

Case Study

Information Security Management System (ISMS) based on ISO/IEC 27001:2005 for Rajiv Gandhi University of Health Sciences

Client

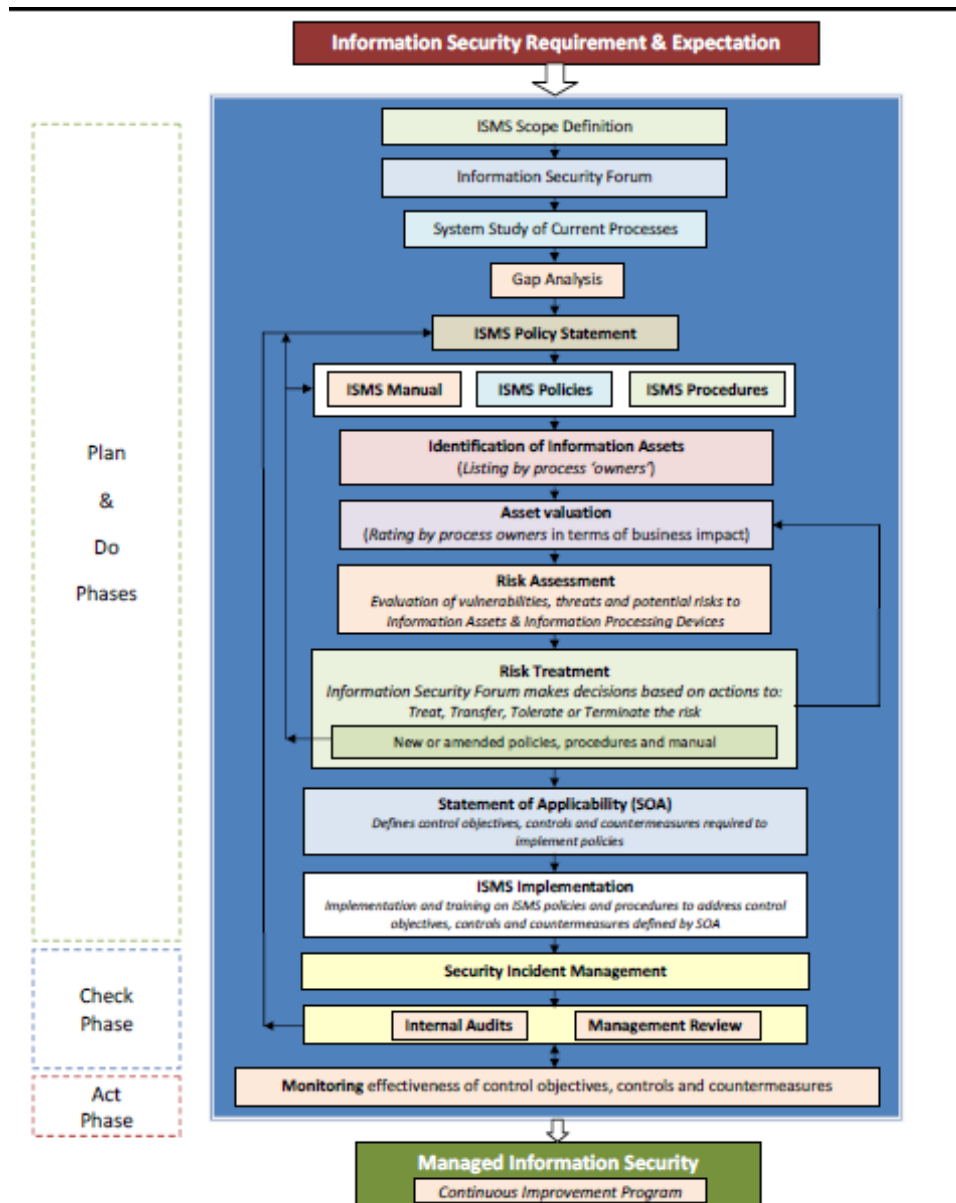
Rajiv Gandhi University of Health Sciences (RGUHS), centered in Bangalore, India, is a unitary university set up in 1996 by the government of Karnataka, India, for the regulation and promotion of higher education in health sciences throughout the state of Karnataka.

The establishment of the university was directed by the Rajiv Gandhi University of Health Sciences Act of 1994. About 276 colleges throughout the state, affiliated with different universities, that were conducting courses related to Medicine, Dentistry, Physiotherapy, Pharmacy and Nursing were placed under the Rajiv Gandhi University in order to establish uniform standards in academics and administration. The university is named after former Prime Minister of India, Mr. Rajiv Gandhi. Originally it was centered in Mysore, but in 1998 the Karnataka State Legislature directed that it be moved to Bangalore. The University runs a course on Health Librarianship

Project

The management team at the Rajiv Gandhi University of Health Sciences (RGUHS), and their Systems and Process team have decided to go for an Information Security Management System (ISMS) for the IT organization. Backend Bangalore Pvt. Ltd. as consultants assisted in establishing, implementing, operating, monitoring, reviewing, maintaining and improving the protection of information assets to achieve business objectives based upon a risk assessment and the organization's risk acceptance levels designed to effectively treat and manage risks.

ISMS Process Flow



Project Team

The project was handled by Dr.S.Ramananda Shetty as Vice Chancellor, Dr. Vasantha Kumar.S as Registrar, Dr S Sacchidanand as Registrar (Evaluation) and B.S. Sreenivasamurthy, Dr. M. Chandrashekar as Deputy Registrar.

Challenges in managing the project

The primary challenge of managing an ISMS project is to achieve all of the project goals and objectives while adhering to classic project constraints (scope, security, 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.

Other challenges include

- Balancing the need for accessibility and the Preservation of “C-I-A”
- Comprehensive databases requires clearly defined security responsibilities that establish accountability
- Key Performance Indicator (KPI) for the organization

RGUHS identified that these issues would only escalate as the project ramped up.

Solution

Backend Bangalore Pvt. Ltd, worked with RGUHS and built an Information Security Management System (ISMS) at RGUHS, Bangalore, based on the requirements laid down in ISO/IEC 27001 comprising of set of policies concerned with information security management.

Top-to-Bottom Approach

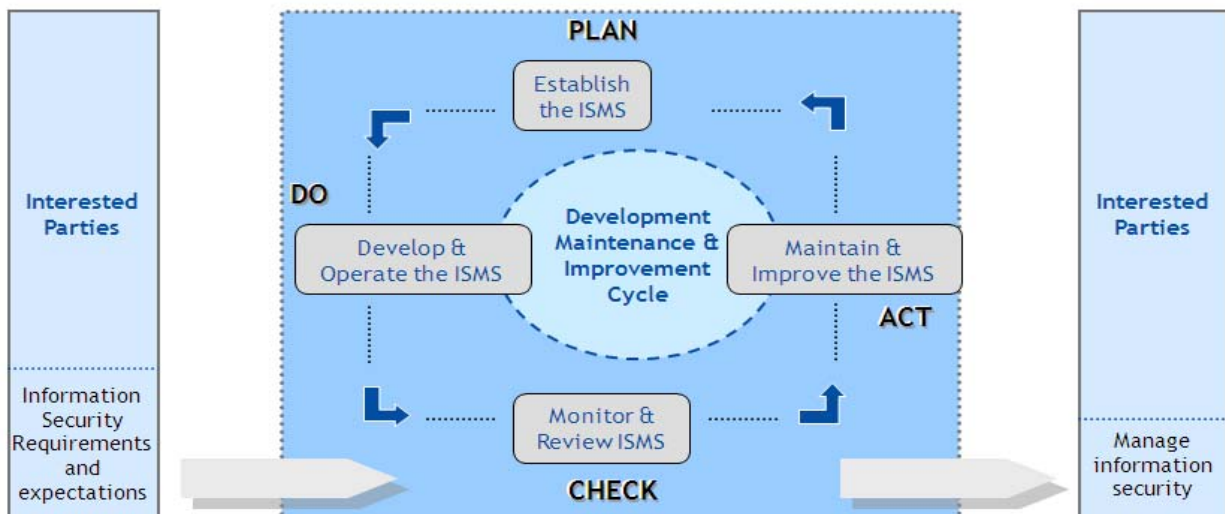
The top-to-bottom approach followed by ISO 27001 helps top management to provide necessary support and direction, which is cascaded down through middle-level management and then to staff members.

As with all management processes, an ISMS must remain effective and efficient in the long term, adapting to changes in the internal organization and external environment. ISO/IEC 27001 therefore incorporates the typical "Plan-Do-Check-Act", or Deming cycle, approach:

- The Plan phase is about designing the ISMS, assessing information security risks and selecting appropriate controls.
- The Do phase involves implementing and operating the controls.

- The Check phase objective is to review and evaluate the performance (efficiency and effectiveness) of the ISMS.
- In the Act phase, changes are made where necessary to bring the ISMS back to peak performance.

:Information Security Standard: ISO/IEC 27001:2005 - PDCA Model applied to ISMS Processes



Results

As a result of Implementing ISMS, RGUHS was able to derive promised deliverables in various fields. Some of the key highlights are listed below.

- Development of a comprehensive & verifiable information security management strategy
- Organizational infrastructure & related data protection activities are addressed
- Information Security effectively transformed into a proactive activity
- Ensure compliance to existing and future information infrastructure-related regulations
- Information security framework aligned with business objectives
- Alignment with leading industry practices and methods
- ISMS driven by RGUHS information strategy

Implementation and Training

Backend Bangalore Pvt. Ltd. had implemented and trained the RGUHS staff with ISMS Awareness and training program, Security awareness training, Lead and internal auditor training and 5 day audit training. To ensure that project members are adept at using the system, Backend Bangalore Pvt Ltd ran customized training modules for all participants.