7799 Goes Global

ISMS International User Group

London 30 November 2004

Sanjay B. Lollbeharree (Mauritius)

"The Government of Mauritius intends to rollout ISO/IEC 17799 across the whole Civil Service with the visible sign of success being judged through certification of each ISMS against BS7799-2. The presentation will explain how we are doing this and our progress so far. One early win, amongst others, of the approach we are taking is empowering senior public officers to decide for themselves what information security they need to support their business objectives; a capability that did not exist before the project started. The phase of the project which covered deployment of the standards within four pilot sites was achieved in less than four months, from a standing start."

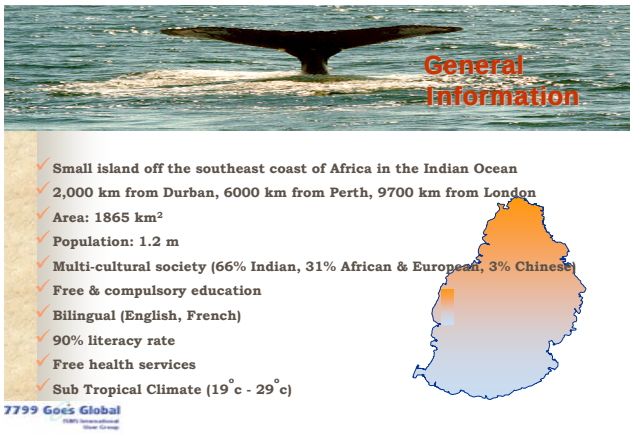
Mr. Sanjay B. Lollbeharree started his career in ICT in 1991, specialising in systems analysis, design and development and has worked for a number of private sector entities in Mauritius and abroad. In 1994, he joined the Mauritian Civil Service as Project Manager at the Central Informatics Bureau within the Ministry of Information Technology & Telecommunications where he has been involved in the implementation of a wide variety of computerisation projects in Government. This experience has allowed Sanjay to develop extensive ICT project management skills. In 2001, Sanjay was appointed Deputy Director of the Central Informatics Bureau. His responsibility scaled from managing individual projects to embrace planning and managing the overall Civil Service computerisation programme. He has been closely linked to a number of e-government initiatives including the elaboration of an e-government master plan, setting up of a Government Online Centre to house the government portal and the establishment of a government intranet system for interconnecting the various Ministries and Departments into a single secure network. He has also been instrumental in the implementation of ISO/IEC 17799 security standards in the Civil Service in Mauritius. Mr. Lollbeharree is a holder of a Master of Technology in Computer Engineering and a Master of Business Administration and he is presently reading for a PhD in the area of e-Government.

Slide 1 - Title

Slide 2 - General Information

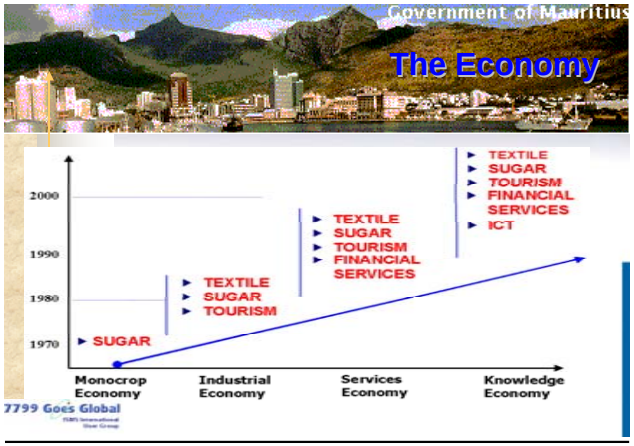
Mauritius is a small island of an area of around 2000 km to the south east coast of Africa. Its population of around 1.2 million forms a mosaic of different races, cultures and religions. Most Mauritians are bilingual, being equally fluent in English and French.

Eleven year schooling is compulsory and education is free up to the tertiary level.



Slide 3 - The Economy

Over the past three decades, the Mauritian economy has continuously reengineered itself from a mono crop economy dependent essentially on sugar into a more diversified structure comprising sugar, textile, tourism and financial services. Preferential market access for sugar and textile products to the EU has helped these two sectors to develop at a healthy rate. However, with the forthcoming dismantling of trade preference and likelihood of drop in price of sugar on the EU market, the sugar and textile sectors are facing major challenges and might run out of steam.



Slide 4 - ICT Vision

Government is placing high hope and investing a lot in the ICT sector to strengthen the economy. High priority is being accorded to developing the ICT sector into the fifth pillar of the economy to generate revenue and create employment.

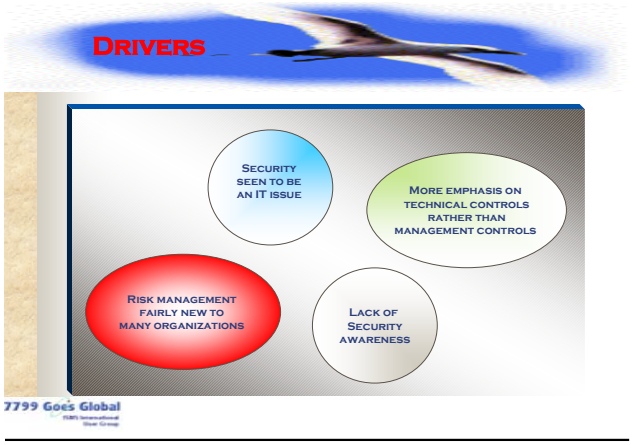
ICT is seen to be the engine of growth which would allow Mauritius to leapfrog into the first division of nations.

Slide 5 – e-government (Critical Success Factors)

E-government is one of the building blocks which would pave our way towards realising our ICT vision. E-government is the application of ICT to improve the efficiency, effectiveness, transparency and accountability of governments. E-government is a major undertaking. One of the prerequisites is the development of a security culture. Successful e-government must build trust between government and businesses and citizens. Besides enacting appropriate cyber legislation, Government must deploy necessary infrastructure and standards to protect information from attack and misuse.

There is need to develop a structured approach against threats posed by viruses/hackers, employee fraud, computer abuse, disasters and other dangers.

Slide 6 – Drivers



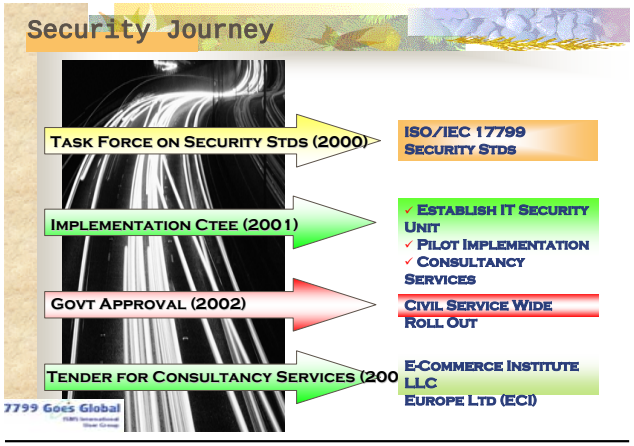
Adoption of an internationally recognised information security standard is seen as one solution. In fact, several drivers have been creating a growing demand for such standards. Firstly, security was being wrongly perceived within several organisations as an IT issue when it is foremost a management concern. Research has shown that fraud or cases of IT abuse often occur due to the absence of basic controls, with a significant amount of all detected fraud found by accident. Poor supervision of staff and lack of proper authorization procedures are frequently mentioned as the main causes of security incidents. There was a lack of security awareness and focus was dominated by technical controls rather than management controls. Poor or lack of security awareness is a major threat. People are the weakest link in the security chain while technology can only help reduce risks to a certain point. Everyone has to understand that it is their personal responsibility to manage risks and assets. Furthermore, risk management and business continuity were fairly new to many organisations.

Slide 7 – Security Journey

The Government of Mauritius Security journey as far as implementation of ISO/IEC 17799 security standards is concerned started in year 2000 with the setting up of a task force on security. Government generates and manages a huge amount of information which has become an essential resource in our information society. Protecting such information has become a major challenge given the risks posed by rapid technological development and the widespread opening up of networks.

The task force on security had as mandate to scan through best practices and advise on the appropriate approach to address IT security within the Civil Service. The adoption of the ISO/IEC 17799 information security standards was the main recommendation of the task force.

In 2001, an implementation report was elaborated which proposed the setting up of an IT Security Unit within the Ministry of Information Technology & Telecommunications to mainly act as facilitator and internal auditor in the implementation of the security standards in Ministries and Departments. The implementation of the standards on a pilot basis and development of a methodology for roll-out with the assistance of security experts was also proposed. In 2002, the recommendations of the implementation committee were approved and the green light was also obtained for the eventual roll-out of the standards throughout the Civil Service. A tender exercise was launched and E-commerce Institute LLC Europe Ltd (ECI) was selected for providing consultancy services to the Government of Mauritius.

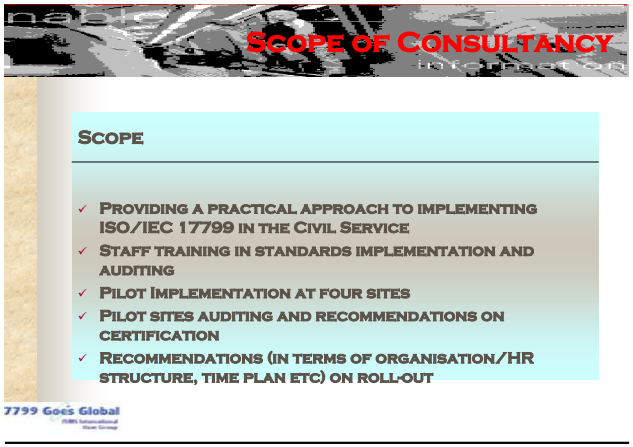


Slide 8 – Scope of Consultancy

The scope of the consultancy delivered by Dr. David Brewer and Mr William List from ECI covered the following –

- Provide a practical approach to implementing ISO/IEC 17799 in the Civil Service
- Train staff of the IT Security unit for assisting in the implementation of the standards, carrying out audits and in other areas deemed necessary
- Implement the standards in 4 pilot sites with the assistance of local staff
- Audit the pilot sites after the implementation of the standards and provide recommendations on certification

Recommend (in terms of organisation/HR structure, time plan etc) on how to proceed with the roll-out of the standards at other sites within the civil service.



Slide 9 – Approach

It was realised at the initiation of the project that in order to meet the Civil Service's intention to implement ISO/IEC 17799 to a standard capable of being certified it was necessary to use the mechanism of an information security management system (ISMS) as set out in BS 7799 Part 2.

The benefits of adopting an ISMS approach include helping businesses to

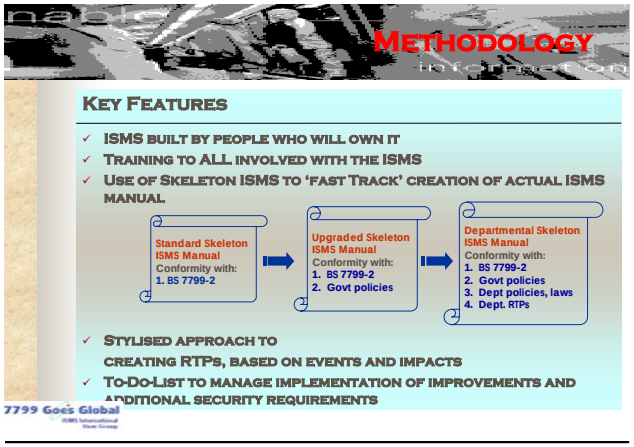
- implement effective information security that really meets business requirements
- manage risks to suit the business circumstances
- manage incident handling activities
- integrate information security into business life and develop a security culture.

BS 7799-2 has a set of mandatory requirements. These include maintaining a documented ISMS that records the information security policies and procedures of the organisation. These must be designed to address business security issues.

The creation of an information security forum (ISF) including senior management was mandated. Management is required to evidence their involvement in approving the original ISMS and its subsequent modification. It should ensure that internal audits are conducted and appropriate changes are made following any incident. Management is also required to see to it that the ISMS is improved over time and that adjustments are made to reflect changes in business activities and technology employed in the organisation.

Slide 10 – Methodology (key features)

The consultants devised a methodology for applying BS 7799-2 known as the Gamma-W^m List Methodology. The key features of the methodology are:



- **The ISMS is built by the people who will own it**. This approach ensures that the ISMS accurately addresses their business concerns and that they develop necessary skills to operate and maintain the ISMS.

- **Training is given to all people involved with the ISMS**. The training covers essentially ISMS administration and audit.

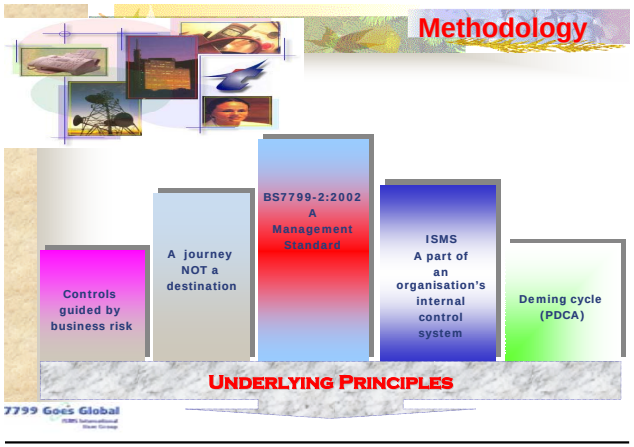
- **Use of a Skeleton ISMS Manual to 'fast track' the creation of the actual ISMS Manual**. Embedded within this Skeleton are all the mandatory requirements of BS 7799-2. It is a living electronic document, created using web technology. It can be linked to policy and procedures documents electronically. Each site needs to flesh out

the skeleton by personalising appropriate sections and taking into account central as well as departmental information security policies.

- **A stylised approach to creating RTPs based on events and impacts**. The methodology already includes certain standard events and this list has to be extended by adding others which are specific to the business processes of the organisation concerned. This approach ensures that the business needs of the organisation are not left out.
- **A To-Do-List is maintained to manage the implementation of desirable improvements and additional security features that may subsequently be identified.**

Slide 11 – Methodology (Underlying principles)

BS 7799 Part 2 tells an organisation how to build and maintain an ISMS. It has been developed as a management system standard to be in harmony with other ISO management system standards. It has been road-tested with regard to third party certification using the same process and standards as ISO 9001 and ISO 14000. It is that part of an organisation's internal control system that deals with the security of information & technology.



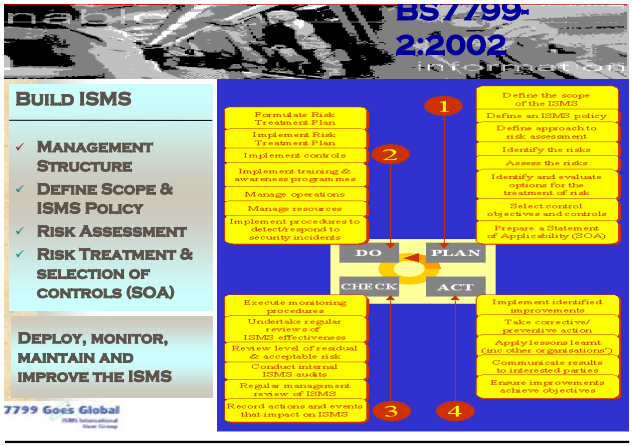
Based on the Deming "Plan-Do-Check-Act" cycle (i.e. plan what you want to do, do it, check that it is working, and take appropriate action if not), the ISMS is a living entity, allowing management to continually ensure the right level of security to meet their ever changing business needs, to anticipate and react to new threats and vulnerabilities, and take appropriate action when things go wrong.

The selection of information assurance controls is predominantly determined by risk assessment and this assessment must be performed in the context of meeting the organisation's business objectives.

Finally, an ISMS is a journey and not a destination. Actually, at any point in time, there may be corrective/preventive actions and improvements that are identified and have to be implemented. There may also be incidents that are in the process of being dealt with. It is the task of the internal control system and therefore the ISMS to manage these activities.

Slide 12 – BS 7799-2:2002 (Build ISMS)

The diagram illustrates the different steps involved in building and maintaining an ISMS based on the PDCA cycle.



Broadly speaking, there is need to establish an implementation structure with active involvement of top management. Management has a key role to play in the process of developing and operating the ISMS to ensure that risk assessments are carried out in the context of the business.

The next step is to clearly define the boundaries and policies of the ISMS following which the risk assessment starts. This is where events, which are qualified as bad things that cause trouble to the business, are identified. The damage or impact of each event is then characterised. The occurrence of an event may give rise to several impacts and may also trigger other events.

The elaboration of Risk Treatment Plans (RTP) then follows. RTP relates to the treatment

process of selection and implementation of measures to modify risk. This involves identifying the assets impacted by each event and listing the applicable threats. Risks leading to a particular impact are then identified and appropriate controls and measures are applied to address those risks.

As seen earlier, ISMS is a journey and not a destination. This implies that the ISMS needs to be maintained and improved over time to cater for evolving business needs.

Slide 13 – Pilot Implementation Framework

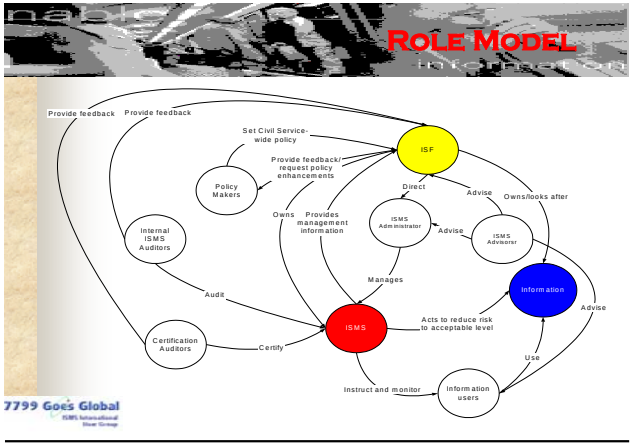
In order to closely monitor the pilot implementation of the security standards, a steering committee was set up under the coordination of the Ministry of Information Technology & Telecommunications to guide and oversee the project. The committee met regularly to review and approve deliverables submitted by consultants and made appropriate recommendations and suggestions.

The four pilot sites selected for the exercise were the Ministry of Social Security, the Passport & Immigration Office, the Civil Status Office and the Treasury Department. All these sites have to a large extent already computerized their activities.

Slide 14 – Role Model

A role model defining the responsibilities and interactions of all the actors (ISF, ISMS administrator, Internal ISMS Auditors, ISMS Adviser, Certification Auditor, Policy maker) involved with the ISMS was elaborated and applied to the different pilot sites.

The ISF is the highest authority within each site which approves policy and takes responsibility for accepting residual information assurance risk. It also ensures that Civil Service-wide policy set by policy makers is also taken on board. Without establishing an ISF, the exercise cannot take off as there is no approval forum. The ISMS Administrator is responsible for day-to-day running of ISMS while the ISMS advisor provides necessary advice for the implementation, administration and auditing of the ISMS. While Internal ISMS Auditors check conformance of ISMS and staff actions to ISMS policy, certification auditors carry out external audits for the sake of certification. Finally, information users who are generally staff and potentially the public consume the information.



In general, one actor may play several roles, for example, many people will play the role of information user, some of which may simultaneously play another role, such as ISMS Administrator. Conversely, several actors may play the same role.

Within each site an information security forum was established with the involvement of top management to develop and maintain an ISMS. The consultants along with the trained staff of the IT security Unit provided necessary advice and close guidance to each pilot site. The IT security unit staff subsequently also operated as internal auditors.

Slide 15 – Training

BS 7799-2 places demand on training and the need to appraise and record the effectiveness of the training. It places further demand on security awareness-training and competence.

Training was conducted in two parts namely an ISMS training course and an audit training course. The ISMS training was imparted to everyone involved in the four pilot sites and the eventual roll-out. The audit training was followed by the actors that played the roles of ISMS Advisor and Internal ISMS Auditor.

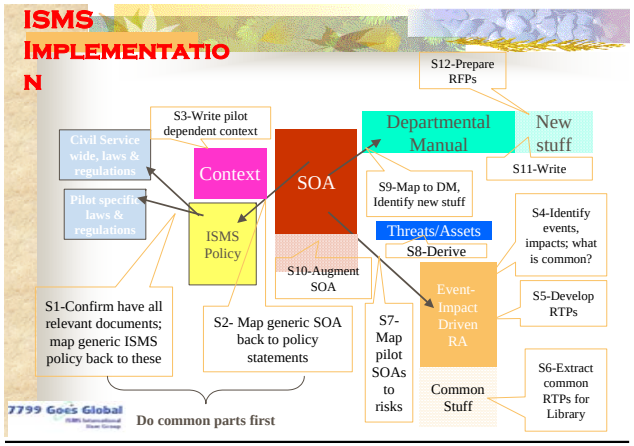
The training programme provided an appreciation of the standards ISO/IEC 17799:2000 and BS 7799-2:2002. It covered instruction and practice in the development of the ISMS Manual as a whole, and in the development of Risk Treatment Plans, technicalities of using the skeleton ISMS Manual to produce the Pilot's ISMS Manual and other elements that comprise an ISMS such as incident handling and Internal ISMS Auditing. It also addressed use of the ISMS by management with focus on review of those sections of the manual that require management approval, particularly the confirmation of the acceptability of residual risks, modifying the schedule of events, impacts and the results of the Risk Treatment Plans.

A brief explanation of a technique for using computer enquiry tools to detect anomalies in large volumes of data was also given to the internal ISMS auditors. These techniques, known in the audit world as Computer Assisted Audits Techniques (CAATs), are however not a requirement of BS 7799-2.

Slide 16 – ISMS Implementation (steps)

The various steps required for constructing the ISMS Manual for the pilot sites are shown diagrammatically. Certain tasks may be performed in parallel if more than one person are involved.

It is to be noted that a large volume of effort is spent on the development of the Risk Treatment Plans.



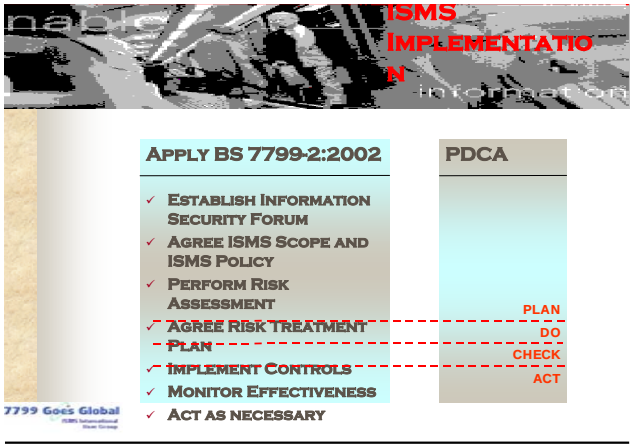
Slides 17 & 18 – ISMS Implementation (Apply BS 7799)

Each site followed the agreed methodology based on the PDCA cycle to develop their ISMS.

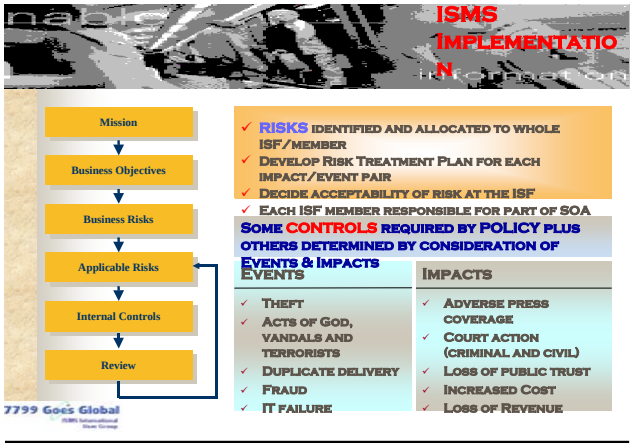
After having established their ISF with management involvement, each pilot site clearly defined the scope of their activities that would be covered by the ISMS. Given that ISMS implementation was a completely new initiative, the scope was carefully traced to keep the project with manageable limits and maximise chances of success.

The risk assessment then followed with the identification and analysis of events and impacts from which assets and threats were derived. Elaboration of RTP's along with application of appropriate controls were undertaken with the assistance of the IT security unit team and expert advice of the consultants.

The skeleton manual already featured a built-in near completed prototype ISMS policy that covered all the requirements of BS 7799-2. Furthermore, standard RTP's and ready-



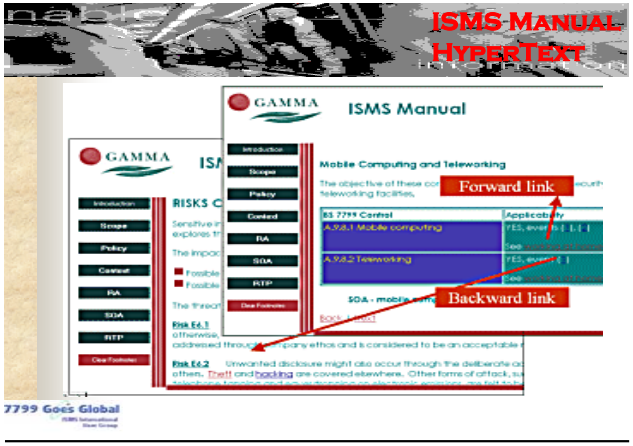
made event, impact, asset and threat lists were embedded in the skeleton. These lists were augmented by each site to reflect their respective specificities.



Slide 19 – ISMS Manual (Hypertext)

The construction of the ISMS manual was based on hypertext technology and FrontPage software which required familiarity with browser technology. The ISMS manual carries lots of cross-references which are efficiently handled by FrontPage. Web based technology also supports multiple windows, making it vastly superior to navigating a single electronic document.

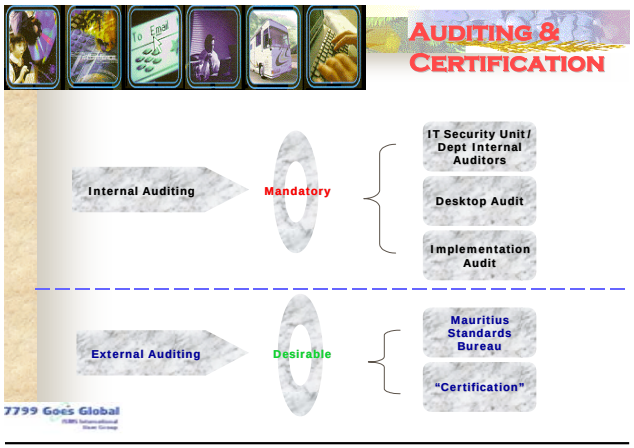
The choice of the hypertext technology as such rendered construction, navigation and maintenance of the ISMS manual relatively easy and user-friendly.



Slide 20 – Auditing & Certification

Internal auditing is a mandatory requirement of BS7799-2. It was performed in two stages. The first stage is the desktop audit whose purpose is to determine technical compliance of the ISMS documentation with BS 7799-2. Implementation audit is carried out in the second stage to discover whether the organisation practices what it preaches.

All the pilot sites were successfully audited by the IT security unit staff and certain departmental staff with the assistance of the consultants. No non-conformities were detected. Some observations were merely made. Audit reports were drafted and passed to the departmental management for any necessary action.



The logical step following internal auditing is certification. Certification of an ISMS gives an independent view of how effective the information security is, which in itself provides other benefits to stakeholders and customers. Management taking such a step is an indicator of the business being aware of the risks they face and being prepared to take action to manage these risks to protect their business. In the context of the Civil Service, certification is seen as the public demonstration that the Civil Service's policy of conformity to the standard has been implemented. In addition, it provides confidence to citizens that ministries have procedures in place to manage information security and to modify procedures as appropriate to address the evolution in the use of Information Technology in the Civil Service.

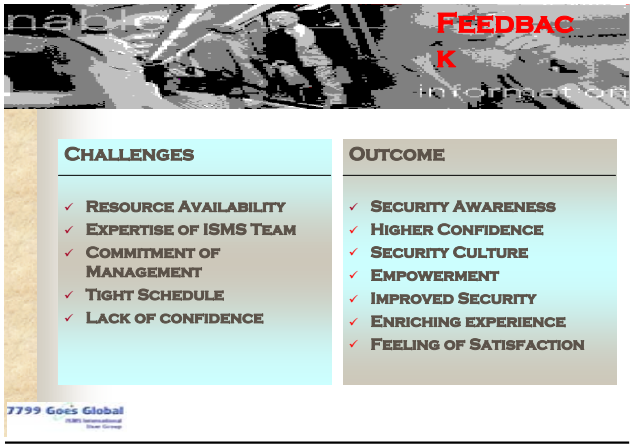
The Mauritius Standards Bureau (MSB) which is the national certification body was entrusted the responsibility to perform the certification work. No major non-conformities were reported while a few actions were added to the "To-Do-list". Given that the MSB was still in the process of getting accredited for BS7799-2, the outcome of the audit was

restricted to 'soft' certification. Once the MSB completes its accreditation which is imminent, the 'soft' certification would be upgraded into full-fledged certification after the successful completion of surveillance audits.

While the internal auditing process took barely a couple of hours, the certification audit was completed in less than one day for each site. This rapidity was attributed to the electronic format of the ISMS manual and its completeness with regard to BS 7799-2 requirements.

Slide 21 – Feedback

One of the key challenges faced by the pilot sites during the implementation process was shifting of appropriate resources to the project at the expense of other business activities which suffered a temporary slow down. There was also initially a feeling of lack of confidence among certain officers regarding the chances of success of the exercise. Officers involved had to put in much effort to develop a good understanding of the standards and the process given the newness of the assignment and the tight schedule set to show results. Engagement of top management was not straightforward since security was perceived as a technical rather than a management issue. Intense marketing and close central coordination were necessary to secure management buy-in and commitment.



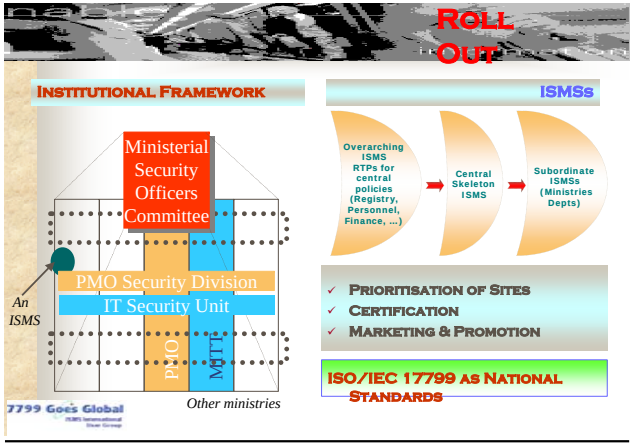
An increasing awareness and appreciation of information assurance by everyone involved was witnessed which set the foundation for the building up of a security culture. A general feeling of satisfaction and achievement prevailed among all members with regard to their contribution and dedication to the successful implementation of the security standards. Senior management felt more empowered to decide what information

assurance controls they needed to fulfil their business objectives. The successful adoption of the standards by the sites was qualified as passing an important milestone in their journey towards establishing a more congenial and secure atmosphere and heightening confidence in their businesses.

The overall time from start of the exercise to 'soft' certification of all the sites was about four months which was really amazing when compared to the relatively much longer period required for ISO 9001 certification. It was unanimously agreed that the methodology adopted along with the electronic skeleton ISMS manual catalysed the implementation process.

Slide 22 – Roll-Out

Following the successful pilot implementation of the standards, government of Mauritius has already initiated action for the roll-out of the standards across the civil service.



An institutional framework is being set up to monitor and facilitate the entire roll-out. A committee at the level of the Prime Minister's Office would act as policy maker and would spearhead the initiative. Other divisions and units within the structure would assume the roles of ISMS advisors and ISMS auditors.

An overarching ISMS would be developed which would support central policies and procedures applicable to the entire Civil Service. This would be utilised as a central ISMS skeleton for preparing ISMSs for individual Ministries and Departments.

Given resource constraints, the roll-out would be effected in a phased manner. Priorities would be established on the basis that activities posing the greatest potential risk from

breaches of information security to the government would be dealt with first.

The provision of information security awareness training for all officers is a requirement of BS7799-2. As part of the rollout, due consideration would be given to enhancing information security awareness through induction courses, campaigns and other forms of communication.

Ministries and Departments would certainly be encouraged to consider certification by the Mauritius Standards Bureau to hold a tangible proof of compliance to the standards. Certification would be an element of pride for the organisation and a reward to all those involved for their positive contribution.

Mauritius being already a safe tourist destination, Government through the proactive adoption of the ISO/IEC 17799 standards has strived to project a similar safe image of the country for business. This has acted as a trigger for the Mauritius Standards Bureau to seek accreditation for BS 7799-2. The ISO/IEC 17799 is now already in the process of being proclaimed as a national standard and it is expected that besides Ministries and Government Departments other organisations from the private sector will also join in to adopt the standards.

Slide 23 – THANKS