

CASE STUDY – RISK ADVISORY SERVICES

Security Program Evaluation for a Multinational Commercial Bank to Meet Compliance Needs

CHALLENGE

The bank had a global presence with an extensive network of branches, ATMs, and remittance centers. Over the past three decades, the bank has expanded aggressively and provided a full range of banking products and services to retail and corporate customers.

An increase in targeted attacks against organizations across the globe resulted in regulatory authorities mandating all banks to submit a report on the effectiveness of respective information security programs. The authorities stipulated minimum requirements for evaluation and had set strict timelines for submission. The bank management got committed to become the first to demonstrate compliance.

The bank relied heavily on technology and had layers of infrastructure, systems, and applications, both new and old, posing a big challenge for the evaluation of controls and measuring their effectiveness.

The challenges include:

- **Comprehensive Assessment of Information Security Program:** Assessment to span all areas of the client information security program and control framework ranging from governance to operations.
- **Assessment to be Completed in 60 Days:** Involve stakeholders to identify critical data, and its sensitivity, location, storage, forms, and how it is moved within and outside the organizational perimeter and complete assessment in 60 days.
- **Requirements Spanned Across Business Functions:** Ensure users across business functions understood the criticality of safeguarding information so that data leaks can be tackled at source.
- **Assessment had to Cover Across Geographies:** Bank's global presence added to the complexity of completing the assessment within the stipulated time.

SOLUTION APPROACH

The engagement was delivered in three different phases: Planning, Effectiveness Evaluation, and Report Creation.

Planning

- Requirements interpreted and illustrated to the client for common understanding.
- Timeline for delivering the report was agreed upon considering the dependencies.
- Applications and systems to be evaluated were finalized by identifying the stakeholders.
- Detailed project plan was created with the appropriate toll gates.

Effectiveness Evaluation

- Explain assessment objectives to stakeholders and provide them the inputs required from respective business functions.
- Establish a centralized PMO to collect, track, and support individual project teams.
- Follow-up discussions with stakeholders, escalate and manage any project deviations.

Report Creation

- Create Requirement Response Report to include observations, conclusions, and recommendations.
- Provide the client the opportunity to confirm and validate facts before the final version is published and submitted.

KEY PROJECT ACHIEVEMENTS



Business continuity and disaster recovery plan for the entire bank across geographies and business functions successfully tested.



Incident management processes tested by simulating various real-time scenarios.



Recommendations for information security strategy, objectives, and tactical plans provided.



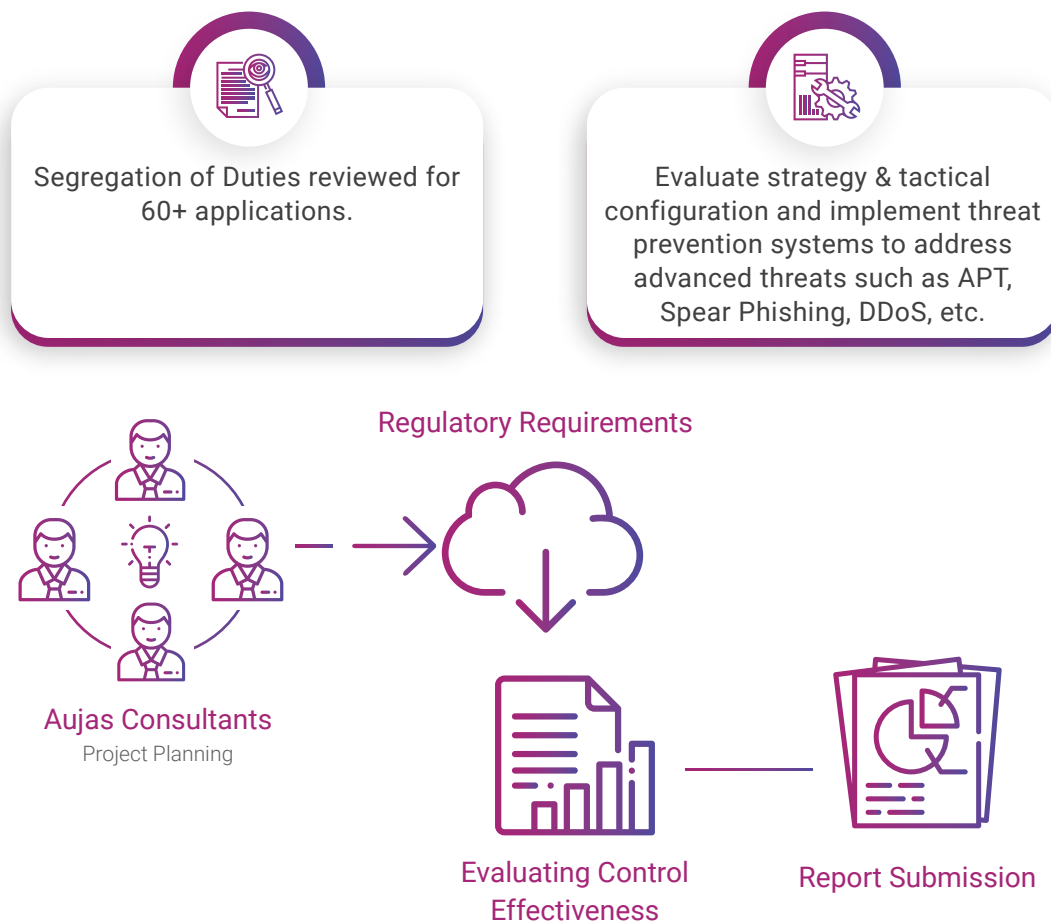
Risk Assessment for 60+ business applications, their platforms, interfaces, and infrastructure (300+ servers) conducted.



Vulnerability assessment and penetration testing performed on IP infrastructure.



Security Operations Center and Network Operation Center process evaluated for effectiveness.



CLIENT BENEFITS

- Gained a comprehensive view of security controls across business functions.
- Provide compliance reports to the regulatory authority within the stipulated timeline.

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 & Management, 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

