Rolling out of an Information Security Management System on a global scale

Background

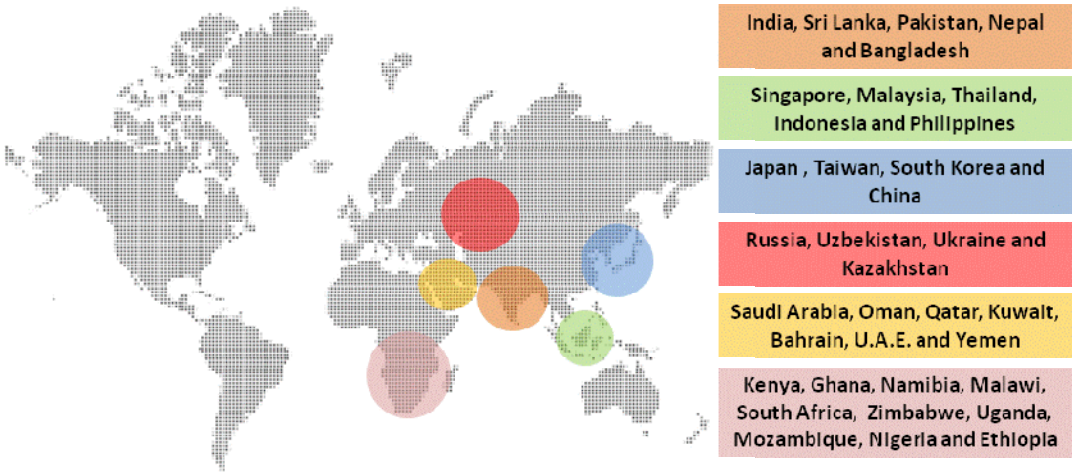
Part of a Zurich based global travel group, our client was established in 2001 in India, as a specialist partner for diplomatic missions worldwide. Serving diplomatic missions by managing all the administrative and non-judgmental tasks related to the entire lifecycle of a visa application process, our client enables diplomatic missions to focus entirely on the key tasks of assessment and interview.

Our client's business depends entirely on the trust diplomatic missions place in them. As a rule, all their business dealings are conducted strictly as per the code of ethics laid down by the respective governments.

Our client has made major investments in software development in order to handle large volumes of applications, including proprietary software systems for passport tracking, database creation and data upload. They have entered into several technical and support agreements with leading IT hardware and software giants to ensure compliance to security policies and also adhere to meeting the stringent norms of diplomatic missions on IT Security and Data Protection.

The primary objective for the client was to certify its head office and Data Centre in Mumbai. Understanding the criticality of information being handled, it became necessary for the client to roll out the organizational information security best practices to its units spread across 75 locations in 35 countries.

Our client engaged with MIEL e-security to carry out health checks and internal reviews on various systems and procedures so as to ensure robustness and continuous monitoring of their commitment to agreed customer service levels. The client provided MIEL the mandate to ensure its security policies, procedures and their implementation on the ground was consistent with their global initiatives as well as industry standards such as ISO 27001.



MIEL's Approach

MIEL e-Security provides individually customized solutions to each of its client, keeping a key 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 Visa Application Centres (VACs)

As the VACs are the core of the business for our clients hence it is of paramount importance for them to ensure that business process and the supporting infrastructure are 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 at each and every VAC.

IT Security Health Check

All workstation at the VACs 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 VAC 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 are monitored on an ongoing basis.

Firewalls at the VAC level 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.

Workstations at the VACs are protected using Symantec End-Point Security solution. Using this product the users are given limited access to the workstation depending on their job role.

Altiris (a security protection suite from Symantec) is used for Patch Management of workstations to ensure that OS level patches are always in an updated state.

ISO 27001 Compliance

ISO 27001 has been accepted as a global standard towards protection of information. As such our clients wished to ensure that the processes at the VAC adhere to the ISO 27001 standard thereby re-assuring the various government data was adequately protected. Following broad activities are carried out as part of ISO 27001 compliance at the VAC level:

- 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
- Management awareness
- Incident reporting & management
- Change control management
- Compliance audits

Change management procedures are followed to keep track of any changes that are made either in the applications used or in the IT infrastructure at the data centre and the VAC. Incident management procedures are followed to keep track of incidents that happen or are likely to happen. A process is in place 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

All data collected by the Visa Application Centre (VACs) is stored at the CDC (Central Data Centre). The client wished to have the CDC facilities certified for ISO 27001 and enforce stringent physical security checks.

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 is re-tested to make sure that vulnerabilities were effectively closed.

- The websites which are used to collect data employ strong encryption mechanism like SSL to make sure that data in transit is protected.

- Deployment of Symantec Critical Server Protection to protect the servers from external threats like Cross-Site scripting attacks, SQL injection attacks, malicious code execution etc. This product further enhances the security architecture of the servers in addition to the IPS mentioned above.

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 a project on a global scale is 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.

The activity of roll-out began with an in-depth understanding of the business of the global units. This included a comprehensive study of business at a unit based out of Mumbai. An ISMS was framed for the unit based on the requirements and ISMS of head office.

The framing of this ISMS was then moulded into an approach that would then be used to document and implement an ISMS across all global units.

Templates and plans were compiled as a part of this approach to be used at all global units. These templates were in line with the business requirements of the unit, requirements of the organization and also requirements of ISO27001.

Consultants then travelled across all locations to customize the templates and implementation as per local requirements of that country. Additionally, the consultants also carried out a vulnerability assessment of critical systems at the units.

An independent audit at each location ensured that the ISMS was in line with the requirements of ISO27001, the organization and rules and regulations of that country.

This project was completed in **25 weeks**, with the deployment of over **30 consultants**.

Conclusion

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

Our client has now gone ahead and got its head quarters certified for ISO 27001. The joint effort between our client and MIEL ensured that the client was recommended for certification immediately after the audit by the certification body!

Furthermore, the security standards in their VAC's globally is now at a premium baseline, ensuring optimum security for their data. The government missions that the client deals with have also expressed their satisfaction at the standard of security at all locations.