DECISION LENS AND FEDRAMP OVERVIEW

"What is FedRAMP?"

The Federal Risk and Authorization Management Program, or 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 saves an estimated 30-40% of government costs, as well as both time and staff required to conduct redundant agency security assessments. As a FedRAMP Compliant CSP, Decision Lens offers enhanced security, assurance, and compliance for its customers throughout the federal government, including Department of Defense.

WHAT ARE THE BENEFITS?

Real Cost Savings: Reduce acquisition time, save certification costs, reduce duplicated effort, and focus on agency-specific requirements with a Software as a Service (SaaS) solution that meets government cloud security and availability requirements.

Enhanced Security: Implementation of over 300 rigorous security controls to protect sensitive customer data.

Increased Availability & Reliability: Highly available and reliable cloud platform hosted on Amazon Web Services (AWS) GovCloud Infrastructure as a Service (IaaS).

Independently Verified Compliance: FedRAMP Moderate and DoD IL4 controls are assessed annually by a FedRAMP accredited Third Party Assessment Organization (3PAO).

Continuous Monitoring: Able to respond immediately to threats through regular system log monitoring, file integrity monitoring, intrusion detection and prevention, vulnerability scanning, and penetration testing to ensure ongoing system integrity and availability.

Transparent Reporting: Agencies can receive monthly reports detailing Decision Lens' Continuous Monitoring activities and analysis. ATO package is available for review by any customer or potential customer.

DECISION LENS OVERVIEW

Decision Lens is the complete, end-to-end software solution and business process for identifying, prioritizing, analyzing, and measuring which investments, projects, or resources will deliver the highest returns to your organization, while empowering you to quickly react to ever-changing data.

Decision Lens is a FedRAMP-compliant Cloud Service Provider (CSP) and has been granted an Agency Authority to Operate (ATO) by GSA and DOI. Decision Lens has demonstrated compliance with FedRAMP requirements based on the NIST 800-53 Rev. 4 Moderate baseline as well as the Impact Level 4 requirements from the Department of Defense Cloud Computing Security Requirements Guide.

FEDRAMP SOLUTION MATRIX

Personnel Security

- Corporate controls around employee background checks, transfer, and termination
- Cleared personnel occupying sensitive positions such as security officer and system administrator

Awareness and Training

- Initial and annual security awareness training leveraging leading commercial training providers
- Role-based security training for users with sensitive security roles

Auditing and Accountability

- Continuous diagnostic monitoring of system activity
- Defined audit log content
- Non-repudiation of privileged actions
- Centralized monitoring and reporting

Incident Response

- Incident response capability fully documented and tested at least annually
- Full government incident reporting mechanisms, including DIBnet ICF

Configuration Management

- All changes controlled, documented, and approved prior to deployment
- Tight configurations supporting security hardening and least functionality (CIS benchmarks and DISA STIGs)

Identification and Authentication

- Multi-factor authentication via Google Authenticator
- Password complexity enforcement
- Password management options (expiration, history)

Planning

- 560+ page System Security Plan documenting the full security posture of Decision Lens Software.
- DoD SSP Addendum addressing General Readiness controls and Impact Level 4 controls.
- All security planning activities are coordinated with numerous stakeholder groups, internal and external to DL Security

Security Assessment & Authorization

- Full FedRAMP package available for Agency review & authorization.
- Continuous, monthly updates of known issues via POA&M (Plan of Actions & Milestones)
- Continuous monitoring reports available on an ongoing basis, compiled monthly, submitted to OMB MAX.

Maintenance, Physical and Environmental Protection, Media Protection

- Fully provided by Amazon Web Services, a FedRAMP compliant Infrastructure-as-a-Service provider

Contingency Planning

- Contingency and disaster recovery plan fully documented and tested
- Guaranteed application availability with AWS regions (US East/West) and load balancing across multiple availability zones
- Customer data backups every 4 hours, securely moved from US East to US West Access Control

Access Control

- Account Management
- Well-defined separation of duties and least privilege role-based access
- Privileged use monitoring
- Deny by default Network ACLs
- Invalid login attempts lockout
- Custom legal notice/warning banner per customer instance

Risk Assessment

- Decision Lens undergoes an initial full assessment of all 325 controls in the FedRAMP baseline, the entire IL4 baseline, and annual controls of a subset every year thereafter
- Fully credentialed vulnerability scans, at least monthly, for all servers, web applications, and databases
- Critical/high vulnerabilities are remediated ASAP

Systems and Services Acquisitions

- All potential products are assessed for impact on Decision Lens security posture
- Any services with significant interconnectivity must also be FedRAMP compliant, e.g. AWS
- Best practices agile development process makes security a priority
- Veracode static and dynamic code scans
- Fully defined and documented Supply Chain Risk Management plan

System and Communications Protection

- External connections for both DL admin staff and customers are secured with FIPS 140-2 approved algorithms and strong cipher suites
- Denial of Service protection provided by AWS
- Restrictive, granular boundary protection implemented through AWS Security Groups
- Encrypted customer database backups

System and Information Integrity

- Continuous system monitoring at the AWS VPC and server level
- File integrity monitoring of vital system and application files
- Fully separate development and production environments and support staff
- Vulnerability fixes and application bug fixes deployed to production quickly and safely through flaw remediation process