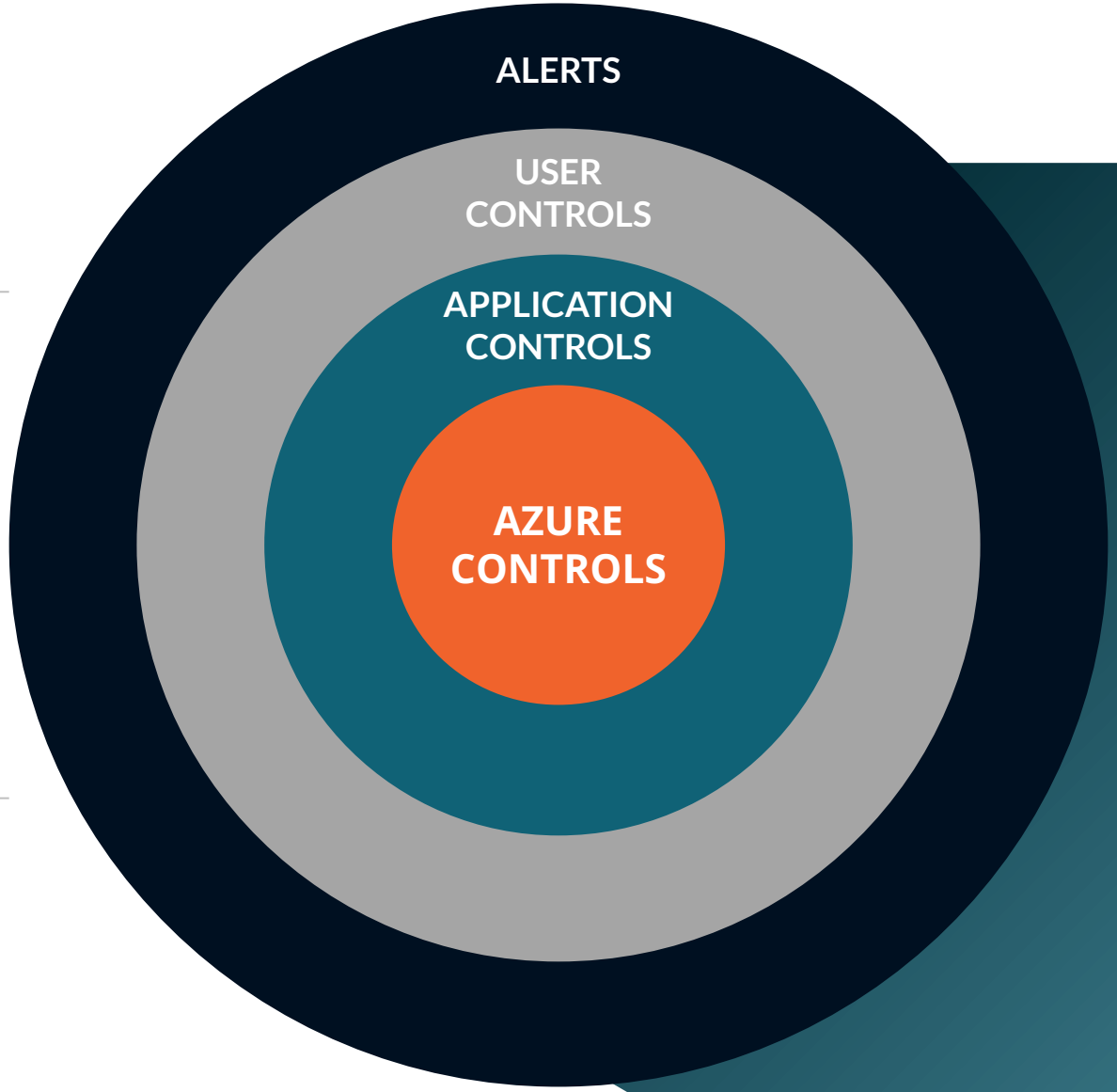
DiligenceVault

DATA SECURITY OVERVIEW

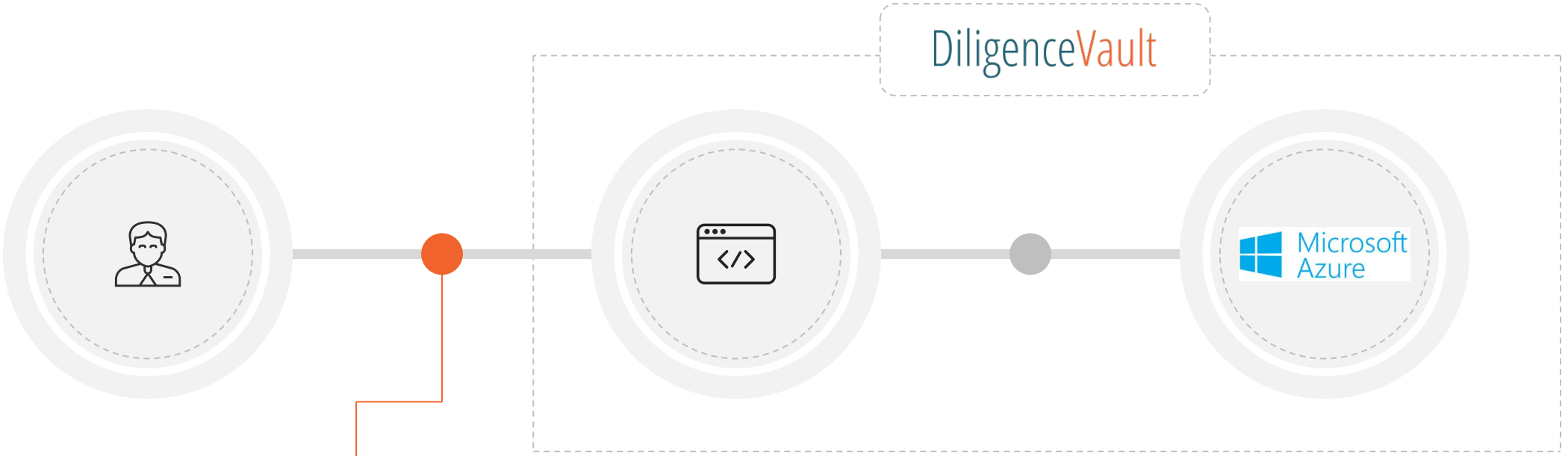
2023

Layers of Data Security Control



Architecture leverages industry best practices and is designed with controls at each layer of data access

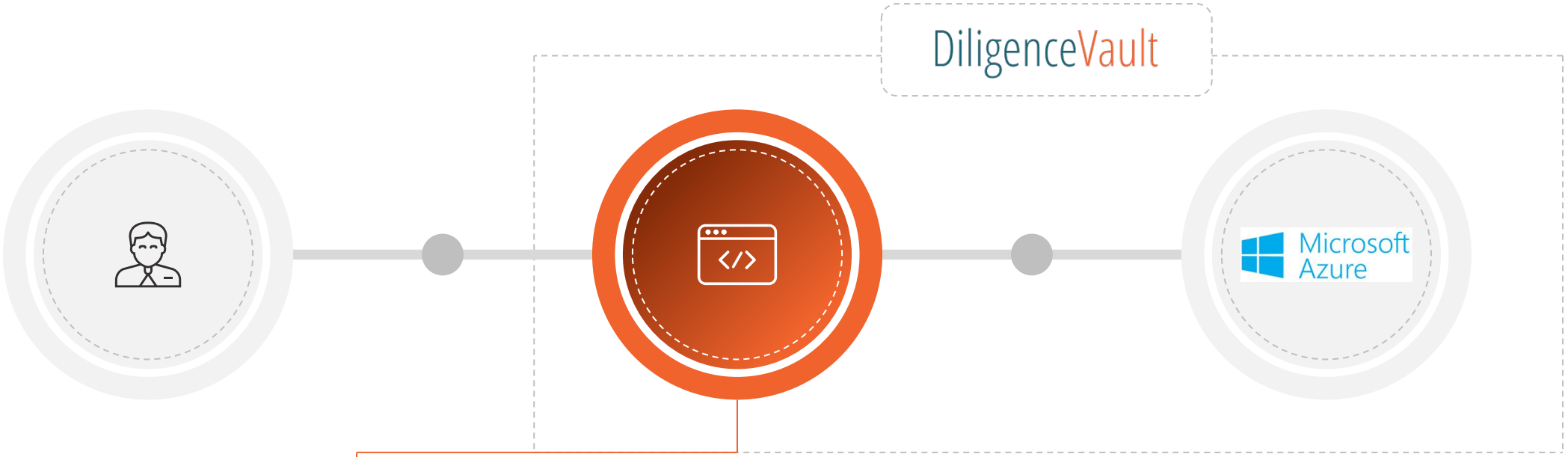
User Access Security & Controls



01

- Complex password and configurable reusability criteria
- Two-factor authentication
- IP address whitelisting
- Domain whitelisting
- Single sign on
- Role-based authorization
- Token-based session management
- Access failure lockouts and security alerts
- Traffic monitoring and IP address logging

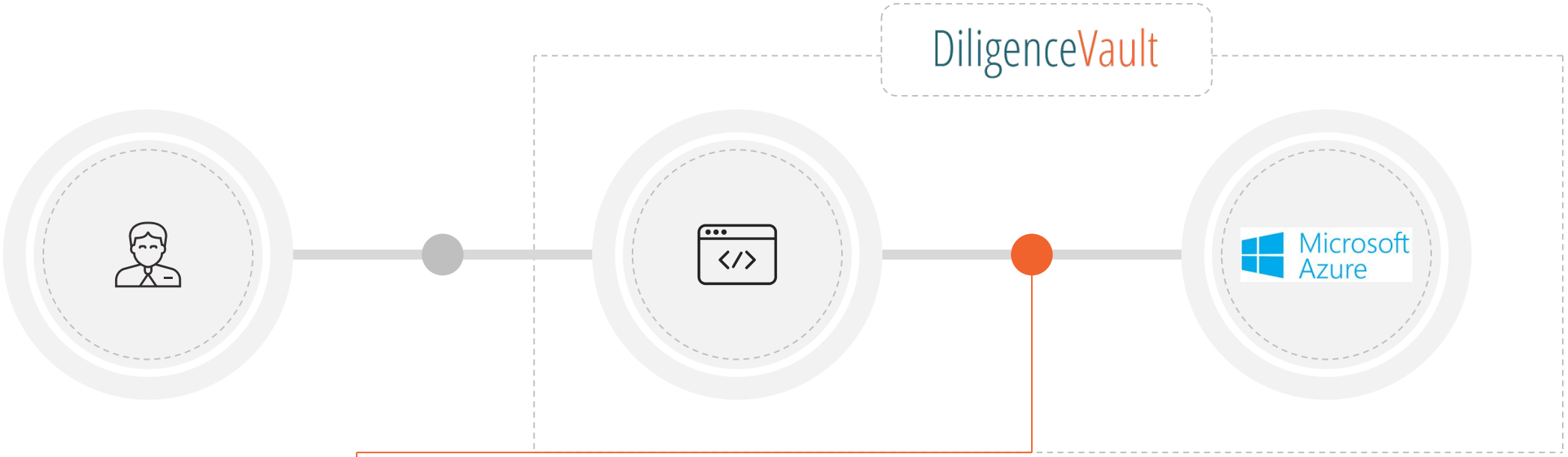
Product Security & Controls



02

- Data encryption in transit
- Signed URLs with expiry for document access
- Identifying information masking
- Pre-authorization at each request
- Cross server scripting protection
- Periodic application penetration testing
- SOC 2 Type II & ISO 27001 certification for the application
- Security and service degradation alerts

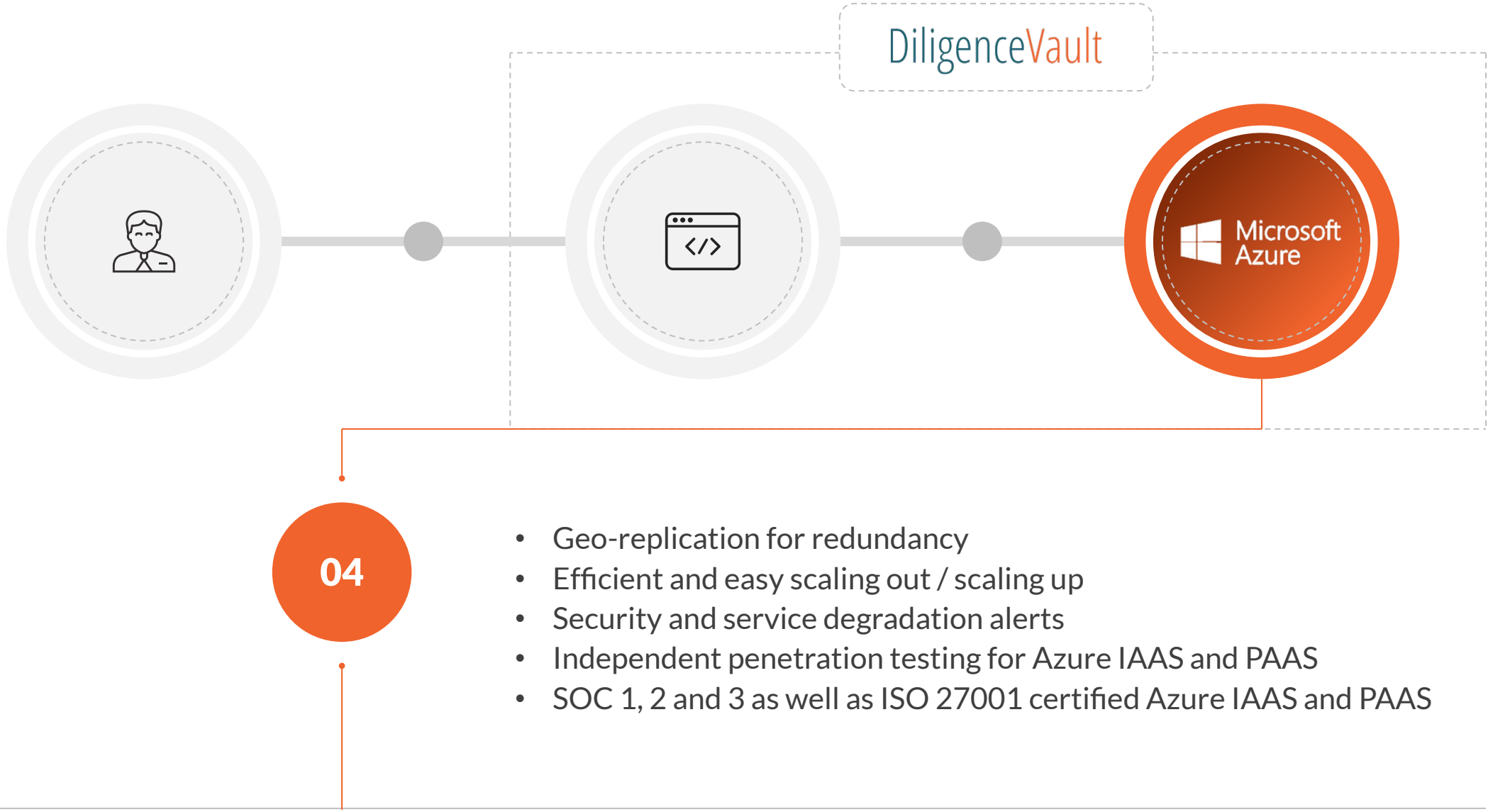
Data Security & Redundancy



03

- Data encryption at rest
- Data masking
- IP whitelisting
- Institutional controls for patching
- Periodic DR & BCP testing across infrastructure, application and microservices
- Auditing / logging for threat detection
- Security and service degradation alerts

Infrastructure Security & Redundancy



- Geo-replication for redundancy
- Efficient and easy scaling out / scaling up
- Security and service degradation alerts
- Independent penetration testing for Azure IAAS and PAAS
- SOC 1, 2 and 3 as well as ISO 27001 certified Azure IAAS and PAAS

DiligenceVault's Operational Controls

— Our commitment and capacity towards providing the best-in-class services for our clients

Application Security Enforcement

Security aspects of the application are reviewed during peer reviews as well as there is periodic sharing of best practices. Application data subprocessor selection goes through security review and list can be found here

Change Management

There is a formal framework for change management to the production infrastructure and software. The process if tightly coupled with different environments to manage the change management process which is documented in JIRA.

Training and Awareness

Everyone at DiligenceVault receives security and privacy awareness training both as part of their on-boarding and as a refresher on an ongoing basis. Alerting on social engineering and phishing attempts is strongly encouraged.

Incident Management

An alerting process is in place for unauthorized access to the application and the infrastructure. There is a formal incident management program in place to ensure corrective action and notification to the clients.

THANK YOU!

FOLLOW US ON LINKEDIN	https://www.linkedin.com/company/diligencevault
VISIT OUR WEBSITE	www.diligencevault.com
CHECK OUT OUR BLOG	https://diligencevault.com/blogs/

DiligenceVault