Case Study on
Virtual chief Information security officer (vCISO)

A snapshot of what we can do for you

Case Study – VCISO

Background

- Client is one of the leading businesses in the cloud telephony services.
- The Client provides cloud-based customer service and sales call handling solutions to businesses in Southeast Asia, South Asia, and the Middle East.
- Client engaged our consultants for GDPR and ISO 27001 consultancy & implementation support services
- GDPR and ISO 27001 implementation was crucial given the nature of business to manage the privacy of the PII of the employees and customers

Objectives

- Strategize, plan and execute security strategy (customed RoadMap) that aligns with the business goals
- Communicate to the management on various latest information security threats and advice possible solutions for the same.
- Establish an Incident Management and Breach response procedure and educate the employees accordingly
- Conduct periodic Internal audit's and suggest the Corrective and preventive actions accordingly.
- Periodically assess the risk related to organization as well as third parties as well as within the organization.
- Delivering awareness and trainings to employees and other staff members regarding information security best practices and industry trends.

Challenges

- Organization lacks the appropriate resources, skills and knowledge required for implementation of GDPR and ISO 27001
- Departments were not aware of their responsibilities regarding information security and privacy.
- New joiners and existing employees were not made aware about their responsibilities regarding information security and privacy
- Organization was not aware of the solutions which were to be implemented for avoiding the cyber threats.
- Risk associated with the third parties were not being monitored by the organization.

Industry Sector

Telecom	✔

Services utilized

Vendor risk assessments	✔
GDPR and ISO 27001 implementation	✔

Business Areas addressed

IT & Technology	✔
Legal	✔
Accounts	✔
Support	✔

Case Study – VCISO

Our Role

- Vendor Risk Assessment Support
- Customer Onboarding Support (Cyber Security & Compliances)
- Cyber Security Risk Assessment Exercises
- Conducting Phishing Simulation Exercises
- DR Drills
- Conducting Training and Awareness for all employees and staff members regarding best practices
- Determine Proper Security Frameworks
- Establish Strategy and Implementation of Information Security
- Review and Change Current Internal Security Controls
- Serve as an Industry expert (HIPAA, PCI-DSS, NIST, ISO 27001, various standards, and compliances)
- Facilitate the integration of security into business strategy, process & culture

Results / Benefits

- Remediation actions were defined and implemented for the issues identified during information security and privacy audits.
- Information security and Privacy awareness and training sessions were periodically conducted for the existing employees and also implemented during the on-boarding of employees which helped in reducing the privacy breaches and increased the know-how of handling private data of the customers and employees.
- Organization was able to comply with their Information security and privacy legal and statutory requirements.
- A well-defined Incident Management and Breach response procedure was established and implemented within the organization.
- Policies and procedures were implemented to monitor the risks associated with the third parties.
- Organization was able to cater to the information security and privacy requirements of their clients and, hence increasing the business growth of the organization.

Industry Sector

Telecom	✔

Services utilized

Vendor risk assessments	✔
GDPR and ISO 27001 implementation	✔

Business Areas addressed

IT & Technology	✔
Legal	✔
Accounts	✔
Support	✔