Rolling out of an Information Security Management System

Background

Our client, one among the top three private insurers in India, is a union between one of the largest global insurance groups and a financial institution controlled by a leading auto maker in India.

Our client had made major investments in its IT Infrastructure to support its life insurance operations and was concerned about the security and privacy of their customer data. Our client also had a heavy dependency on third parties service providers and vendors for IT support.

The primary objective for the client was to implement ISO 27001 at its Data Centre operations in Pune and slowly roll out the security management system to cover zonal offices and regional offices across India. The following IT functions were in scope for the ISMS Certification:

1. IT infrastructure management
2. Data centre Management
3. Database Administration
4. Data warehouse Management
5. Application development & maintenance
6. Quality Assurance

The client engaged MIEL e-security consultants to implement ISO 27001 based management system and subsequently build an information security roadmap to extend its ISMS certification scope to cover larger part of their organization.

MIEL's Approach

MIEL e-Security provides individually customized solutions to each of its client, keeping an eye on both the security objectives and the overall business goals. For every new assignment, the Project Management Team studies the processes of the new client in micro-detail. Meticulous planning by our highly qualified project managers ensures that the client is informed on each milestones and its deliverables before the commencement of the project.

Data Security Measures at the Central Data Centre

As the Data Centre is the core that hosts the entire business critical infrastructure for our client hence it was of paramount importance for them to ensure that IT Operational processes and the supporting infrastructure were adequately protected from known risks.

MIEL carried out a series of technical and process based audits for the client. The findings from our audit were quickly translated into realistic and practically implementable guides to improve the security posture.

IT Security Health Check

All workstations at the Data Centre and IT Operations floor underwent an IT Security Health Check whereby they were scanned for vulnerabilities using best-of-breed scanners. Any vulnerability that was found was promptly fixed by their IT team.

The network infrastructure at the Data centre level like routers, switches, firewalls underwent non-intrusive penetration testing to find out the possibilities of external threats that have the capability of materializing. Any such findings were promptly fixed and monitored on an ongoing basis.

Based on MIEL recommendations, firewalls at the Data Centre were configured with strict access control rules which allowed outbound traffic as per business requirements blocking all other traffic like messengers, web mails, and other internet browsing.

ISO 27001 Compliance

As such our clients wished to ensure that the processes at the Data Centre adhere to the ISO 27001 standard thereby re-assuring that the various customer and business data was adequately protected. Following broad activities were carried out as part of ISO 27001 compliance at the Data Centre and IT Operations:

- Risk Assessment & Risk treatment of business process and associated assets
- Mitigation of risk based on risk analysis
- Training of end-users to make them aware about information security risks
- Physical security review
- Implementation of ISO 27001 controls using technology
- Development of Information security policies and procedures
- Management awareness and end user training on periodic basis
- Incident reporting & management
- Change control management
- Compliance audits

Change management procedures were followed to keep track of any changes that are made either in the applications used or in the IT infrastructure at the data centre. Incident management procedures are followed to keep track of incidents that happen or are likely to happen. A process was institutionalised to learn from incidents and take measures to put controls in place which will ensure that incidents are not repeated.

Data Security Measures at Data Centre

Some of the key proactive measures implemented by MIEL onsite included:

- The servers were adequately protected by firewalls deploying latest technologies of gateway anti-virus, Intrusion Prevention Systems (IPS) and a stringent access control list which is managed only by the client IT team.

- Implementing an effective purging policy which deletes the data after a specific period of time as per client requirements.

- To ensure that the client's web servers & database servers were adequately protected from external as well as internal threats, an internal vulnerability assessment and an external penetration testing was carried out from a hacker's perspective. The recommendations made from these tests were implemented by the IT Infrastructure & Applications teams respectively.

- Additionally, the website was tested using the black box testing approach to find out any vulnerability in the application which could potentially be exploited. The recommendation of the black box testing were implemented by the application team and was re-tested to make sure that vulnerabilities were effectively closed.

- The websites which were used to collect data had deployed strong encryption mechanism like SSL to make sure that data in transit was protected.

Following activities were done proactively to ensure security of servers:

- **Vulnerability assessment:** A detailed vulnerability assessment of servers hosted at Data Centre was carried and a report was submitted to client IT team.

- **Setting up of policies and procedures for patching, monitoring and back-up of the servers.**

- **Physical Security at the Data Center:**
    - Enforcement of stringent physical security measures
    - Hosting of servers in secure areas with a biometric system access control. This area and all other areas in the CDC are continuously monitored via CCTV.
    - The area where the servers are hosted is adequately protected by fire protection systems and has adequate back-up of power supplies.

Project Management

The primary challenge of managing the project was to achieve all of the project goals and objectives while adhering to classic project constraints (scope, quality, time and budget). The secondary—and more ambitious—challenge is to optimize the allocation and integration of inputs necessary to meet pre-defined objectives.

The client was provided with a carefully defined and detailed set of activities, along with the deployment plans for various resources to achieve the project goals and objectives. MIEL worked closely with the client to overcome several logistical challenges to complete the project well before time.

Templates and plans were compiled as a part of this approach to be used consistently across all IT operational departments. These templates were in line with the business requirements of the unit, requirements of the organization and also requirements of ISO27001.

An independent audit ensured that the ISMS were in line with the requirements of ISO27001, the organization and rules and regulations of India.

This project was completed in **20 weeks**, with the deployment of **2 consultants**.

ISO 27001 Certification Maintenance

Upon achieving certification, the client wanted to avail of MIEL's expertise in ensuring that the appropriate processes were being followed consistently and the information security posture demonstrated a continual improvement. To meet the client requirement, MIEL deployed experienced consultants to the client site on a full time basis to drive the information security program.

This consultant is responsible for the following activities:

1. Maintenance and monitoring of user accounts / logins / passwords and access permissions for all the mentioned systems in the scope.
2. Monitoring and maintenance to be done on regular basis and any deviation to the policy to be brought to the notice of the client officials. Subsequently corrective steps or suggestion to be made to the client officials to comply with the security policy.
3. Maintaining records (user accounts/ privileges/ access to various systems) and submission of periodic reports and recommendations on the same to the client.
4. Development of measures for improvement in system security policies and procedures at the client site.
5. Submission of Compliance report with reference to IS Policies & procedures and IS Security Policies & procedures on the periodic basis.
6. Regularly review various records relating to user accounts/ privileges/ access to various systems and submit periodic report and suggestions on the same to the client.
7. Review, evaluation and monitoring of SLAs.
8. Alignment of information security policies, standards, procedure and guidelines with business objectives.
9. Incident management including incident identification, containment, handling and escalation process.
10. Training to the Implementation team on modification and updating of policies and procedures as and when required.
11. Security awareness training for new employees
12. Handholding the client during their surveillance audit for ISO 27001 by external auditor.
13. Review and Amendment to Asset Register, Risk Assessment and Risk mitigation
14. Half Yearly ISMS Audit

Conclusion

MIEL has ensured the all its project milestones were met in both a timely fashion, along with the maximum client satisfaction.

Our client has now based its confidence in MIEL services and have entrusted the maintenance of its ISMS certification to MIEL.