Performing initial, annual and significant change assessments for cloud service providers

**Partnerships**
- Membership and active participation with American Council for Technology and Industry Advisory Council (ACT-IAC) for improvements in FedRAMP certification process
- Partnership with Amazon Web Services (AWS) for support to AWS-based business solutions and Microsoft for support to Microsoft Azure solutions
- Agreements with qualified teaming partners to enhance the depth of expertise available to customers

**Perspecta Third Party Assessment Organization (3PAO)**

Performing initial, annual and significant change assessments for cloud service providers

**Balancing complex mission and cloud initiatives**

Perspecta Third Party Assessment Organization (3PAO) is an accredited Federal Risk Authorization and Management Program (FedRAMP) 3PAO conducting security assessments for cloud service providers (CSP).

Perspecta 3PAO has extensive experience in security control implementation and the evaluation of mission critical information systems for various government agencies. We provide customers with the technical, policy and operational insight required for a successful compliance assessment to achieve FedRAMP Authority to Operate (ATO) certification, FISMA Compliance (NIST 800-53 Rev 4), NIST 800-171 Compliance, Department of Defense (DOD) Risk Management Framework (RMF) compliance and the CC SRG.

Perspecta 3PAO performs initial and periodic assessments of security controls for CSP. Granted initial accreditation under FedRAMP in July 2013, Perspecta 3PAO was successfully re-certified by the American Association for Laboratory Accreditation (A2LA) in July 2020.

As FedRAMP will only review security assessment packages from CSPs that have been assessed by an accredited 3PAO, Perspecta 3PAO provides the path for either the preparation of assessment or the formal assessment and continuous monitoring of services.
We provide multiple levels of security assessment services for cloud products and services to help our customers comply with FedRAMP requirements.

Assessment services include:
- Training / technical education
- FedRAMP overview, readiness and ATO process requirements
- ATO documentation package and contents
- Security control implementation guidelines
- Continuous monitoring requirements
- FedRAMP Ready Assessment
- FedRAMP Initial Authorization Assessment
- FedRAMP Annual Assessment for Continuous Monitoring
- FISMA (NIST SP 800-53) and DOD Cloud Computing SRG (FedRAMP+)
- NIST SP 800-171
- Vulnerability assessment and compliance scans
- Multi-vector penetration testing

Advisory services include:
- Classification alignment for accreditation areas
- Shared compliance evaluations
- ATO document package creation
- Security control implementation subject matter expertise
- Gap assessment
- Training/technical education

Experience
- Advisory services to CSPs for implementation of the required security controls to satisfy FedRAMP IaaS and SaaS ATO requirements
- FedRAMP ATO security assessments for CSP to achieve agency IaaS and SaaS ATO
- FedRAMP Readiness Assessment for CSP to achieve the FedRAMP Ready status
- Training on the rigors of ATO process and proper documentation

Perspecta 3PAO security assessment services
- As an assessor, Perspecta 3PAO conducts independent security control assessments conforming to requirements, to result in compliance or (Agency/FedRAMP) ATO certification
- As an advisor, Perspecta 3PAO assists organizations to develop an understanding of the requirements, impacts to their business and best practice approaches to obtaining compliance or (FedRAMP or Agency) ATO certifications

About Perspecta
Perspecta, formed through the combination of DXC's U.S. Public Sector business with Vencore and KeyPoint Government Solutions, is currently listed on fedramp.gov as Perspecta 3PAO.

We bring a diverse set of capabilities to U.S. government customers in defense, intelligence, civilian, health care and state and local markets. With offerings in mission services, digital transformation and enterprise operations, our nearly 14,000 employees work tirelessly to not only execute the mission, but support the backbone that enables it.