** or visit **oracle.com**. Outside North America, find your local office at: **oracle.com/contact**.

blogs.oracle.com   facebook.com/oracle   twitter.com/oracle

This device has not been authorized as required by the rules of the Federal Communications Commission. This device is not, and may not be, offered for sale or lease, or sold or leased, until authorization is obtained.

Disclaimer: If you are unsure whether your data sheet needs a disclaimer, read the revenue recognition policy. If you have further questions about your content and the disclaimer requirements, e-mail REVREC_US@oracle.com.