AUJAS CYBERSECURITY

NSE NSEIT

CASE STUDY – THREAT MANAGEMENT SERVICES

ISMS Framework Evaluation and Assessment of Existing Security Posture for a Large Bank

CHALLENGE

The bank has a sizeable presence with offices around the world offering services such as retail banking, commercial banking, treasury services, and home finances to a customer base of over 2 million.

To meet the growing security challenges and comply with PCI DSS and local regulatory requirements, the bank implemented an integrated ISMS framework comprising of appropriate policies, processes, and procedures with technology controls and governance. They also had established a modern security infrastructure and technology and a 24/7 network and security operations center. Now, they wanted to implement perimeter security controls for network segregation, IP and port filtering, content management, gateway antivirus, intrusion detection and prevention systems.

The following were the project requirements:

- Evaluate current information security posture and effectiveness of implemented controls
- Identify security vulnerabilities, address people, processes, and technology issues across regions.
- Ensure business users understand the criticality of having a business continuity plan and preparedness required to handle a breach.
- Evaluate the effectiveness of existing ISMS framework.
- Assess implemented controls and recognize existing security risks against regulatory and PCI requirements, with ISO 27001 as the baseline.

SOLUTION APPROACH

1. ENGAGEMENT PLANNING

- Kick-off & planning meeting
- Plan development & finalization
- Stakeholder identification
- Deliverables finalization
- Logistics planning

2. SECURITY POSTURE ASSESSMENT

- Interview the stakeholders
- Review processes & supporting documentation
- Conduct risk assessment on application and underlying infrastructure
- Perform technical assessment to assess tech controls
- Asses user awareness

3. BCP/DRP ASSESSMENT

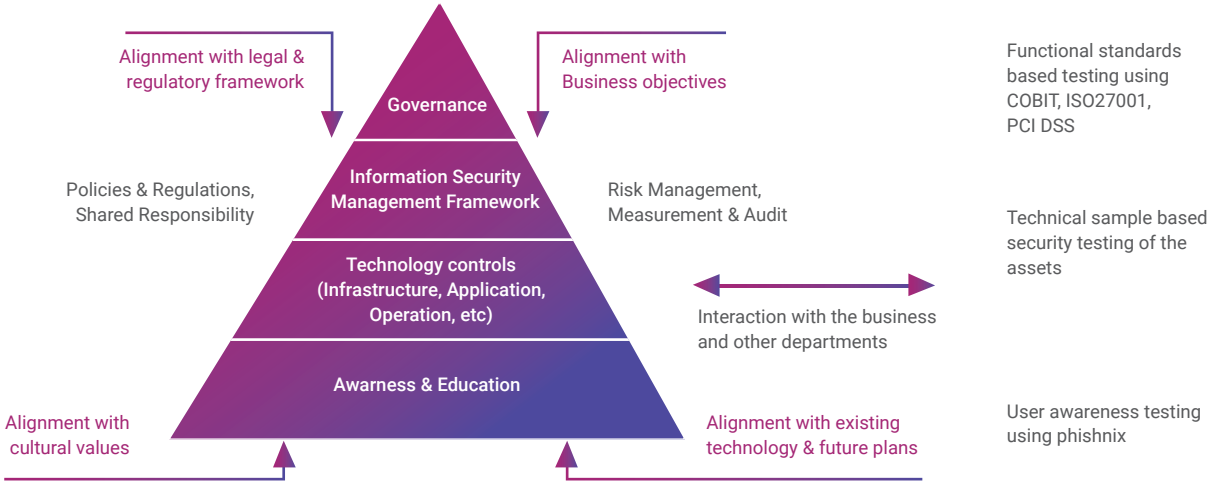
- Review the BCP/DRP plans & governance
- Review testing models & roles/ responsibilities
- Review documentation & build assessment matrix
- Observe BCP/DRP
- Identify potential gaps & improvement areas

4. CLOSURE

- Review the reports with customer
- Finalize the reports
- Conduct workshop for all business and technical stakeholders
- Present the overall findings to IS leadership
- Signoff

Aujas threat management experts used a top-down approach to assess functional risks on governance and information security management systems. The technology risk assessments included network architecture security assessment, penetration testing, vulnerability assessments, and configuration reviews for core IT networks, systems and applications.

Phishnix, an innovative phishing diagnostic solution from Aujas was leveraged to assess the level of user awareness within organization against social engineering attacks. Aujas also participated in BCP/DRP testing as observers and validated the functioning of the BCP/DRP team and their readiness in the event of a breach.



Top-down risk assessment approach

BENEFITS

Identified security weakness and vulnerabilities in people, process, and technology assets across regions.

Articulated and documented effective security controls to leverage identified strengths.

Recommendations for improved security posture by addressing security vulnerabilities and implementing enhanced controls.

Security and compliance trackers a`long with reports for regulators to enable due diligence.

ABOUT AUJAS

Aujas cybersecurity is an enterprise security service provider for organizations across North America, Asia Pacific, and EMEA regions. Aujas has deep expertise and capabilities in Identity and Access Management, Risk Advisory, Security Verification, Security Engineering & Managed Detection and Response services. By leveraging innovative products and services, Aujas helps businesses build and transform security postures to mitigate risks. The service focus is to strengthen security resilience by minimizing the occurrence of sophisticated attacks and threats while offering 360-degree visibility and protection across enterprise infrastructure.

For more information, do visit us at www.aujas.com or you can also write to us at contact@aujas.com