Implementing ISO/IEC 27001

Computer Security Week 30th November 2006

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

Certificate No. IS 85916 Certificate No. FS 30710

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

The ISMS Standards

ISO/IEC 27001

Information Security Management Systems - Requirements

ISO/IEC 17799

- Security Policy
- Organising Security
- Asset Management
- Human Resources
- Physical and Enviro
- Commu ications
- Access Co
- Information and Maintenance
- Information S
- Business Cont
- 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

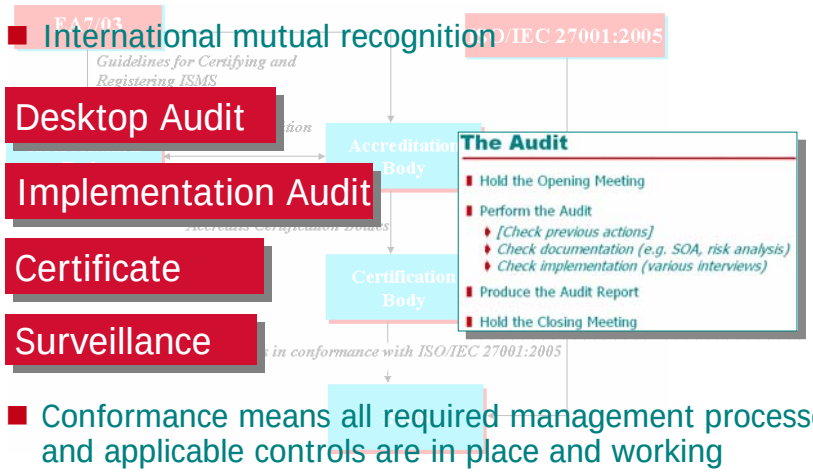
- International mutual recognition

Desktop Audit

Implementation Audit

Certificate

Surveillance



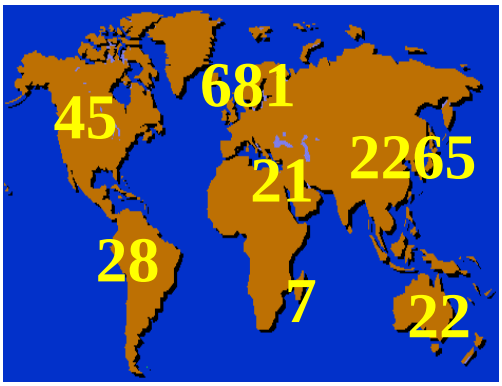
- Conformance means all required management processes and applicable controls are in place and working

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



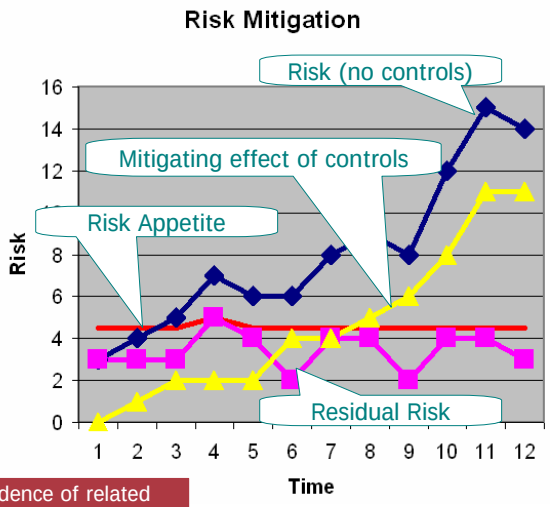
ISMS Registrations by Continent

5 November 2006

Implementation Strategies

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

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

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

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*

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

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

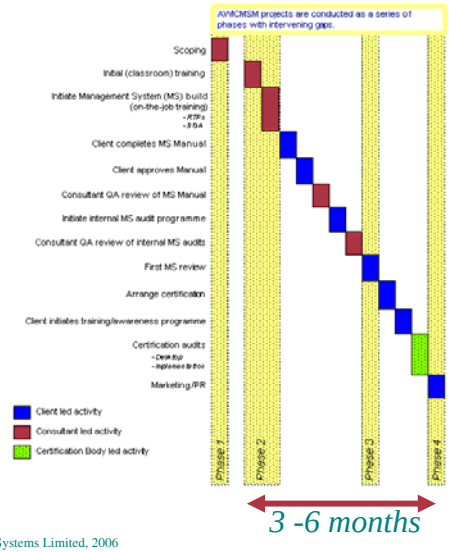
The Fast Track Approach

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

[Strategies 2 and 3]

Overview

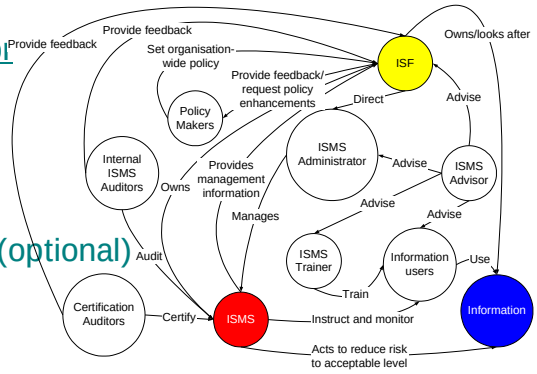
- Classroom/on-the-job training, throughout at least one PDCA cycle
- Role Model
- To-Do-List concept
- Overarching/subordinate ISMS
- Event-impact RTPs
- Skeleton ISMS
- Integrate with existing internal control structures
- Marshal existing procedures/ records



Role Model

Role Model

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



The "To-Do-List" Concept

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… p…
- B… b…
- A…
- M…

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:

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

©Gamma Secure Systems Limited, 2006

Which Means ...

- Management standards, including ISO/IEC 27001 insist that the man
- B
- A
- M

- **Can have entries in progress**
- **Entries will be corrective, preventive or improving in nature**
- **There should be evidence that any risk is being**

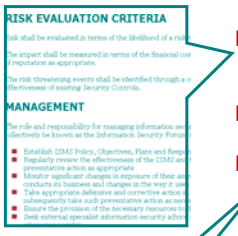
The To-Do-List

Reference	Action		
MSR Actions 19.11/ 19.13	Add G4 and G5 See CRF.		
MSR Action 19.3	Produce new H		
New ISMS Stand	ISO/IEC 2700		
			1. Presented for review
	tice; and the MS records.	051130	As at 051103:

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

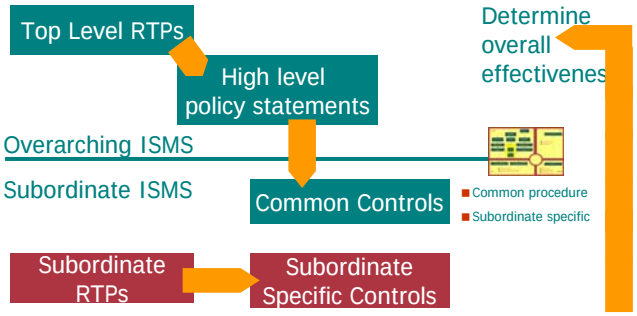
ISMS Policy



- 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*"

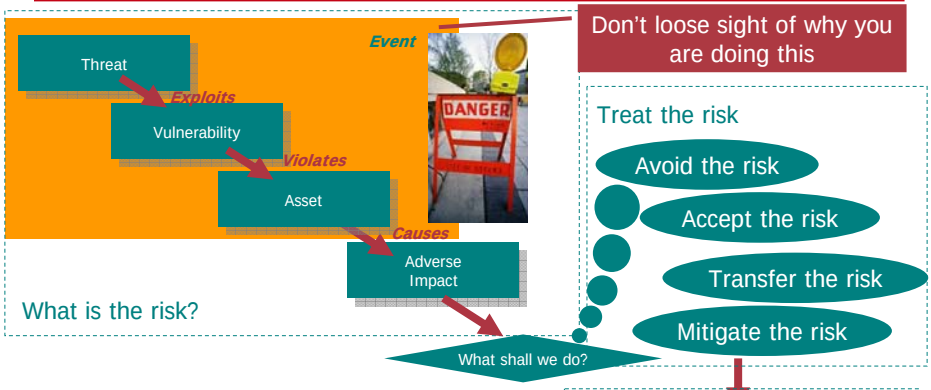
Overarching & Subordinate ISMSs

- Hierarchy of ISMSs
- Superior set policy for subordinate



Event-driven Risk Treatment Plans

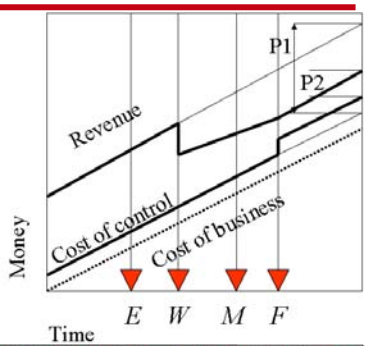
Risk Treatment Plans



- 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 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	

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

Covers all 133 controls

- 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

Example RTP (1)

- Acts of God for a library (early 1900s – no IT)
- Threat agents: fire, flood, cyclone, vermin
- Assets: building, staff, books
- Impacts: inability to carryout some or all of the business of being a library

Example RTP (2)

- Can we prevent the event?
  - *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 risk*
  - *Cyclone? No*
  - *Vermin? Not cost effective*

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*

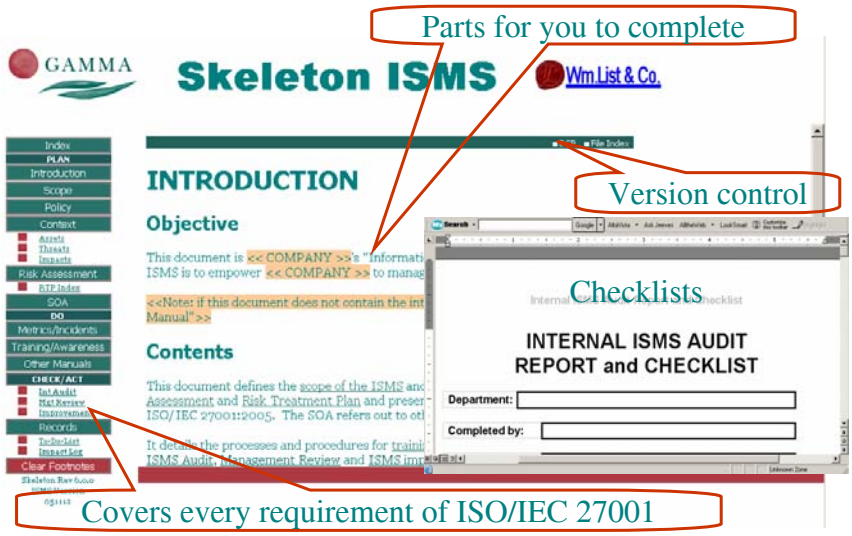
Example RTP (4)

- 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
- THE END OF THE STORY

Skeleton ISMS



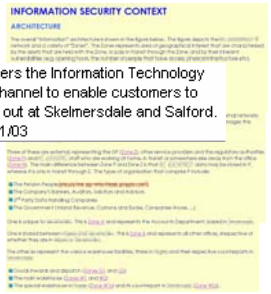
Skeleton ISMS

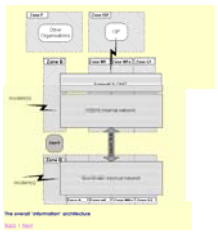
- Built-in facility for document control
- Space to define scope and context
- Prototype policy
- Provision for RTPs
- Virtually complete SOA (with built-in hyperlinks to policy statements and standard events)
- Facility for including training and awareness
- Internal audit proforma and checklist
- Management 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





Skeleton ISMS

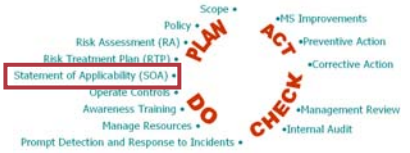
- There is a prototype ISMS policy
- Most words are there to ensure compliance with the standards
- Some to simplify production of the SOA
- Customise with reference to relevant corporate policies

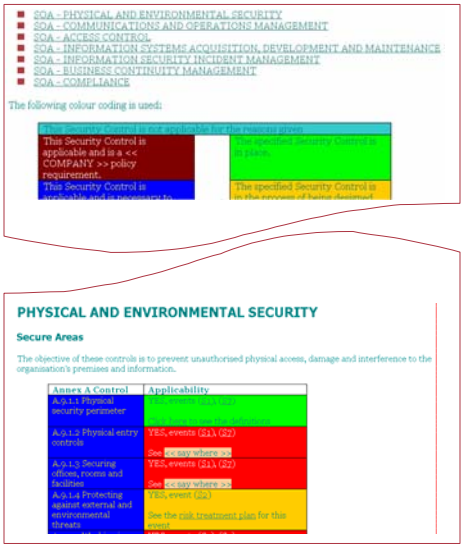
Skeleton ISMS

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

Skeleton ISMS

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



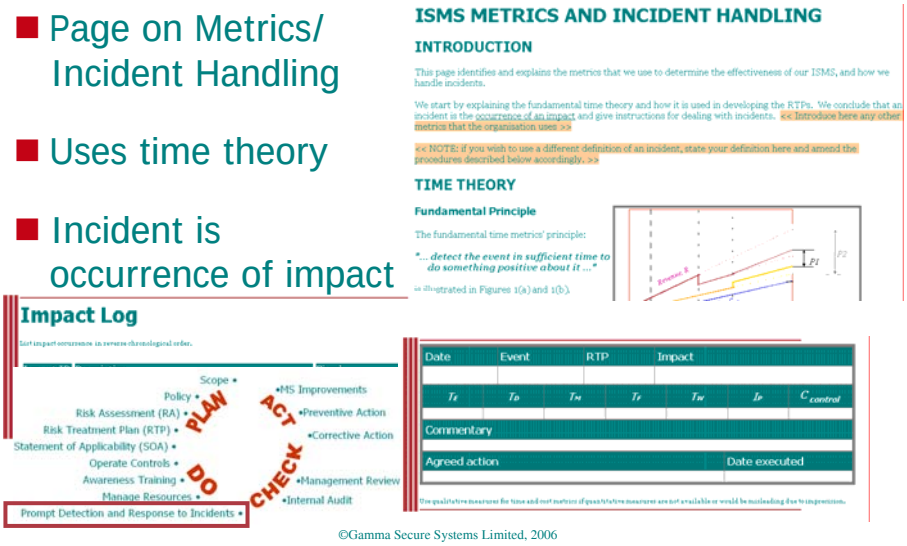


Skeleton ISMS

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

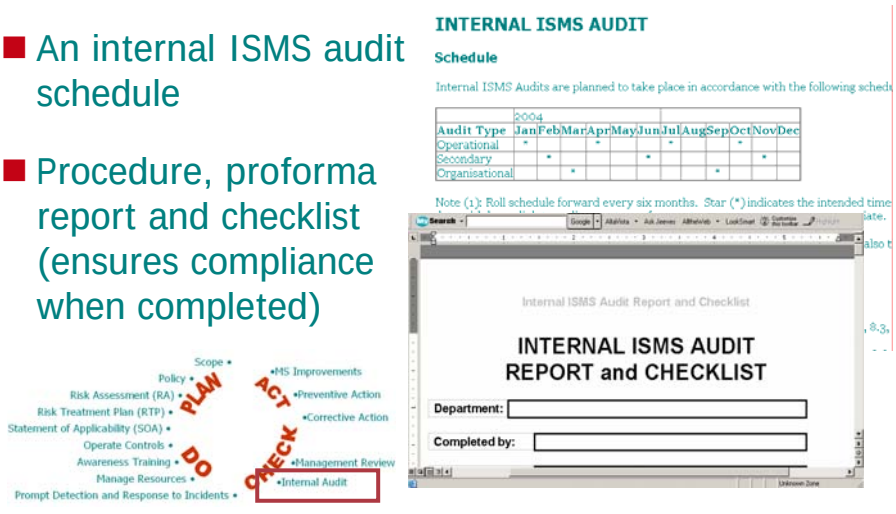
Skeleton ISMS

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



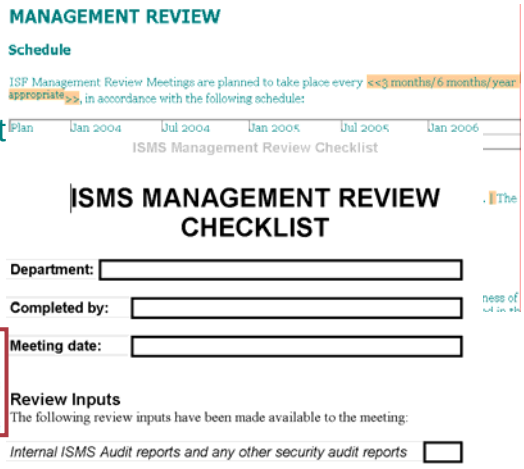
Skeleton ISMS

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



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:

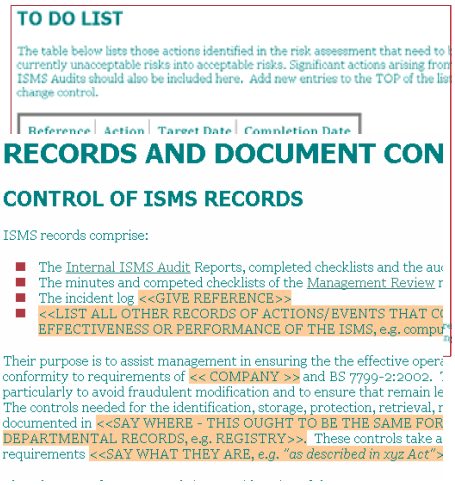
Review Inputs

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
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 lis
change control.

Reference | Action | Target Date | Completion Date

RECORDS AND DOCUMENT CON

CONTROL OF ISMS RECORDS

ISMS records comprise:

- The Internal ISMS Audit Reports, completed checklists and the au
- The minutes and competed checklists of the Management Review r
- The incident log <<GIVE REFERENCE>>
- <<LIST ALL OTHER RECORDS OF ACTIONS/EVENTS THAT C
EFFECTIVENESS OR PERFORMANCE OF THE ISMS, e.g. compu

Their purpose is to assist management in ensuring the the effective opera
conformity to requirements of << COMPANY >> and BS 7799-2:2002.
particularly to avoid fraudulent modification and to ensure that remain le
The controls needed for the identification, storage, protection, retrieval, r
documented in <<SAY WHERE - THIS OUGHT TO BE THE SAME FOR
DEPARTMENTAL RECORDS, e.g. REGISTRY>>. These controls take a
requirements <<SAY WHAT THEY ARE, *e.g. "as described in xyz Act"*>

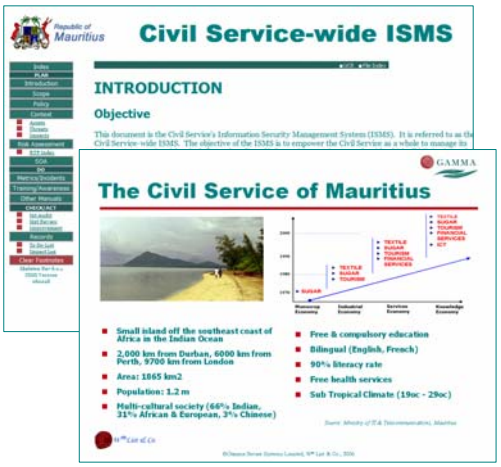
Conformance with Standard

INDEX

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



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

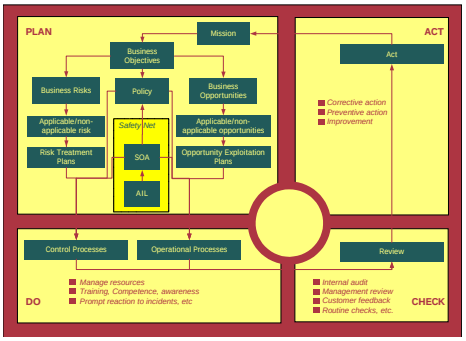
Eastern Europe

- 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)

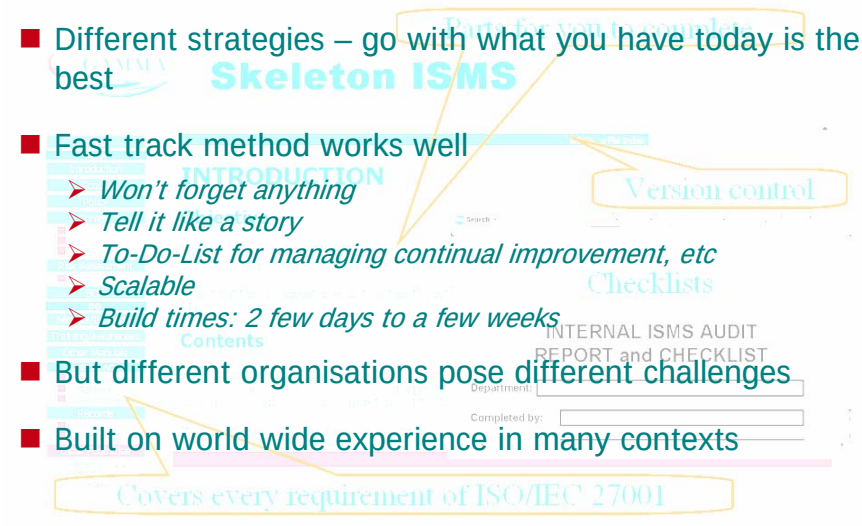


- ISO/IEC 27001 component built in 6 days

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



Implementing ISO/IEC 27001

Computer Security Week 30th November 2006

Any Questions?

Certificate No. IS 85916

Certificate No. FS 30710

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