FedRAMP

FedRAMP High Readiness Assessment Report (RAR)

Advent

Advent Business Enablement

Version 1
2/23/2022

Company Sensitive and Proprietary
For Authorized Use Only

IMPORTANT: This FedRAMP Readiness Assessment Report (RAR) template is intended for systems categorized at the **High** security impact level, in accordance with the Federal Information Processing Standards (FIPS) Publication 199 security categorization. A RAR template for Moderate systems is available on the FedRAMP web site.

FedRAMP Ready status is valid for one calendar year after designation from the FedRAMP PMO.

THIRD PARTY ASSESSMENT ORGANIZATION (3PAO) ATTESTATION

Vaultes attests to the accuracy of the information provided in this FedRAMP Readiness Assessment Report (RAR) and Advent's readiness to meet the FedRAMP requirements as described in this RAR. Vaultes recommends that the FedRAMP PMO grant Avent "FedRAMP-Ready" status, based on the CSP's security capabilities as of 2/23/2022

This attestation is based on Vaultes' 3PAO Accreditation by the American Association of Laboratory Accreditation (A2LA) and FedRAMP, experience and knowledge of the FedRAMP requirements, and knowledge of industry cybersecurity best practices.

This FedRAMP RAR was created in alignment with FedRAMP requirements and guidance. While this report only contains summary information regarding a CSP's ability to meet the FedRAMP requirements, it is based on Vaultes' active validation of Advent Business Enablement's security capabilities through observations, evidence reviews, personnel interviews, and demonstrated capabilities of security implementations. This FedRAMP Readiness Assessment Report (RAR) is valid for one calendar year after designation from the FedRAMP PMO.

Lead Assessor's Signature:
David Nazario
Vaultes

READINESS ASSESSMENT INFORMATION

Table 0-1. System Information

CSP Name: Advent
System Name (and Abbreviation): Advent Business Enablement
Unique Identifier: 2104524844
Service Model: SaaS

FIPS PUB 199 System Security Level: (High)

Digital Identity Determination Level: (IAL3/FAL3/AAL3)

Fully Operational* as of: 2/23/20220

Number of Customers (US Federal/Others): 3

Deployment Model: Government-Only

System Functionality: Enablement auto builds software processes so no software development effort is required, and the process does not need to deploy, so it does not require any DevSecOps effort or expertise. The process can be executed instantly on an ad-hoc basis or scheduled by a non-technical novice user.

**Fully Operational means that the architectural components of the system are all in place and operating as required, and the technical controls are implemented. However, for a RAR the documentation may be partially developed.*

EXECUTIVE SUMMARY

The Vaultes 3PAO team assessed the Advent Business Enablement solution (2104524844) for FedRAMP readiness. As described in the following sections, Advent is a cloud-based SaaS solution which is nearly entirely based on cloud-native technologies present in the AWS GovCloud environment. The resulting architecture is comprised nearly entirely of FedRAMP authorized AWS cloud services. The Advent solution is a technology-mature implementation which is well architected according to AWS security best practices including multi-tiered segmentation between management, data, and presentation zones. Advent leverages security features within AWS to provide isolation within its environment including multiple VPCs, cryptographic isolation for customer data, and very limited external connection exposure. The notable strengths to the Advent solution include the previously mentioned focus on cloud-native technology, strong isolation for data storage and transmission, and limited attack surface from external connections and dependencies. In combination, these strengths provide significant reductions in risk exposure and threat vectors for the organization and environment and demonstrate that Advent possesses the security, technical and process maturity to permit Vaultes to recommend Advent Business Enablement as FedRAMP Ready.

Additional areas of consideration for the Advent solution include Advent's usage of an internal JSON Web Tokens (JWT) implementation to configure application permissions and integrate with other SAML-based identity providers. The usage of JWT is common across the Federal government within Oauth 2.0 implementations but may cause additional validation burden for the PMO and 3PAO in a full assessment in order to review the Advent internal identity configurations and permissions implementation for completeness. Secondly, the Advent documentation will require updates to the SSP, policies and procedures, and the additions of at least 3 policies and procedures in order to fully address FedRAMP requirements. The Vaultes team estimates the level of documentation completion at 65%.

Federal Mandates - Advent Business Enablement leverages existing FedRAMP authorized solutions for key generation and key management providing FIPS 140-2 validated cryptographic modules where used. Key generation policies and procedures lack specific guidance on key selection and requirements. The Vaultes team reviewed the cryptography in use for database storage, encryption keys, and validated that AWS endpoints by the Advent Business Enablement solution in use are appropriate AWS FIPS endpoints. All ingress and egress connections to AWS are encrypted with FIPS validated cryptography. Vaultes reviewed the configuration of the application by reviewing the code base and confirmed that encryption settings in use are referencing approved algorithms. Advent Business Enablement supports SAML assertions through the use of JSON Web Tokens (JWT) which integrates with SAML based solutions including Common Access Card(CAC) and Personal Identity Verification (PIV). Vaultes reviewed the configuration of the application's SAML assertions within the Advent Business Enablement source code. DIdentity Level 3 protections are achieved with a hardware (TPM-backed) cryptographic signature which was reviewed by Vaultes as part of the assessment. The Advent Team leverages AWS Security Hub, AWS Inspector, AWS Config, and Nessus to perform vulnerability scanning, and has historical evidence of vulnerability remediation of High vulnerabilities within 30 days, Moderate vulnerabilities within 90 days, and Low vulnerabilities within 180 days. The system utilizes retention policies on S3 buckets which exceed NARA guidelines for online and near-online storage. Vaultes manually validated that the Advent DNS resolution supports DNS Security (DNSSEC).

Advent Business Enablement uses granular roles within the application to provide least privilege and separation of duty functions within the application. Multi-factor authentication is configured for all system access including Advent Business Enablement system administrators. The system requires separate accounts for privileged and non-privileged access to the application which is enforced through IAM roles. All privileged actions (access and modification) are logged by the system. The Advent system does not have a mature SIEM capability providing centralized and real-time analysis of security events. The Advent Business Enablement solution leverages images hardened against the CIS benchmarks as the operating system baseline for EC2 instances in the environment. The baseline image settings are retained in GitLab which includes all services running on the system. The status of configuration settings is tracked using Inspector and Nessus to confirm that drift does not occur. The Advent team has a mature change management policy and process which includes change approvals and a fully functioning Change Control Board (CCB).

TEMPLATE REVISION HISTORY

Date	Description	Template Version	Author
4/26/2017	Initial release version	1.0	FedRAMP PMO
8/28/2018	Added clarifications throughout. Added requirements that provide better visibility into system interconnections and external services.	1.1	FedRAMP PMO
2/13/2019	Verbiage added to the top of document and to the 3PAO attestation stating the expiration date of the report.	1.2	FedRAMP PMO
7/31/2020	Updated to include Locality checks for data centers	1.3	FedRAMP PMO
4/1/2021	Updated Table 4-3 Transport Layer Security to include TLS 1.3	1.4	FedRAMP PMO
1/4/2022	Added clarifications throughout. Updated to clarify requirements that apply to CSPs pursuing a JAB P-ATO but do not apply to an Agency ATO. Rearranged sections to reduce duplicate information and improve document flow. Updated instructional notes.	1.5	FedRAMP PMO