Vencore Corporate Overview

Core Service and Solution Capabilities
- Systems Engineering & Integration
- Data Analytics
- Cyber Security
- Advanced Research

Security Clearances
- Multiple Clearance Levels

Trust
- Secure Facility

Customers
- Department of Homeland Security
- Department of Defense
- Department of State
- General Services Administration
- NASA
- Commercial organizations
- CSPs

Why Vencore?
- Certifications include CISSP, CISA, CRISC, CECS, FITSI-A, ITIL Expert
- FedRAMP Accredited 3PAO
- CMMI Maturity Level 3; ISO 9001:2008;
- ISO 20000-1:2011; AS9100
- Accredited ITIL Training Provider
- Experience in ISO, CMMI, AS9100 and other national / international quality programs
- Long history of involvement in audits / assessments / appraisals
- Highly credentialed and experienced assessment staff
- Deep bench of experienced information assurance staff
- Qualified teaming partners
- Innovative solutions to support defense, security and intelligence organizations
- A premier provider of world-class technology, responsive solutions and innovative solutions
- A proven, reliable partner to the U.S. Government and industry

Contracts include:
- Information Technology Support Services (ITSS-4); Federal Supply Schedule 70
- U.S. Army Aviation and Missile Command (AMCOM) Expedited Professional and Engineering Support Services (EXPRESS)
- Professional Engineering Services: Federal Support Schedule 871

VENCORE™

FOR MORE INFORMATION
Vencore 3PAO
15052 Conference Center Drive
Chantilly, VA 20151
Tel: (571) 521-7700
3PAO@vencore.com

VENCORE™

FedRAMP 3PAO Accredited SM

FedRAMP SM

Third Party Assessment Services for Cloud Service Providers

Vencore is a Federal Risk Authorization and Management Program (FedRAMP) accredited third party assessment organization (3PAO) for conducting security assessments for cloud service providers (CSPs).

Cloud Computing Security Challenges

Cloud computing is fundamentally changing the way organizations work with data. With its unlimited scalability, potential cost savings and virtualized mobile access, cloud architecture is increasingly attractive to federal government and commercial organizations.

Although most CSPs have considerable experience in data center management, application hosting and virtualization, they may not have the ability to balance performance with the diverse security needs of a large customer base. Assessing the risks associated with cloud computing, such as data integrity, privacy, recovery and multi-tenant isolation, is critical to the adoption of cloud technologies. The solution lies with the cloud security services of Vencore, a FedRAMP accredited 3PAO.

Vencore 3PAO plays a key role in the development and implementation of FedRAMP and Risk Management Framework (RMF) requirements for our customers. Our extensive knowledge of FISMA and other regulatory compliance mandates allows us to help transform the way government and commercial organizations work as they move IT infrastructure and services to a cloud environment. We align our customers with the correct policies, procedures and systems to meet National Institute of Standards and Technology (NIST) and other regulatory security controls. Vencore provides organizations with a thorough evaluation of the security risks and exposure that stem from cloud computing for all data types and sensitivity levels, and we help prepare them and their systems for the rigors of Authority To Operate (ATO) granted by FedRAMP JAB or federal agencies.

Training

Vencore offers the following training modules:

1. Cloud Computing Fundamentals
2. FedRAMP and 3PAO Overview
3. FedRAMP Requirements and ATO Certification Process
4. FedRAMP Security Controls and Implementation Guidelines
5. FedRAMP Continuous Monitoring REquirements

How can we help you with your FedRAMP needs?

As an accredited 3PAO, Vencore can provide advisory services or assessment services.

As an advisor, we can assist CSPs with understanding the requirements, impacts to their business and best practice approaches to obtaining FedRAMP certification.

For CSPs interested in becoming an authorized FedRAMP provider, Vencore can conduct an independent assessment conforming to FedRAMP requirements.

What is FedRAMP?

FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization and continuous monitoring for cloud products and services. This approach uses a "do once, use many times" framework that will save funds, time and staff required to conduct redundant agency security assessments. To become ATO granted by FedRAMP JAB or Federal Agencies, CSPs must use a FedRAMP-accredited 3PAO to independently validate and verify that they meet the FedRAMP requirements.

What is a 3PAO?

A 3PAO is an independent third party assessment organization to verify CSPs' conformance to FedRAMP requirements. Vencore is a 3PAO and operates a comprehensive management system and audit/assessment practice based on years of experience in achieving national and international quality credentials. Vencore 3PAO personnel have the required skills and experience to carry out assessments in accordance with FedRAMP requirements. The Vencore 3PAO organization is able to draw on a deep bench of highly qualified Information Assurance staff to support 3PAO engagements. In addition, the Vencore 3PAO organization has established agreements with qualified teaming partners to enhance the depth of expertise available to clients.

Vencore 3PAO Services

Consulting - Review of a CSP's security architecture and security controls; support in the development of the required documentation and implementation of the security controls to satisfy FedRAMP requirements and includes:

- SSP review and development support
- Other required documentation review and development support
- Security controls review and implementation support
- ATO application package development support

Pre-Assessment - Preliminary review and gap analysis to determine a CSP's security architecture and safeguard requirements that includes a review of the following:

- System Security Plan (SSP)
- Security policies and procedures
- Security controls

Assessment - Independent, multilevel security testing and assessment that includes:

- Security Assessment Plan (SAP) development
- Documentation audit
- Security testing
- Authenticated scans
- Penetration testing
- Security Assessment Report (SAR) development

Continuous Monitoring - Continuous monitoring to ensure ongoing FedRAMP compliance that includes:

- Authenticated scans
- Penetration testing
- Subset of Security Controls Assessment
- Assist in CSP self-attestation, change control and incident response reporting