ISO/IEC 27001:
a comprehensive approach to Information Security

Republic of Mauritius
Ministry of IT and Telecommunications, IT Security Unit

Computer Security Week 1st December 2006

Certificate No. IS 85916

Certificate No. FS 30710

Dr. David Brewer
Gamma Secure Systems Limited
www.gammassl.co.uk

Agenda

- ISO/IEC 27001
- ISO/IEC 17799
- Certification
- Case Studies
- Summary

- ISO/IEC 27001 is a *management system standard*
- ISO/IEC 17799 (27002) *is a catalogue of controls you might use*
- Other standards concern guidance, metrics, risk assessment and certification

ISO/IEC 27001

Information Security Management Systems - Requirements

ISO/IEC 27001

Information Security Management Systems - Requirements

©Gamma Secure Systems Limited, 2006

Policy

ISMS Policy

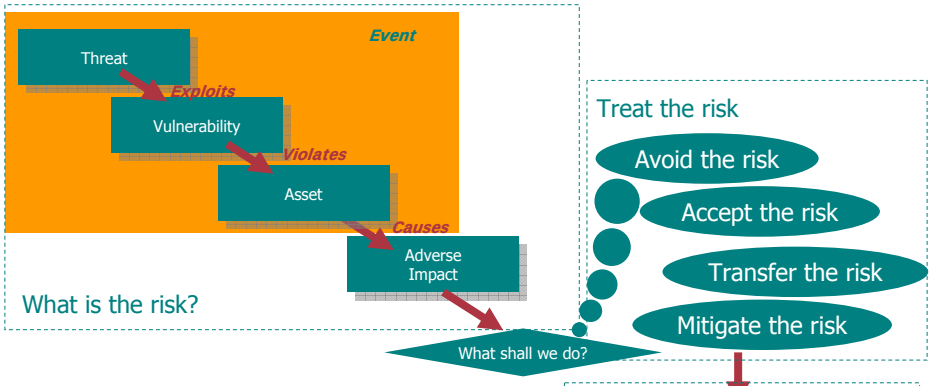

RISK EVALUATION CRITERIA

MANAGEMENT

- Statements to cover the requirements of the standard
- The boss wants it done that way
- Policy requirements set by a higher authority (e.g. Group HQ), as a result of their risk assessment (perhaps)
- Local policy requirements (e.g. to link to HR policy/procedures, quality policy/procedures …)
- Statements to reduce effort later (policy does not explain why, whereas risk assessment does), e.g. "*good password practice shall be followed*"

Risk Treatment Plans

Risk Treatment Plans



- Proportionality → controls should be commensurate with the risk
- Decide which of the 133 controls in Annex A are applicable

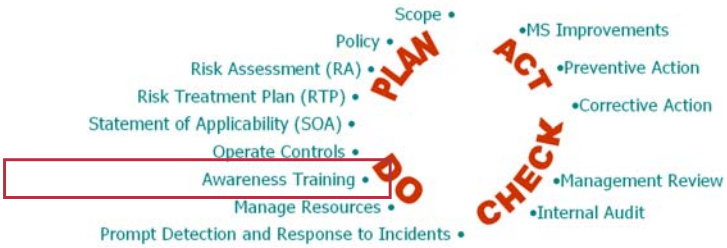
Statement of Applicability

Statement of Applicability

- Policy/RTPs should have identified all controls, but has anything been overlooked?
  - *What do other people do?*
  - *What do they do that applies to us?*
  - *If it applies do we do it?*
- This is just what the SOA (Annex A ~ IS 17799) is about
  - *Go through all 133 controls, say whether applicable or not*
  - *Justify by giving the reason for its selection or exclusion*
- SOA ←→ "Alternative Ideas" List (AIL)
- It is a "safety net"

NOTE: The Statement of Applicability provides a summary of decisions concerning risk treatment. Justifying exclusions provides a cross-check that no controls have been inadvertently omitted.

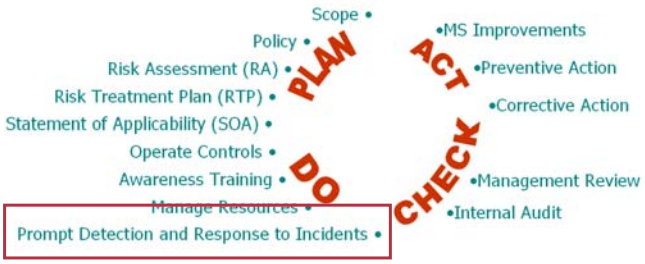
Awareness Training



Awareness Training

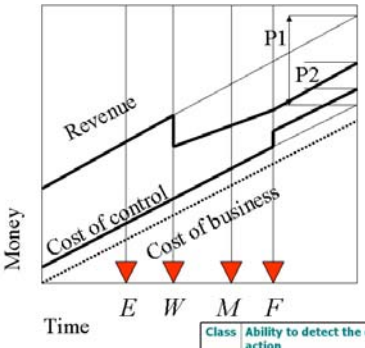
- Awareness, training and competence
  - *Security principles*
  - *Attacks*
  - *Policies/procedures*
  - *Incidents*
  - *Key points*

Incident Handling



Prompt Detection …

- Incident Identification and Reporting
- Incident Handling and Escalation
- Communicating Results and Tidying Up

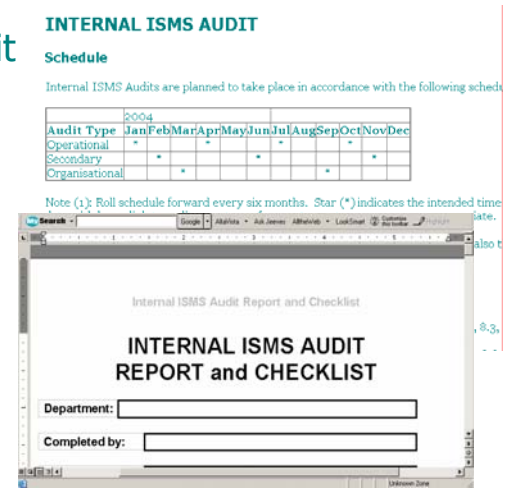


Class	Ability to detect the event and take recovery action	Type
1	Prevents the event, or detects the event as it happens and prevents it from having any impact	Preventive
2	Detects the event and reacts fast enough to fix it well within the time window	Detective
3	Detects the event and just reacts fast enough to fix it within the time window	
4	Detects the event but cannot react fast enough to fix it within the time window	
5	Fails to detect the event but has a partially deployed BCP	Reactive
6	Fails to detect the event but does have a BCP	
7	Fails to detect the event and does not have a BCP	

Internal ISMS Audit

Internal ISMS Audit

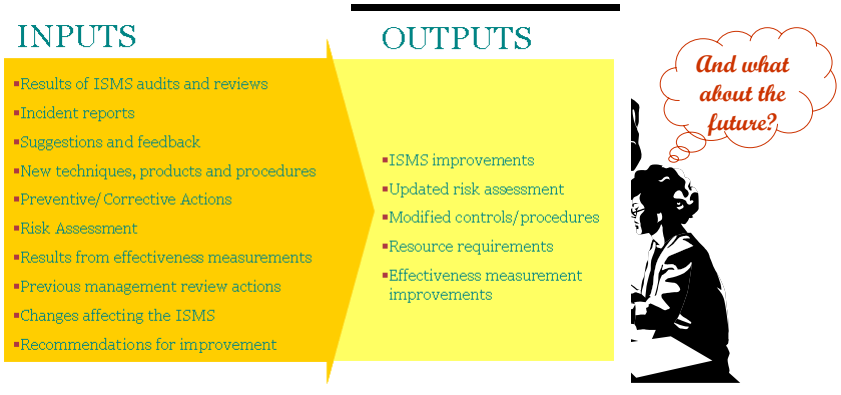
- An internal ISMS audit schedule
- Regularly check that controls as implemented meet policy objectives, e.g. reduce risks to the accepted level



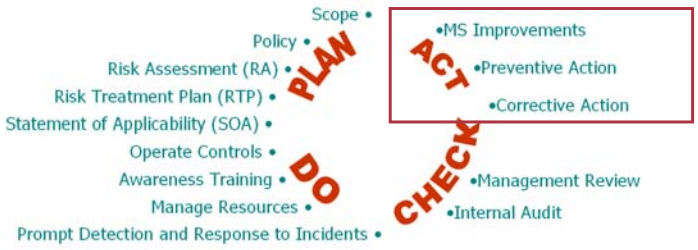
Management Reviews

Management Reviews

- The RTP owners periodically take stock of the ISMS – is it effective?



Metrics - Effectiveness



Metrics

- Need to assess effectiveness of ISMS
- Guidance will be in ISO/IEC 27004 – still under development

Interpreting the Results

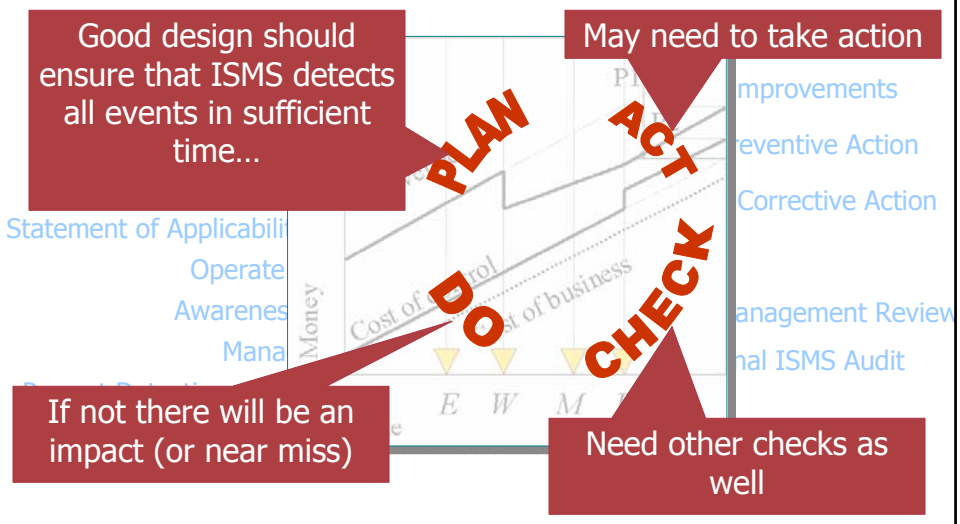
- Perfect
- On target
- Below target, but close
- Way below target

- 1 - %CFES = (TCFES / TC) x 100
  where TCFES = ∑ co-workers who have received training in security, and TC = Total no. of co-workers
- F – PFS = (IPF / TIS) x 100
  where IPF = ∑ Security incidents caused by lack of training, and TIS = Total no. of security incidents
- 1 - %SPSM = (TSP / TSA) x 100
  where TSP = ∑ Information systems protected from malware, and TSA = Total number of systems threatened by malicious software

Extracts from New ISO Work Item on ISMS metrics

- Detect event in sufficient time to prevent or mitigate impact

ISMS Effectiveness



ISO/IEC 17799

Code of Practice for Information Security Management

ISO/IEC 17799

Typical IS Events Addressed by SOA

- Theft
- Acts of God, vandals and terrorists
- Fraud
- IT failure
- Hacking
- Denial of service
- Disclosure
- Breach of the law
- Inappropriate deployment of people

Typical Business Impacts of Concern

- Adverse press coverage
- Organisation ceases trading
- Inability to carry out all or some of its business
- Loss of customer confidence
- Loss of revenue
- Increased costs
- Prosecution

Limitations

- Covers physical, environmental and personal security, compliance with the law etc, but …
- … IT component focuses on IT platforms
- There is very little on business applications
- Nevertheless scope of ISO/IEC 27001 is everything concerning information security, including the business applications
- If you want, use another AIL

CERTIFICATION

Accredited Certification

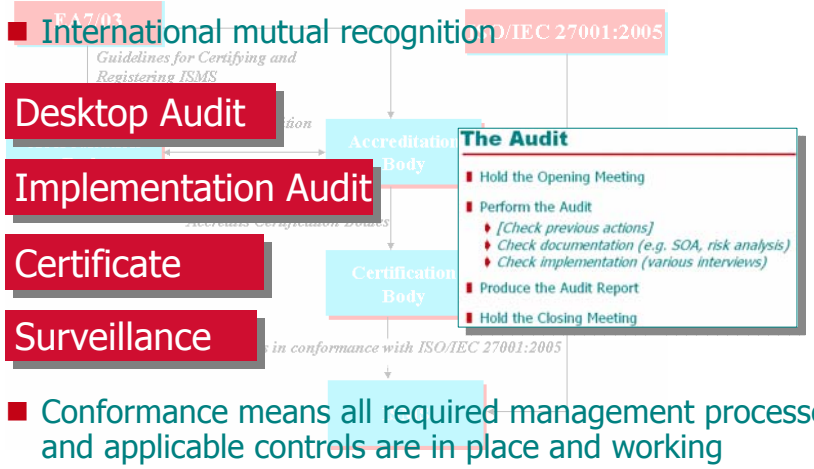
- International mutual recognition

Desktop Audit

Implementation Audit

Certificate

Surveillance



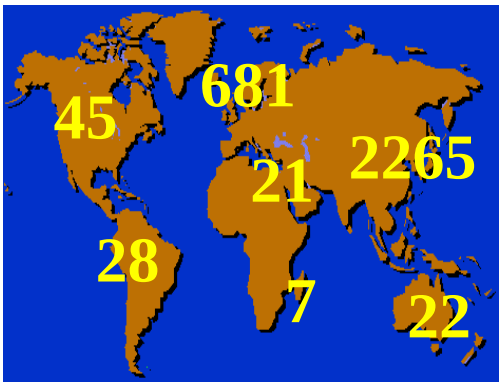
- Conformance means all required management processes and applicable controls are in place and working

Non Conformities

A non-conformity "is the absence of, or failure to implement and maintain, one or more required management system elements, or a situation which would, on the basis of objective evidence raise significant doubt as to the capability of the ISMS to achieve the security policy and objectives of the organisation."

This definition comes from EA7/03

International Take-up



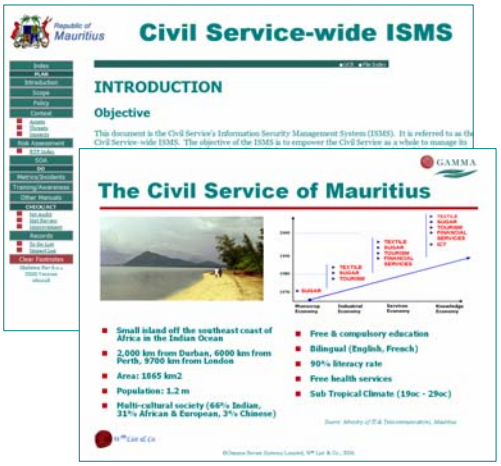
ISMS Registrations by Continent

5 November 2006

CASE STUDIES

Mauritius

- Civil service-wide roll out
- Treasury, Civil Status, Passport & Immigration, Social Security, GOC, …
- Plus a civil service-wide ISMS
- Covers all business applications properly
- Drive towards being a cyber island of quality
- Has significantly increased security awareness – essential for a cyber-culture



Middle East

- Telecommunications * Petroleum
- Scope – just the IT department, so just IT not the business applications
- Need to take care because the ISMS is not responsible for everything
- Could use similar ISMS architecture as Mauritius to extend scope

- Facilitating increased awareness and tuning of policies to business requirements (i.e. not just following ISO/IEC 17799 blindly, especially where the guidance is inappropriate)

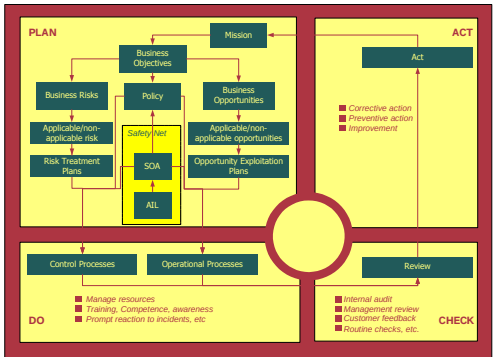
Eastern Europe

- Air traffic control

- Business (air traffic control) excluded as subject to international regulations, so just IT component
- Just started – wants a market differentiator

United Kingdom

- Fully integrated management system
- Covers all business applications properly
- ISO 9001
- ISO/IEC 27001
- Finance
- Health and Safety
- Sales and Marketing (opportunity exploitation)
- Key to running the business better



SUMMARY

Summary

- Comprehensive standard for information security
- Management standard (Plan-Do-Check-Act)
- Allows controls to adapt to changing circumstances (policy getting in the way of the business? – change the policy)
- Comprehensive IT-platform focussed AIL
- Increases awareness – better security – better business

ISO/IEC 27001: a comprehensive approach to Information Security

Republic of Mauritius

Ministry of IT and Telecommunications, IT Security Unit

Computer Security Week 1st December 2006

Any Questions?

Certificate No. IS 85916

Certificate No. FS 30710

Dr. David Brewer
Gamma Secure Systems Limited
www.gammassl.co.uk