

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

©Gamma Secure Systems Limited, 2006

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
- 

©Gamma Secure Systems Limited, 2006

ISO/IEC 27001

Information Security Management Systems - Requirements

ISO/IEC 27001

Information Security Management Systems - Requirements



Policy



ISMS Policy

RISK EVALUATION CRITERIA
 Risk shall be evaluated in terms of the likelihood of a risk event occurring and the impact that the event could have on the organization if it occurs.
 The risk threatening events shall be identified through a risk assessment process.
 The risk threatening events shall be identified through a risk assessment process.
 The risk threatening events shall be identified through a risk assessment process.

MANAGEMENT
 The role and responsibility for managing information security shall be defined in the Information Security Policy.
 The role and responsibility for managing information security shall be defined in the Information Security Policy.
 The role and responsibility for managing information security shall be defined in the Information Security Policy.

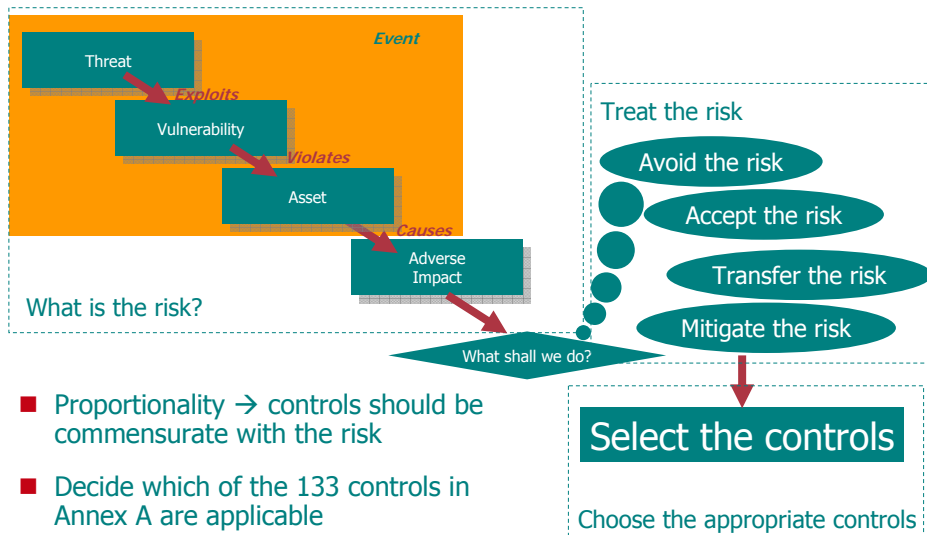
- Statements to cover the requirements of the standard
- The boss wants it done that way
- Policy requirements set by a higher authority (e.g. Group HQ), as a result of their risk assessment (perhaps)
- Local policy requirements (e.g. to link to HR policy/procedures, quality policy/procedures ...)
- 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?

YES, policy xyz, events, abc
 see reference
 Clause N/A reason
 Link forward to procedure manuals etc.

- 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

Link back to risk treatment plan

- 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

Key points

Key points

Key points

Key points

Key points

Key points

Eavesdropping

- TEMPEST (computers radiate)
- Wireless networks
- Wireless telephones (no encryption)
- Stand next to a person using a mobile



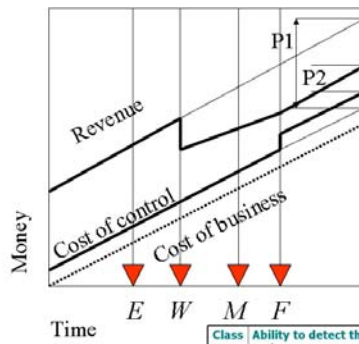
Incident Handling



©Gamma Secure Systems Limited, 2006

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 DCP	Reactive
6	Fails to detect the event but does have a DCP	
7	Fails to detect the event and does not have a DCP	

©Gamma Secure Systems Limited, 2006

Internal ISMS Audit



©Gamma Secure Systems Limited, 2006

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

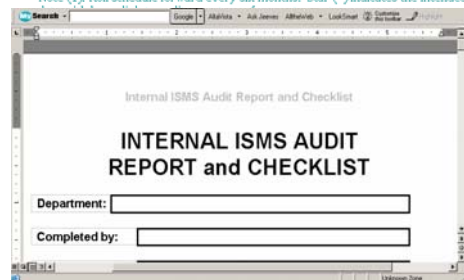
INTERNAL ISMS AUDIT

Schedule

Internal ISMS Audits are planned to take place in accordance with the following schedule:

Audit Type	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
Operational	*											
Secondary		*										
Organisational			*									

Note (1): Roll schedule forward every six months. Star (*) indicates the intended time date.



©Gamma Secure Systems Limited, 2006

Management Reviews



Management Reviews

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

INPUTS

- Results of ISMS audits and reviews
- Incident reports
- Suggestions and feedback
- New techniques, products and procedures
- Preventive/Corrective Actions
- Risk Assessment
- Results from effectiveness measurements
- Previous management review actions
- Changes affecting the ISMS
- Recommendations for improvement

OUTPUTS

- ISMS improvements
- Updated risk assessment
- Modified controls/procedures
- Resource requirements
- Effectiveness measurement improvements



Metrics - Effectiveness



©Gamma Secure Systems Limited, 2006

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

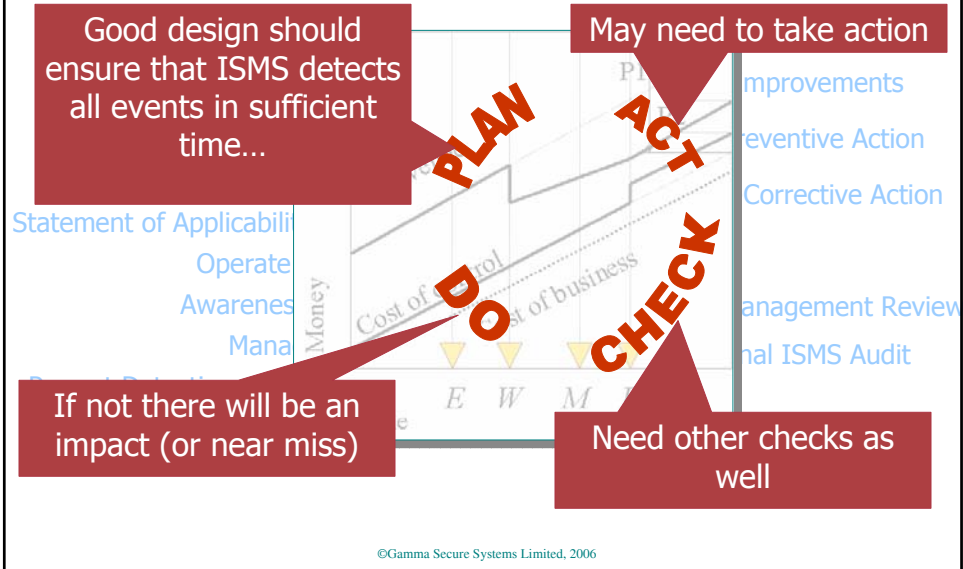
- $1 - \%CFES = \frac{TCFES}{TC} \times 100$
 where $TCFES = \sum$ co-workers who have received training in security, and $TC =$ Total no. of co-workers
- $F - PFS = \frac{IPF}{TIS} \times 100$
 where $IPF = \sum$ Security incidents caused by lack of training, and $TIS =$ Total no. of security incidents
- $1 - \%SPSM = \frac{TSP}{TSA} \times 100$
 where $TSP = \sum$ 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

©Gamma Secure Systems Limited, 2006

ISMS Effectiveness



ISO/IEC 17799

Code of Practice for Information Security Management

ISO/IEC 17799

- Security Policy
- Organising Security
- Asset Management
- Human Resources
- Physical and Environmental Security
- Communications and Operational Management
- Access Control
- Information Systems Acquisition, Development and Maintenance
- Information Security Incident Management
- Business Continuity Management
- Compliance

- Roles and responsibilities
- Screening
- Terms and conditions of employment

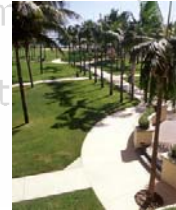
- Prior to employment
- During employment
- Termination or change of employment

Typical IS Events Addressed by SOA

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

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

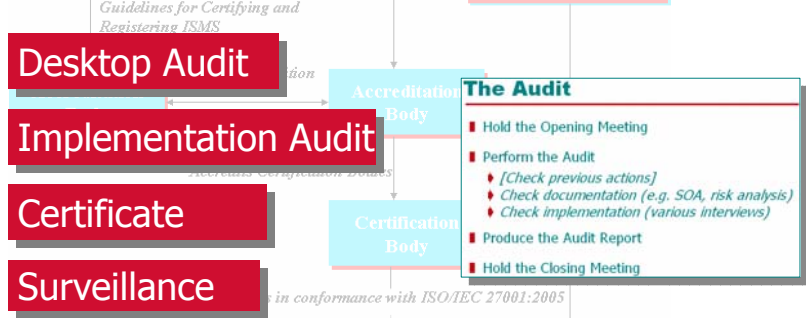
- Covers physical, environmental and personal security, compliance with the law etc, but ...
- ... IT component focuses on IT platforms
- There is very little on business applications
- Nevertheless scope of ISO/IEC 27001 is everything concerning information security, including the business applications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



CERTIFICATION

Accredited Certification

- International mutual recognition / IEC 27001:2005



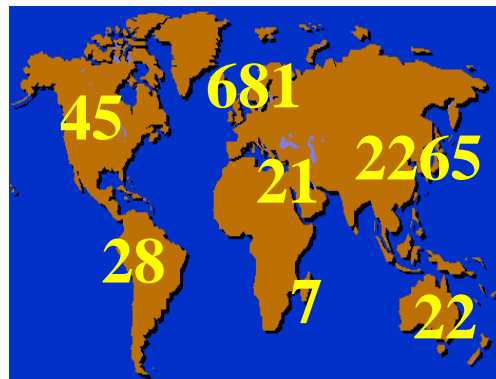
- Conformance means all required management processes and applicable controls are in place and working

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



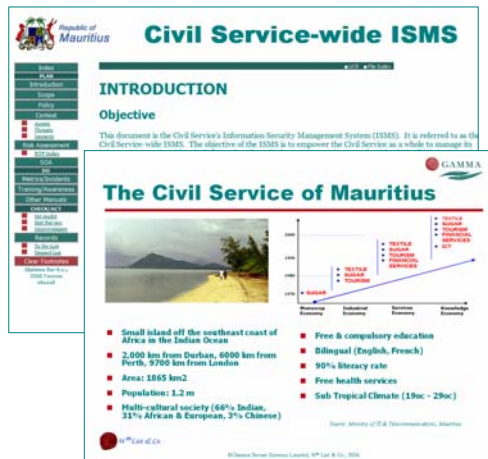
ISMS Registrations by Continent

*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



Civil Service-wide ISMS

INTRODUCTION

Objective

This document is the Civil Service's Information Security Management System (ISMS). It is referred to as the Civil Service-wide ISMS. The objective of the ISMS is to empower the Civil Service as a whole to manage its

The Civil Service of Mauritius

Small island off the southeast coast of Africa in the Indian Ocean

2,000 km from Durban, 6000 km from Perth, 9700 km from London

Area: 1845 km²

Population: 1.2 m

Multi-cultural society (66% Indian, 31% African & European, 3% Chinese)

Free & compulsory education

Bilingual (English, French)

90% literacy rate

Free health services

Sub Tropical Climate (19oc - 29oc)

©Gamma Secure Systems Limited, 9th Jan 8, 2006

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)



©Gamma Secure Systems Limited, 2006

Eastern Europe

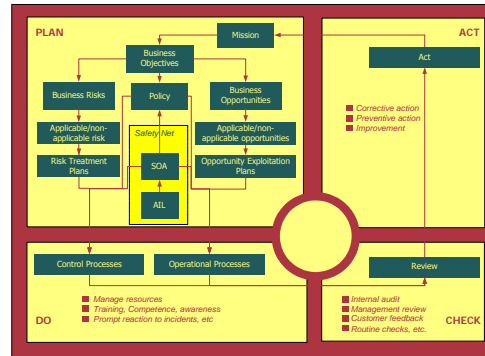
- Air traffic control
 - Air Traffic Management Regulations
 - ISO/IEC 27001 Annex A (the ISMS AIL)
 - SOA (applicable controls)
 - Non-applicable controls
- Business (air traffic control) excluded as subject to international regulations, so just IT component
- Just started – wants a market differentiator



©Gamma Secure Systems Limited, 2006

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



©Gamma Secure Systems Limited, 2006

SUMMARY

©Gamma Secure Systems Limited, 2006

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

©Gamma Secure Systems Limited, 2006

ISO/IEC 27001: a comprehensive approach to Information Security



Computer Security Week 1st December 2006

Any Questions?



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

©Gamma Secure Systems Limited, 2006