

# Implementing ISO/IEC 27001



Computer Security Week 30<sup>th</sup> November 2006



Certificate No. IS 85916



Certificate No. FS 30710

*Dr. David Brewer*

*Gamma Secure Systems Limited*

*[www.gammassl.co.uk](http://www.gammassl.co.uk)*

©Gamma Secure Systems Limited, 2006

## Agenda

- ISMS standards
- Implementation strategies
- Fast track
- 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

# The ISMS Standards

## ISO/IEC 27001

### Information Security Management Systems - Requirements



# ISO/IEC 17799

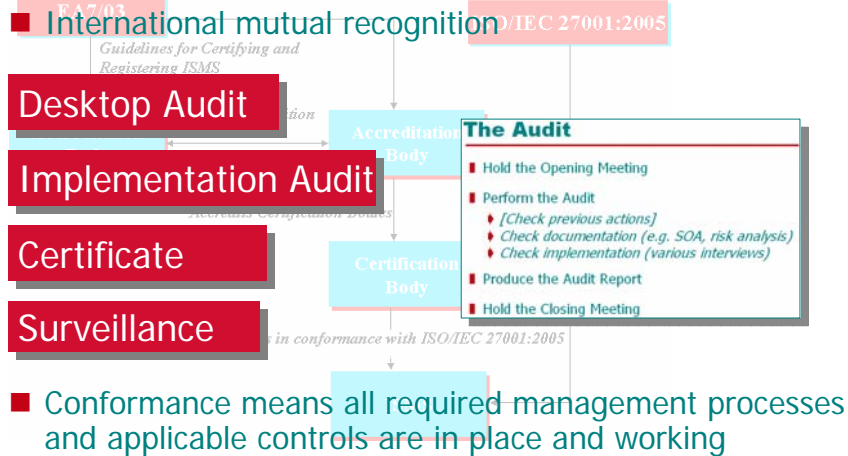
- Security Policy
  - Organising Security
  - Asset Management
  - Human Resources
  - Physical and Environmental Security
  - Communications Security
  - Access Control
  - Information Security Management
  - Information Security Incident Management
  - Business Continuity Management
  - Compliance
- Roles and responsibilities
  - Screening
  - Terms and conditions of employment
- Prior to employment
  - During employment
  - Termination or change of employment

# Caveat

- 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



# Accredited Certification



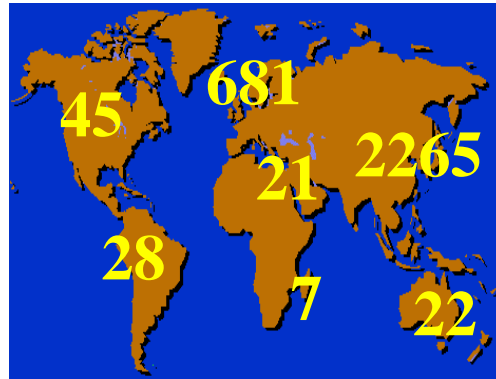
# Non Conformities

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

©Gamma Secure Systems Limited, 2006

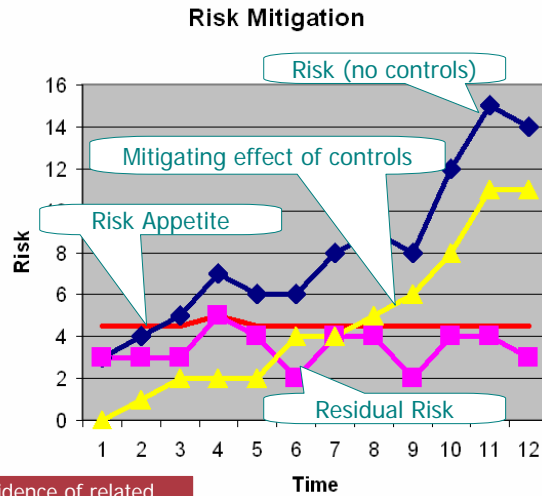
---

# Implementation Strategies

©Gamma Secure Systems Limited, 2006

## Risk as a Function of Time

- Risk changes with time
- New/improved controls are used to mitigate the risk
- Residual risk must be within the risk appetite
  - Else you stop work while things are fixed
  - Or risk appetite must be increased



There will be little/no evidence of related security incidents

©Gamma Secure Systems Limited, 2006

## Strategies

- Build a brand new system 1
  - Aim to comply with ISO/IEC 17799
  - Carry out the Risk Assessment/Treatment and determine the controls from that 2
- Go with what you have today 3
- Start-up – usually 2

©Gamma Secure Systems Limited, 2006

## Strategy 1 – New (17799)

- Develop brand new policies and procedures according to ISO/IEC 17799
- Upside
  - *Looks fantastic*
- Downside
  - *Can take a long time (1½ - 2 years)*
  - *Control might be counter-cultural or over-the-top*
  - *Too much documentation that nobody reads*
  - *Risk assessment might be meaningless*
  - *Scope for plenty of non-conformities*
  - *Management system process often get forgotten*

As the controls are “new” no one knows what to do, so the auditor is likely to find that they are not followed. They will take time to bed in.

Vasa: sank in 1628 within 1 mile of the start of her maiden voyage

©Gamma Secure Systems Limited, 2006

## Strategy 2 – New (Tailored)

- Develop brand new policies and procedures driven by actual needs
- Upside
  - *Custom made*
- Downside
  - *May still take a long time (6 – 18 months)*
  - *Scope for non-conformities while new controls are bedded in*
  - *Management system process may get forgotten*

©Gamma Secure Systems Limited, 2006

## Strategy 3 – Now

- Just document the controls as they are now
- Upside
  - Very quick (3 – 4 months)
  - Focus is on the management system processes
  - Use the management system to manage change
- Downside
  - Writing down what you do now can be soul destroying
  - Must accept that weak controls represent an acceptable risk
  - Some scope for non-conformities if actual practices are indefensible or corrective actions not in place

## Which is Best?

- Strategy 1 is a hiding to nothing
- Strategy 2 and 3 are compatible, but why wait?
- Apply 3, the use it to create 2

**Strategy 1 – New (1779)**

- Develop brand new policies and procedures. ISO/IEC 17799
- Upside
  - Looks fantastic
- Downside
  - Can take a long time (1½ - 2 years)
  - Control might be counter-cultural or
  - Risk assessment might be meaningless
  - Scope for plenty of non-conformities
  - Management system process often get

*As the new one comes and they get in the way*

**Strategy 3 – Now**

- Just document the controls as they are now
- Upside
  - Very quick (3 – 4 months)
  - Focus is on the management system processes
  - Use the management system to manage change
- Downside
  - Must accept that weak controls represent an acceptable risk
  - Some scope for non-conformities if actual practices are indefensible or corrective actions not in place

**Strategy 2 – New (Tailored)**

- Develop brand new policies and procedures driven by actual needs
- Upside
  - Custom made
- Downside
  - May still take a long time (6 – 18 months)
  - Scope for non-conformities while new controls are needed in
  - Management system process may get forgotten



## ISO 9001 Experience

---

- Early implementations typically Strategy 1
  - *Quality managers documented nice to have systems*
  - *Lots of non-conformities*
  - *Lots of retrospective activity prior to audits*
- Now frowned upon by assessors
- Best advice “just document what you do”
- It’s then into the continuous improvement cycle

---

## The Fast Track Approach

(see <http://www.gammasl.co.uk/topics/ics/FTISMS.pdf> for an open specification)

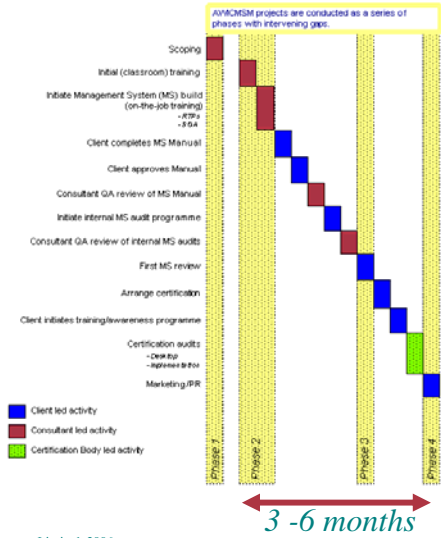
*[Strategies 2 and 3]*

# Overview

- Classroom/on-the-job training, throughout at least one PDCA cycle

- Role Model
- To-Do-List concept
- Overarching/subordinate ISMS
- Event-impact RTPs
- Skeleton ISMS

- Integrate with existing internal control structures
- Marshal existing procedures/records



©Gamma Secure Systems Limited, 2006

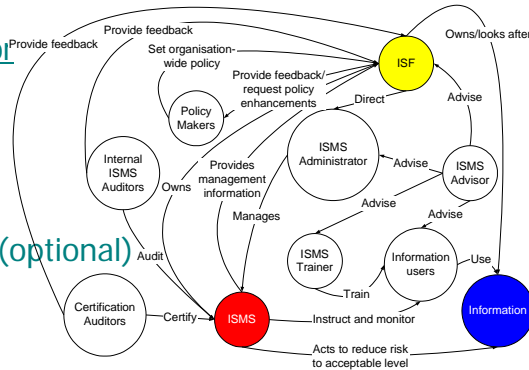
# Role Model

©Gamma Secure Systems Limited, 2006

## Role Model

---

- Information Security Forum (ISF)
- ISMS Administrator
- Internal ISMS Auditor
- ISMS Trainer
- ISMS Advisor
- Certification auditor (optional)
- Policy Maker



©Gamma Secure Systems Limited, 2006

## *The "To-Do-List" Concept*

©Gamma Secure Systems Limited, 2006

## The "To-Do-List" Concept

- Management standards, including ISO/IEC 27001 insist that the management processes must be in place
- But new security processes may be required because risks change
- At any point in time:
  - Existing security procedures in place
  - Newly identified ones still-to-do
- Managed using a "To-Do-List"

## The "To-Do-List" Concept

- Management standards, including ISO/IEC 27001 insist that the man
- **Can have entries in progress**

### The To-Do-List

Reference	Action		
MSR Actions 19.11/ 19.13	Add G4 and G5 See CRF.		
MSR Action 19.3	Produce new H		
New ISMS Standard	ISO/IEC 2700 Make the neces		
MSR Action 19.17	Add new risk (		
			1. Presented for review
Extend MS to cover OEPs	Create and add the Sales and Marketing Practice; and add the Sales and Marketing reviews to the MS records.	051130	As at 051103:

- Entries will be corrective, preventive or improving in nature
- There should be evidence that any risk is being managed

## Which Means ...

- Management standards, including ISO/IEC 27001, insist that the management system must be able to demonstrate that it can have entries in progress

### The To-Do-List

Reference	Action
MSR Actions 19.11/ 19.13	Add G4 and G5 See CRF.
MSR Action 19.3	Produce new H
New ISMS Standard	ISO/IEC 27001

- Entries will be corrective, preventive or improving in nature
- There should be evidence that any risk is being managed

- B
- b
- A
- I

Don't like what you do now, think it a non-acceptable risk in the *near future*, or just want a look 'n see - just put on the To-Do-List with an appropriate priority

## Overarching and Subordinate ISMSs



# ISMS Policy

**RISK EVALUATION CRITERIA**  
 Risk shall be evaluated in terms of the likelihood of a risk...  
 The impact shall be measured in terms of the financial cost...  
 The risk threatening events shall be identified through a...  
 Effectiveness of existing Security Controls.

**MANAGEMENT**  
 The role and responsibility for managing information security...  
 Effectively be known as the Information Security Forum...  
 Establish ISMS Policy, Objectives, Plans and Procedures...  
 Regularly review the effectiveness of the ISMS and...  
 Implement corrective actions as appropriate...  
 Monitor significant changes in exposure of their...  
 Conducts its business and changes in the way it...  
 Take appropriate defensive and corrective actions...  
 Subsequently take a such preventative action as...  
 Ensure the provision of the necessary resources...  
 Seek external specialist information security advice.

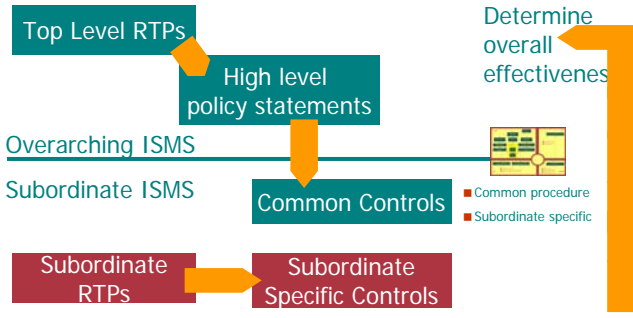


- Statements to cover the requirements of the standard
- The boss wants it done that way
- Policy requirements set by a higher authority (e.g. Group HQ), as a result of their risk assessment (perhaps)
- Local policy requirements (e.g. to link to HR policy/procedures, quality policy/procedures ...)
-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



# Overarching & Subordinate ISMSs

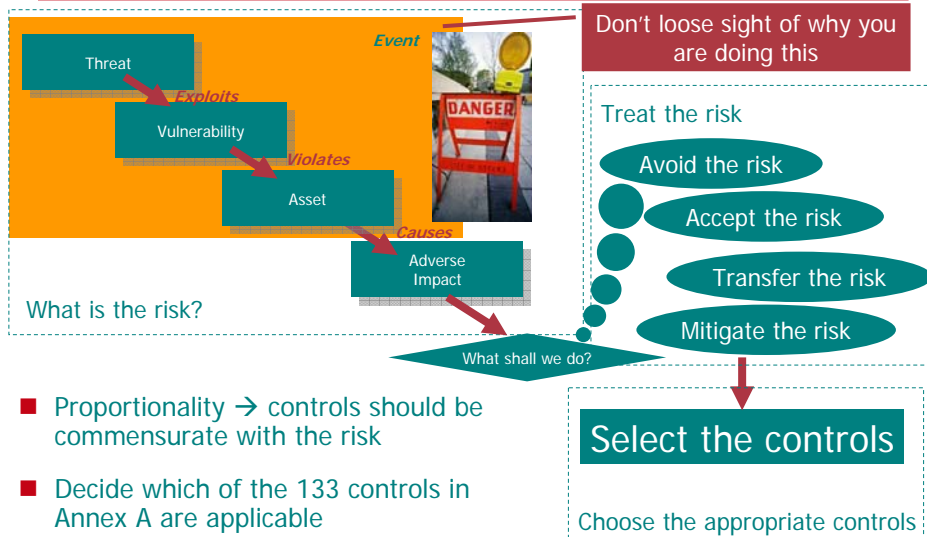
- Hierarchy of ISMSs
- Superior set policy for subordinate



# Event-driven Risk Treatment Plans



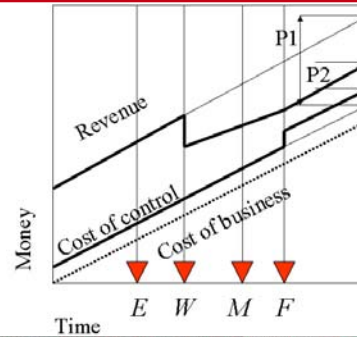
# Risk Treatment Plans



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

## Tell it Like a Story

- Predicated on "Time Model"
- Repeats the question "what if it doesn't work"
- Expressed in business terms in language everyone can understand



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

©Gamma Secure Systems Limited, 2006

## Typical IS Events and Impacts

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

Covers all 133 controls



©Gamma Secure Systems Limited, 2006



## Example RTP (1)

---

- Acts of God for a library (early 1900s – no IT)

The internal networks are connected to the Internet. There are also various modem access the internal networks remotely and read data, modify it, introduce malicious

- Threat agents: fire, flood, cyclone, vermin

The impacts of such events are:

- Assets: building, staff, books

■ Possible inability to carry out some or all of our business, see E5.1, E5.2, E5.3, E5.4

■ Possible unwanted disclosure of sensitive information (e.g. Groups F, K), see E5.2

- Impacts: inability to carry out some or all of the business of being a library

**Risk E5.1** A hacker could bring about our inability to carry out some or all of our business. The first line of defence against such an attack is the firewall. The ISP will therefore whether this firewall is always correctly configured, or if it is under attack. Not acceptable risk because there is a second line of defence, which lies in hardening the "Hotfix and service pack upgrades". However:

## Example RTP (2)

---

- Can we prevent the event?

The internal networks are connected to the Internet. There are also various modem access the internal networks remotely and read data, modify it, introduce malicious

➤ *Fire? Possibly :: state what we do, e.g. no smoking, lightning conductors, ..*

➤ *Flood? Library on top of a hill, 2000 feet above sea level, no history of flooding :: acceptable*

■ Possible unwanted disclosure of sensitive information (e.g. Groups F, K), see E5.2

■ risk court action against our company for breach of the Data Protection Act

➤ *Cyclone? No*

➤ *Vermin? Not cost effective*

**Risk E5.1** A hacker could bring about our inability to carry out some or all of our business. The first line of defence against such an attack is the firewall. The ISP will therefore whether this firewall is always correctly configured, or if it is under attack. Not acceptable risk because there is a second line of defence, which lies in hardening the "Hotfix and service pack upgrades". However:

## Example RTP (3)

---

- Fire – suppose preventive measure does not work, can we detect it?
  - Yes – smoke detectors, but this is 1905 so perhaps rely on sense of smell
  - Can we put it out? We can try – buckets of sand to hand, plenty of people, spare buckets, a full well and staff well trained (volunteer fire people)
  - What if we fail? Evacuate (save the staff), write a news report

## Example RTP (4)

---

- Cyclone – can we detect it?
  - Yes, very windy
  - What do we do? Close the shutters, take the most valuable books into the cellar and hide
  - What if the building collapses?
  - No problem, there is an escape route, well maintained used by smugglers of old
- Vermin – can we detect them?
  - Yes, regular inspection..

## Example RTP (5)

### ■ What if all fail (including flood)?

- *Well we are not the only library on the island*
- *There are copies of the most important books held in a mountain vault*
- *There are libraries overseas*
- *We are insured*

### ■ What if that fails? That is an acceptable risk

**Risk E5.1** A hacker could bring about our inability to carry out some or all of our b... such an attack is the **firewall**. The ISP pi... if it is not properly configured, or if it is under attack. Ne... acceptable risk because there is a second line of defence, which lies in hardening th... "Hotfix and service pack upgrades". However:

### ■ THE END OF THE STORY

## Skeleton ISMS

### Skeleton ISMS

WmList & Co.

Parts for you to complete

Version control

Covers every requirement of ISO/IEC 27001

# Skeleton ISMS

- Built-in facility for document control
- Space to define scope and context
- Prototype policy
- Provision for RTPs
- Virtually complete SOA (with built-in hyperlinks to policy statements and standard events)
- Facility for including training and awareness
- Internal audit proforma and checklist
- Management system review checklist
- Procedures for corrective action etc.
- To-Do-List and associated procedures
- Records
- Compliance index

# Skeleton ISMS

- There is space to define the ISMS scope, just as it will appear on the 27001 certificate
- And to define the ISMS context

The management of information security that covers the Information Technology activities in the provision of an internet banking channel to enable customers to conduct their banking business remotely, carried out at Skelmersdale and Salford. Statement of Applicability Version 2.0 dated 31/01/03

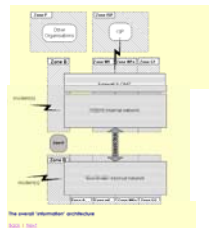


**INFORMATION SECURITY CONTEXT**  
ARCHITECTURE

The overall Information Security Architecture is shown in the Architecture. The figure depicts the Information Security Architecture of the organization. The Information Security Architecture is defined by the scope of the ISMS. The Information Security Architecture is defined by the scope of the ISMS. The Information Security Architecture is defined by the scope of the ISMS.

The scope of the ISMS is defined by the scope of the ISMS. The scope of the ISMS is defined by the scope of the ISMS. The scope of the ISMS is defined by the scope of the ISMS.

The scope of the ISMS is defined by the scope of the ISMS. The scope of the ISMS is defined by the scope of the ISMS. The scope of the ISMS is defined by the scope of the ISMS.



# Skeleton ISMS

- There is a prototype ISMS policy
- Most words are there to ensure compliance with the standards
- Some to simplify production of the SOA
- Customise with reference to relevant corporate policies

## ISMS POLICY

### RISK MANAGEMENT

Information Security Controls shall be selected on the basis of a risk assessment, which shall be carried out at regular intervals. The effectiveness of these controls shall be monitored and adjusted as necessary to reduce the business risk to an acceptable level and ensure that security continues to fulfil <<COMPANY>>'s requirements. Management shall adjust the overall set of Security Controls by relaxing the individual controls, strengthening them or exchanging them with more effective controls, or adding/deleting controls as appropriate.

### ASSETS

Assets, including information, business systems and applications, shall have identified Business Owners who are responsible for determining the level of acceptable risk and implementing the ISMS Policy and associated Security Controls. Assets shall be protected according to the business impacts that might result if their confidentiality, integrity or availability were to be compromised.

Monitor the effectiveness of the ISMS and the Security Controls deployed, and take corrective and preventive action as appropriate.

- Monitor significant changes in exposure of their assets to major threats, changes in the way <<COMPANY>> conducts its business and changes in the way it uses technology, and to take appropriate action
- Take appropriate defensive and corrective action in response to actual or suspected security incidents and independently take such preventative action as necessary
- Ensure the provision of the necessary resources to develop, implement, operate and maintain the ISMS
- Seek external specialist information security advice and review when appropriate and learn from others whenever possible
- Approve (or withdraw approval) for new information systems and/or major initiatives to enhance information security, the ISMS and operational systems, reviewing approved security related processes and communicating these to their employees
- Ensure an evaluation of information security activities throughout <<COMPANY>>
- Champion security throughout the organisation, and thereby promote visibility of Senior Management commitment for information security and the need for continual improvement throughout <<COMPANY>>.

The composition of the ISF is shown in the figure below. <<STATE WHO>> shall be responsible for Internal Audit.

### PERSONNEL POLICIES

All staff (including directors) should be trustworthy and be responsible for implementing the ISMS Policy and Security Controls within their business areas. Unauthorized disclosure, destruction, theft or damage of any asset in contravention of the Security Controls by any employee shall be regarded as cause for appropriate disciplinary action.

# Skeleton ISMS

- Provision to develop RTPs
- The standard eight plus any others

## RISK ASSESSMENT AND RISK TREATMENT

### APPROACH

The risk assessment is performed manually.

It identifies a variety of events (or concerns). Each event describes how a threat might violate the security of the identified assets to cause some impact. (GSI) has to see <<COMPANY>>'s assessment of the severity of these impacts.) The analysis thus takes account of the vulnerabilities that a threat agent may exploit, in the context of existing controls, in order to compromise an asset.

For each impact, within the context of that event, the risks are analyzed and a risk treatment plan is developed to reduce the risk to an acceptable limit.

Each event is then considered in turn, identifying:

### RISKS CONCERNING xxxx

<<DESCRIBE THE EVENT AND IN SO DOING REFER TO THE ASSETS . They are listed here with the correct links (to footnotes), so just delete. Of course, this list needs to be amended if the asset table is changed. If you delete an asset there is no need to change the labelled. Beware of the bookmarks if you do!>>

Asset Groups A, B, C, D, E, F, G, H, I, J, K, L, M, N, O, P, Q, R, S, T, Y, W, X, Y

<<Note all the impacts listed in the adverse impact summary are listed here. Delete those that do not apply. At the end of each line (where it says "see") just a reference to the risk, e.g. see D1-3, or S4-3a). Delete the "Possible/Probable" as appropriate.

- Possible/Probable adverse press coverage, see
- sible/Probable court action against an officer of << COMPANY >>, see
- sible/Probable court action against << COMPANY >>, see
- sible/Probable failure to prosecute, see
- sible/Probable inability to carry out some or all of << COMPANY >>'s business, see
- sible/Probable loss of all forms of data and information, see
- sible/Probable loss of citizen confidence, see
- sible/Probable loss of revenue, see
- sible/Probable loss of the monetary value of property and contents, see
- sible/Probable company goes to the wall/questions asked in Parliament, see

### ASSETS

The principal assets by type are listed in the table below. The person who is delegated responsibility for each asset is derived from the Risk Treatment Plan.

Asset Identifier	THREAT AGENT
Grc	There are a variety of threats
Phy	Fire, flood, cy
A	All employees

### Impact

Adverse press coverage

Company goes to the wall/Ct

Court action against << COM

Court action against an officer

Scope

MS Improvements

Preventive Action

Corrective Action

Management Review

Internal Audit



# Skeleton ISMS

- SOA with hyperlinks to the standard eight events and policy statements
- Skeleton included links to common policies and procedures



- SOA - PHYSICAL AND ENVIRONMENTAL SECURITY
- SOA - COMMUNICATIONS AND OPERATIONS MANAGEMENT
- SOA - ACCESS CONTROL
- SOA - INFORMATION SYSTEMS ACQUISITION, DEVELOPMENT AND MAINTENANCE
- SOA - INFORMATION SECURITY INCIDENT MANAGEMENT
- SOA - BUSINESS CONTINUITY MANAGEMENT
- SOA - COMPLIANCE

The following colour coding is used:

This Security Control is applicable and is a << COMPANY >> policy requirement.	This Security Control is applicable and is a << COMPANY >> policy requirement.
This Security Control is applicable and is a << COMPANY >> policy requirement.	This Security Control is applicable and is a << COMPANY >> policy requirement.

### PHYSICAL AND ENVIRONMENTAL SECURITY

#### Secure Areas

The objective of these controls is to prevent unauthorised physical access, damage and interference to the organisation's premises and information.

Annex & Control	Applicability
A.9.3.1 Physical security perimeter	YES, where (21), (22)
A.9.3.2 Physical entry controls	See the SOA where (21), (22)
A.9.3.3 Physical access to rooms and facilities	See the SOA where (21), (22)
A.9.3.4 Protecting against external and environmental threats	See the risk treatment plan for this control

©Gamma Secure Systems Limited, 2006

# Skeleton ISMS

- There is a facility for recording training and awareness activities for all staff
- Just amend/reference what you do

### TRAINING

It is an ISMS Policy requirement that responsibilities defined in WHERE THESE ARE DONE

- Determining the need for training
- Providing competent training
- Evaluating the effectiveness of training
- Maintaining records of training

### Eavesdropping

- TEMPEST (computers radiate)
- Wireless networks

less telephones (no encryption)

and next to a mobile phone on using a file

The interface includes a 'TRAINING' section with a list of responsibilities and a 'CHECK' section for 'Eavesdropping' with sub-sections for TEMPEST and wireless networks. It also features a 'TRAINING' section with a list of responsibilities and a 'CHECK' section for 'Eavesdropping' with sub-sections for TEMPEST and wireless networks.

©Gamma Secure Systems Limited, 2006

# Skeleton ISMS

- Page on Metrics/ Incident Handling
- Uses time theory
- Incident is occurrence of impact

## ISMS METRICS AND INCIDENT HANDLING

### INTRODUCTION

This page identifies and explains the metrics that we use to determine the effectiveness of our ISMS, and how we handle incidents.

We start by explaining the fundamental time theory and how it is used in developing the RTPs. We conclude that an incident is the occurrence of an impact and give instructions for dealing with incidents. << Introduce here any other metric that the organisation uses >>

<< NOTE: if you wish to use a different definition of an incident, state your definition here and amend the procedures described below accordingly. >>

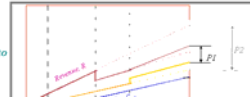
### TIME THEORY

#### Fundamental Principle

The fundamental time metrics' principle:

"...detect the event in sufficient time to do something positive about it..."

as illustrated in Figures 1(a) and 1(b).



### Impact Log

Get Impact occurrence in reverse chronological order.



Date	Event	RTP	Impact
<i>T<sub>e</sub></i>	<i>T<sub>d</sub></i>	<i>T<sub>r</sub></i>	<i>T<sub>w</sub></i>
			<i>I<sub>p</sub></i>
			<i>C<sub>control</sub></i>
Commentary			
Agreed action			Date executed

The qualitative measure for time and cost metrics if quantitative measures are not available or would be misleading due to imprecision.

# Skeleton ISMS

- An internal ISMS audit schedule
- Procedure, proforma report and checklist (ensures compliance when completed)

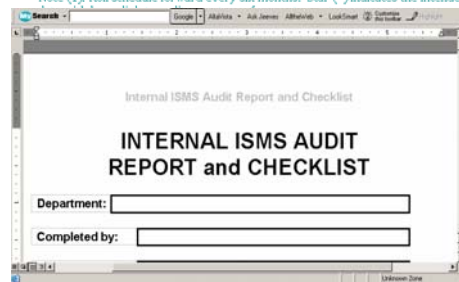
## INTERNAL ISMS AUDIT

### 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.





# Skeleton ISMS

- Initial management review schedule
- Procedure and checklist (for the meeting secretary, which also ensures compliance when completed)

## MANAGEMENT REVIEW

### Schedule

ISF Management Review Meetings are planned to take place every <<3 months/6 months/year appropriate>>, in accordance with the following schedule:

Plan	Jan 2004	Jul 2004	Jan 2005	Jul 2005	Jan 2006
ISMS Management Review Checklist					

## ISMS MANAGEMENT REVIEW CHECKLIST

Department:

Completed by:

Meeting date:

### Review Inputs

The following review inputs have been made available to the meeting:

Internal ISMS Audit reports and any other security audit reports



# Skeleton ISMS

- Procedure for dealing with preventive, corrective actions and improvements
- To-Do-List
- Record and document control section for all

## TO DO LIST

The table below lists those actions identified in the risk assessment that need to be taken to convert currently unacceptable risks into acceptable risks. Significant actions arising from ISMS Audits should also be included here. Add new entries to the TOP of the list and ensure that change control.

Reference	Action	Target Date	Completion Date
-----------	--------	-------------	-----------------

## RECORDS AND DOCUMENT CONTROL

### CONTROL OF ISMS RECORDS

ISMS records comprise:

- The Internal ISMS Audit Reports, completed checklists and the audit findings
- The minutes and completed checklists of the Management Review meetings
- The incident log <<GIVE REFERENCE>>
- <<LIST ALL OTHER RECORDS OF ACTIONS/EVENTS THAT COULD AFFECT THE EFFECTIVENESS OR PERFORMANCE OF THE ISMS, e.g. computer logs>>

Their purpose is to assist management in ensuring the effective operation of the ISMS in conformity to requirements of <<COMPANY>> and BS 7799-2:2002. The records should be particularly controlled to avoid fraudulent modification and to ensure that they remain legible. The controls needed for the identification, storage, protection, retrieval, and disposal of records should be documented in <<SAY WHERE - THIS OUGHT TO BE THE SAME FOR ALL DEPARTMENTAL RECORDS, e.g. REGISTRY>>. These controls take account of the requirements <<SAY WHAT THEY ARE, e.g. 'as described in xyz Act'>>.





# Conformance with Standard

	<b>INDEX</b>	
	<u>ISO/IEC 27001:2005 Requirement</u>	<u>Cross-reference</u>
<b>PLAN</b>		
Introduction		
Scope		
Policy		
Context		
<ul style="list-style-type: none"> <li>■ <a href="#">Assets</a></li> <li>■ <a href="#">Threats</a></li> <li>■ <a href="#">Impacts</a></li> </ul>		
<b>Risk Assessment</b>		
<ul style="list-style-type: none"> <li>■ <a href="#">RTP Index</a></li> </ul>		
<b>SOA</b>		
<b>DD</b>		
Metrics/Incidents		
Training/Awareness		
Other Manuals		
<b>CHECK/ACT</b>		
<ul style="list-style-type: none"> <li>■ <a href="#">Int Audit</a></li> <li>■ <a href="#">Mgt Review</a></li> <li>■ <a href="#">Improvement</a></li> </ul>		
<b>Records</b>		
<ul style="list-style-type: none"> <li>■ <a href="#">To-Do-List</a></li> <li>■ <a href="#">Impact Log</a></li> </ul>		
<b>Clear Footnotes</b>		
Skeleton Rev 6.0.0		
	<b>4 Information security management system</b>	
	<b>4.1 General requirements.....</b>	Introduction
	<b>4.2 Establishing and managing the ISMS</b>	
	<b>4.2.1 Establish the ISMS</b>	
	<ul style="list-style-type: none"> <li>a) <i>Define the scope of the ISMS.....</i> Scope</li> <li>b) <i>Define an ISMS policy.....</i> ISMS Policy                             <ul style="list-style-type: none"> <li>1) framework..... ISMS Policy</li> <li>2) business, legal, regulatory and contractual requirements..... ISMS Policy</li> <li>3) strategic organizational and risk management..... ISMS Policy</li> <li>4) risk evaluation criteria..... ISMS Policy</li> <li>5) management approval..... Introduction</li> </ul> </li> <li>c) <i>Define the risk assessment approach of the organisation.....</i> Risk Assessment</li> </ul>	

# CASE STUDIES

# Mauritius

- Civil service-wide roll out
- Treasury, Civil Status, Passport & Immigration, Social Security, GOC, ...
- Plus a civil service-wide ISMS
- Drive towards being a cyber island of quality
- Has significantly increased security awareness – essential for a cyber-culture
- Just under 4 months from start to finish

**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: 1865 km<sup>2</sup>
- Population: 1.2 m
- Multi-cultural society (64% Indian, 31% African & European, 3% Chinese)
- Free & compulsory education
- Bilingual (English, French)
- 90% literacy rate
- Free health services
- Sub-Tropical Climate (19°C - 29°C)

# Middle East

- Telecommunications \* Petroleum
- Scope – just the IT department
- Need to take care because the ISMS is not responsible for everything
- 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
- Telecomm – 3 weeks to build
- Petroleum – 8 weeks to build



# Eastern Europe

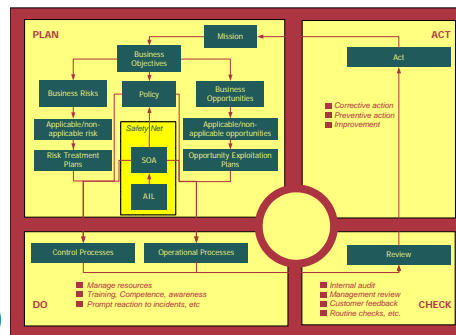
- Air traffic control



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

# United Kingdom

- Fully integrated management system
- ISO 9001
- ISO/IEC 27001
- Finance
- Health and Safety
- Sales and Marketing (opportunity exploitation)
- ISO/IEC 27001 component built in 6 days



# SUMMARY

## Summary

- Different strategies – go with what you have today is the best
- Fast track method works well
  - Won't forget anything
  - Tell it like a story
  - To-Do-List for managing continual improvement, etc
  - Scalable
  - Build times: 2 few days to a few weeks
- But different organisations pose different challenges
- Built on world wide experience in many contexts

Covers every requirement of ISO/IEC 27001

---

## Implementing ISO/IEC 27001



Computer Security Week 30<sup>th</sup> November 2006

*Any Questions?*



Certificate No. IS 85916



Certificate No. FS 30710

*Dr. David Brewer*  
*Gamma Secure Systems Limited*  
*[www.gammassl.co.uk](http://www.gammassl.co.uk)*