Ignyte Assurance Platform Receives FedRAMP 3PAO Designation

Ignyte Platform Inc. announces its FedRAMP third-party assessment organization (3PAO) designation and appears on FedRAMP Marketplace on May 31, 2022.

DAYTON, OH, UNITED STATES, June 1, 2022 /EINPresswire.com/ -- Ignyte Platform Inc. is proud to announce that the Federal Risk and Authorization Management Program (FedRAMP) has recognized it as a designated third-party assessment organization (3PAO). This designation is over a year in the making after Ignyte announced in May of 2021 that it reached ISO 17020:2012 accreditation.

FedRAMP is the United States Federal government's way of ensuring the cloud-based products and services it uses are secure. It was developed and is managed by the FedRAMP Program Management Office (PMO) which works closely with other departments and organizations to ensure a robust and comprehensive authorization process.

> "We're a digital-first audit firm that's built on delivering automated, OSCAL-based FedRAMP assessments. We've been on both sides of the audit process, so we know what it takes..."
>
> *Aaron McCray, COO at Ignyte Platform, Inc.*

An overview of the entire FedRAMP process taken from FedRAMP.org

Any organization that offers a cloud-based product or service to the U.S. government has to comply with FedRAMP.

According to the 2011 FedRAMP Policy memo, FedRAMP is applicable to:

1) Executive departments and agencies procuring commercial and non-commercial cloud services...

2) All cloud deployment models (e.g., Public, Community, Private, and Hybrid clouds)

3) All cloud service models (e.g., Infrastructure as a Service, Platform as a Service, Software as a Service)

Ignyte prefers to break the road to FedRAMP authorization into 6 phases, and one of the most critical phases involves contacting a 3PAO to perform a security assessment. A 3PAO is an independent organization (i.e., separate from the organization being assessed) that performs assessments at the onset of the FedRAMP authorization process on an ongoing basis.

3PAOs are vital for any organization looking to break into the Federal Marketplace. Specialized 3PAOs, such as Ignyte, can also make extremely effective partners to go beyond FedRAMP into the classified Department of Defense market.

“Ignyte is extremely proud to be recognized as a FedRAMP 3PAO,” said Aaron McCray, COO. “We’re a digital-first audit firm that’s built on delivering automated, OSCAL-based FedRAMP assessments. We’ve been on both sides of the audit process, so we know what it takes to make the journey as easy and painless as possible. This designation is a huge achievement for us and wouldn’t have been possible without the support and efforts of the entire Ignyte team and our federal partners.”

To become a FedRAMP 3PAO, Ignyte went through a rigorous diligence process for more than a year. The official assessment criteria included the following:

1) Whether Ignyte has a fully operational, and adequately maintained Quality Management System (QMS) that meets ISO 17020 and FedRAMP-specific requirements;
2) Whether the Ignyte team is competent to perform automated cyber inspections of cloud service providers (CSP);
3) Whether Ignyte can demonstrate the technical competence of individual assessors through education, training, technical knowledge, skills, and experience.

Just like a FedRAMP authorization, Ignyte has to undergo a full reassessment every 2 years to maintain its 3PAO status.

Ignyte offers 3 distinct FedRAMP solutions - FedRAMP Certification, FedRAMP+ Certification, and FedRAMP Renewals – all of which leverage Ignyte’s Automation platform.

With over 1000 audits performed and an average cost savings of 35% per project, Ignyte is the perfect 3PAO to engage for FedRAMP audits. Look for Ignyte on the FedRAMP marketplace under the Assessors tab.

About Ignyte
Ignyte Assurance Platform is a leader in collaborative security and integrated GRC solutions created for streamlining compliance and audit processes to enhance the organizational cybersecurity posture of both corporate and Federal government. Its AI-enabled risk

management software is designed to help Chief Information Security Officers (CISOs) manage cyber & regulatory risk and meet multiple regulations at once by leveraging language and intent matching. It maximizes resource time, produces real-time reports, automates the evidence collection processes, and increases overall trust in the organization's regulatory compliance response. As a result, it has reportedly improved the efficiency and GRC efforts of organizations such as Allina Health, Cincinnati Children's Hospital Medical Center, St. Joseph Health Hospital, Global Ordnance, UFCU, and others.

Learn more here: https://ignyteplatform.com/

To view Ignyte's Accreditation Certificate:
https://customer.a2la.org/index.cfm?event=directory.detail&labPID=666D9226-426E-4968-828F-F7BFFDA92056

About ISO/IEC 17020:2012

ISO/IEC 17020:2012 specifies requirements for the competence of bodies performing inspection and for the impartiality and consistency of their inspection activities. It applies to inspection bodies of type A, B or C, as defined in ISO/IEC 17020:2012, and it applies to any stage of inspection.

More information here.

Max Aulakh
Ignyte Assurance Platform
email us here

This press release can be viewed online at: https://www.einpresswire.com/article/574782323

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.
© 1995-2022 Newsmatics Inc. All Right Reserved.