Information Security Standards in Government

The journey towards ISO/IEC 27001

Mrs R. Awotar-Mauree
IT Security Unit
Ministry of IT & Telecommunications
14 March 2006
Agenda

- The first steps
- Consultancy services
- Achievements
- What is Next
The first steps (I) – NITSP 1998

- SHOCKING framework
  - Standards & Practices WG - ‘To develop and implement standards and practices identified’

- IT Security
  - to preserve and protect organisation information assets from intentional or unintentional acts or natural events which may result in their unauthorised disclosure, modification, destruction of information

- Why?
  - Information is an essential resource
  - Government generates and manages a huge amount of information
  - Protecting such information is a major challenge
  - Increasing risks posed by rapid technological development & the widespread opening up of networks
Objective
- review existing security standards worldwide
- make recommendations for the adoption of a suitable standard for the Government

Scope of the standard
- identify the weaknesses of government systems
- provide security measures to avoid financial losses, data losses and overall failure of systems

Committee recommendations
- Adopt ISO/IEC 17799 standard
- Capacity Building on ISO/IEC 17799
- Conduct pilot implementations
The first steps (III)

- February 2002- Govt. approval to implement ISO/IEC 17799 in Civil Service
- September 2002- a tender for consultancy services is floated
- Tender is awarded to E-Commerce Institute LLC Europe
  - Mr W. List & Dr D. Brewer
  - October 2003 to April 2004
Consultancy Services

Objectives

- Provide a practical approach to implementing ISO/IEC 17799 in the Civil Service
- Train staff in standards implementation and auditing
- Implement standards at four pilot sites
- Audit and make recommendations on certification for pilot sites
- Recommend approach for rollout of standards in Civil Service
Consultancy Services

ISMS: Information Security Management System

- Implement effective information security that really meets business requirements
- Manage risks to suit the business circumstances
- Manage incident handling activities
- Build a security culture
- Conform to the requirements of the standards
Consultancy Services

Objectives

- Provide a practical approach to implementing ISO/IEC 17799 in the Civil Service
- Train staff in standards implementation and auditing
- Implement standards at four pilot sites
- Audit and make recommendations on certification for pilot sites
- Recommend approach for rollout of standards in Civil Service
Consultancy Services

Approach

- ISMS built by people who will own it
- Training to ALL involved with the ISMS
- Use of Skeleton ISMS to ‘fast Track’ creation of actual ISMS manual
  - Standard elements are already provided – customise them
  - ISMS is in hypertext – local web site with facility to refer to existing documents (hardcopies or softcopies)
  - Templates to assist in internal audits, management reviews etc.
- Version control
Consultancy Services

- Approach – Skeleton ISMS
  - Develop Risk Treatment Plans in very user-friendly way
  - Tell a story on
    - what is identified as a critical security event/concern
    - say what can cause it (threat)
    - what assets are affected
    - what is the consequential impact
    - Then continue by elaborating how the chances of this event occurring is actually mitigated (risk treatment) until the risks are acceptable or the possibility of the event occurring is reduced to zero
  - To-Do-List: a practical way to manage implementation of improvements and additional security requirements
Consultancy Services

Objectives

- Provide a practical approach to implementing ISO/IEC 17799 in the Civil Service
- **Train** staff in standards implementation and auditing
- Implement standards at four pilot sites
- Audit and make recommendations on certification for pilot sites
- Recommend approach for rollout of standards in Civil Services
Consultancy Services

- Training
  - Teams developing ISMSs in pilot sites
    - Drafting of ISMSs of pilot sites is initiated in training
  - Management staff at pilot sites
    - How to proceed with ISMS use & maintenance
  - Team that will conduct Internal Audits
    - Requirement of standards
Consultancy Services 2003/4

Objectives

- Provide a practical approach to implementing ISO/IEC 17799 in the Civil Service
- Train staff in standards implementation and auditing
- **Implement** standards at four pilot sites
- Audit and make recommendations on certification for pilot sites
- Recommend approach for rollout of standards in Civil Services
Consultancy Services

- Implementation at pilot sites
  - Use skeleton ISMS drafted in training as starting point
  - Team working sessions to complete RTPs
  - Review of work by consultants
  - Team working sessions to map the controls in the Statement of Applicability to
    - RTPs
    - Law or Government wide policy
    - Organisation level policy
    - Write down is done as a general rule
  - Team working sessions to complete other aspects ISMS
  - Consultants reviewed ISMS as a whole
Consultancy Services 2003/4

Objectives

- Provide a practical approach to implementing ISO/IEC 17799 in the Civil Service
- Train staff in standards implementation and auditing
- Implement standards at four pilot sites
- Audit and make recommendations on certification for pilot sites
- Recommend approach for rollout of standards in Civil Services
Consultancy Services

- Audit of pilot sites
  - Internal audits
    - Conducted by trained CIB/CISD staff
  - MSB mock audit
    - Passed desktop audit
    - No major non conformities in implementation audit
Consultancy Services

- Feedback from pilot sites
  - Security Awareness
  - Higher Confidence
  - Security Culture
  - Improved Security
  - Enriching experience
  - Feeling of Satisfaction
Consultancy Services

Objectives

- Provide a practical approach to implementing ISO/IEC 17799 in the Civil Service
- Train staff in standards implementation and auditing
- Implement standards at four pilot sites
- Audit and make recommendations on certification for pilot sites
- **Recommend** approach for *rollout* of standards in Civil Services
Consultancy Services

- Some of the Recommendations
  - Set up an institutional Framework
    - IT Security Unit at MITT to facilitate ISMS development & conduct internal audits
    - Higher instance at PMO Security Division level
  - Establish a high level Civil Service Wide ISMS with all common functions
    - Facilitate & speed up ISMS elaboration in Mins/Depts
    - Easier to propagate changes in common functions
  - Prioritise Mins/Depts sites for ISMS implementations
  - Seek certification services from national bodies
  - Adopt information security standards at National Level
Achievements

- IT Security Unit creation – August 2004
  - Follow-up with pilot sites
  - Additional ISMS site done in 2005
  - Liaise with other Government institutions
    - PMO, CIB, CISD, NCB (GOC)
    - National Audit Office, Internal Control, Police IT Unit, SLO
- Consultancy for Civil Service Wide ISMS - 2006
  - Civil Service wide ISF set up at highest instances
    - priority sites for rollout
    - 3 new ISMSs have been initiated
- National Standard
  - ISO/IEC 17799 adopted in early 2005
  - ISO/IEC 27001 adoption is in progress
- Mauritius Standards Bureau is getting ready to certify sites
IT Security Unit

Set up in August 2004 under the aegis of the Ministry of IT & Telecommunications

Mandate

- Implement Government policies in regard to IT Security
- Assist Ministries/Departments in the implementation of security standards
- Disseminate information on IT security
- Carry out security audits
What is next

- Certification for 5-8 sites
- 4 pilot sites of 2004 to conform to ISO 27001
- Facilitate ISMS development in priority sites identified at the level of the Civil Service Wide ISF
- Maintain the Civil Service wide ISMS
- Integrated management systems…
End Note

‘Information Security is not an IT issue – it is a business issue’

‘There is no such thing as 100% security – we can only strive to remain within the limits of acceptable risks’

‘Information security is a journey on which Government has embarked and is moving on smoothly’