OTC BILATERAL MARGIN SERVICE

THE SITUATION

The financial service client set out to develop a centralized initial margin (IM) infrastructure that supports the mandatory exchange of IM for non-cleared OTC derivatives, as required by new global regulations which take effect from December 2016 for the G15 broker dealer banks and other large systemically important institutes. (i.e. Exposures >$3trillon)

The service sought to introduce several policy and systemic risk benefits to the non-centrally cleared derivatives markets where a disproportionate amount of risk exists and could significantly contribute to the financial stability and orderly markets immediately following a global bank default.

THE CHALLENGE

The client were looking for a vendor to:

1. Design and build end to end cloud infrastructure from development to production

2. Provide support and knowledge transfer to the client's development team in terms of Amazon Web Service adoption and development automation techniques, tools and best practice

3. Lead the ISO 27001 certification from subject matter expertise perspective.

4. Assist with the clients FCA regulatory approval process.

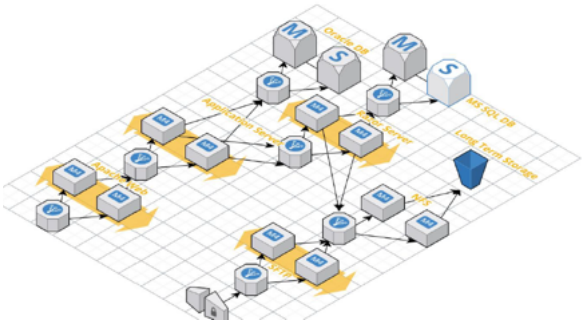
THE SOLUTION

LayerV was successfully selected as AWS Design Partner, Security Advisor and Managed Service Provider.

LayerV staff are all based in the EU to best meet data protection laws. The LayerV European Technical Centre operates 24 x 7 to manage client systems, including operation of the comprehensive managed security service Continuous Compliance. LayerV has been externally audited and certified to ISO27001 and have successfully achieved AWS Manage Service Provider competency.

Design & Build

LayerV worked closely with the in the house architecture and infrastructure teams to produce a high-level design (example below) from the business conceptual architecture.



High Availability

All components were active/active wherever possible, and distributed between Amazon Availability Zones. The high availability requirement meant an individual component failure would not cause a DR event although the DR process was designed to be fully automated.

Performance

Performance was improved through CDN, caching and static content redirection for the client and internal operation team web application.

The compute engine was put into an auto scaling group, with health checks at the hardware and operating system level. In the event of a site or device failure, a new instance would be started.

Cloud Automation

The client had a range of test environments to perform integration, performance, user, member and regulatory risk model validation.
The LayerV automated deployment mitigated most of the additional complexity by improving the speed and quality of software delivery. A process orchestration system was used to take code from the code repository, compile it and place it to a central repository, then to manage the deployment to each environment tier (including environment specific configuration). LayerV worked directly with the 3rd party development agency to transform them to better working practices and the ability to take advantage of automated deployment. This covered items such as source control, branch strategies and configuration management.

Certification ISO 27001 & Regulatory Compliance

LayerV worked together with the client and a security management partner on creation of a ISMS (Information Security Management System) to support both ISO27001 and meet FCA requirements. Working as a combined team, the ISMS was created, enforced and externally audited for ISO27001 certification within 4 months.

Continuous Compliance

Their clients operate in a highly regulated industry so security was critical for all aspects of the design and build. LayerV deployed the Continuous Compliance platform to provide comprehensive security systems, monitoring and processes across the environment. This was central to the achievement of ISO27001 and FCA approval.

The Continuous Compliance tool set is deigned to counteract multiple threats:

- Malicious penetration attack – a traditional direct or phishing attack
- Malicious internal attack (abuse of rights) – elevation of rights
- Accidental misconfiguration – policy non-compliance

Continuous Compliance Offers:

- Audited and dynamically managed Access Control (separation of duty and auditing)
- Managed Encryption Services
- Comprehensive monitoring for Cloud, Hypervisor, OS, Application and Service
- Real-time dynamic CMDB of Cloud inventory
- SIEM (Security Incident and Event Management)
- Managed Anti-malware
- Managed Intrusion Prevention
- Vulnerability Scanning
- Continuous Penetration Testing
- Patch Management
- Password Management