GAMMA

ISO/IEC 27003

(ISMS Implementation Guidelines)

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

BSI REGISTERED UKAS INFORMATION SECURITY MANAGEMENT 003
Certificate No. IS 85916

BSI REGISTERED UKAS QUALITY MANAGEMENT 003
Certificate No. FS 30710

Introduction

- What is ISO/IEC 27003?
- ISO meetings – Melaka, 2010
- Case Study
  - *Getting management buy-in*
  - *Design the ISMS*
  - *Security requirements*
  - *Assessing risks*
- Conclusions

100
1169
4960
70
66
7
30

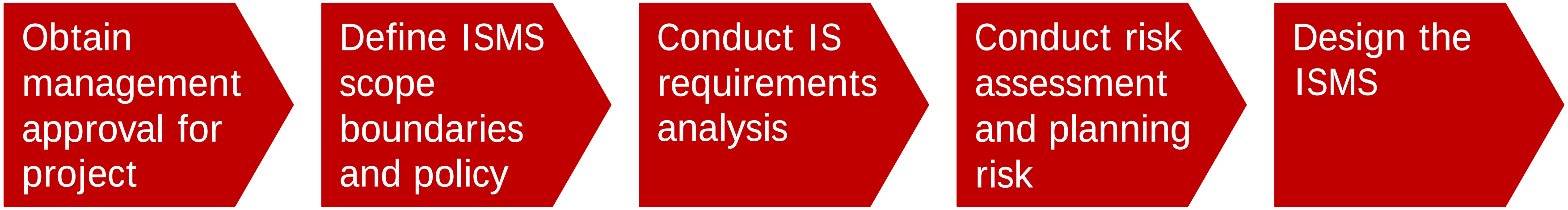
What is ISO/IEC 27003?

Purpose and philosophy

- Guidance document
- Too recent / narrow to be best practice
- Provide practical guidance in developing an *implementation plan* for an ISMS
  - *Prepare plan*
  - *Define project structure*
  - *Gain management approval*
  - *Recognise critical activities*
- Does not cover operational activities

Structure of the standard

- Usual preamble
- 5 'project' phases



Obtain management approval for project

Define ISMS scope boundaries and policy

Conduct IS requirements analysis

Conduct risk assessment and planning risk

Design the ISMS

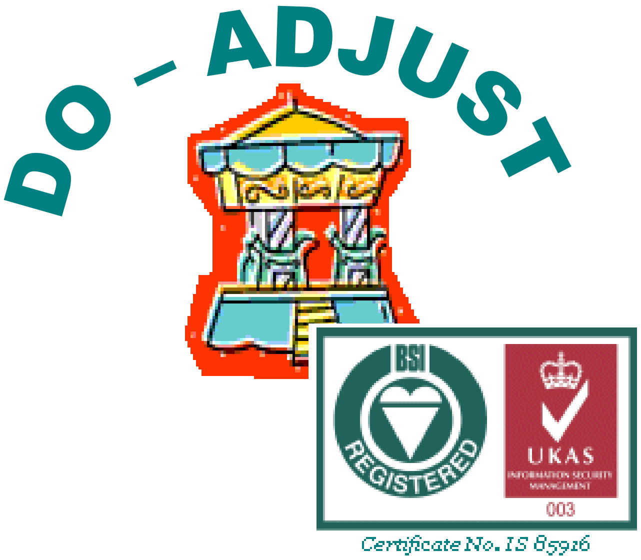
- Supporting annexes:
  - *Activities re 27001; roles & responsibilities*
  - *IA planning; policy structure*
  - *Planning of monitoring and measuring*

Is it any good?

- Yes, but ...
- Remember:
  - *It is the operational ISMS that is certified, not the project*
  - *Many different ways to run a project*
  - *Standard assumes a particular context which may not be true for you*

Why a project?

- Operationally an ISMS is more like a carousel:

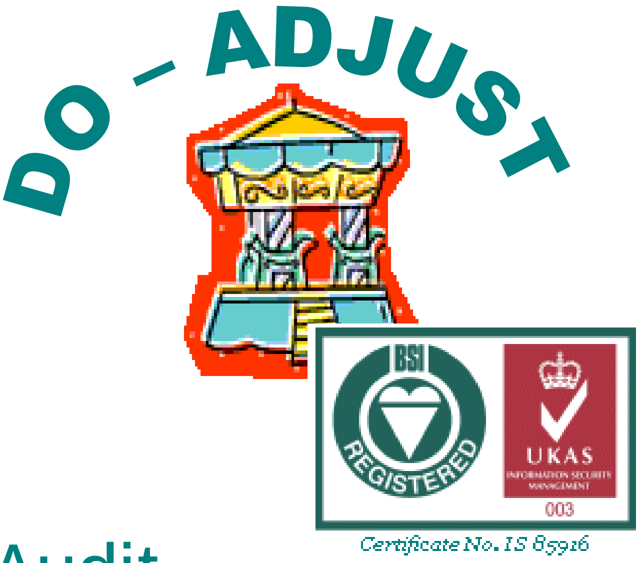


Why a project?

- For a start-up it really is a blank sheet of paper
- But for an established organisation it *will* exist
- Although it may not conform to ISO/IEC 27001
- You must make it so

Why a project?

- The project is to make your ‘ISMS’ conformant to ISO/IEC 27001
- Start-up: create from scratch
- Established: reverse engineer
- Completes with certification
- It will be, however, be fully operational before the Initial Audit



ISO meetings – Melaka, 2010

ISO meetings, Melaka 2010

- ISO SC 27 meets twice a year
- Last one (April) in Melaka, Malaysia
- This standard – WG1
- Just published so revision in a few years

- BUT, a wealth of implementation is being exposed
- We need to get it written down

Case Study

Case study – ground rules

- Draw together a variety of experiences
- Large organisations: Mauritius and elsewhere
- Small-medium organisations
- Project and operational perspectives

Proper Integrated MS, using IMS-Smart Architecture, covering 9K & 27K, Exlayer has BS25999 as well

Gamma Secure Systems

Certificate No. FS 30710

Certificate No. IS 85916

Exlayer (London)

FS538573 ISO9001:2008

IS538574 ISO27001:2005

Management buy-in

- Absolutely essential
- Create ownership from the outset
- Must want a management system to manage the business more effectively, not a certificate
- Whether a business case is required depends on many factors, often *outside* your control

Project organisation

- All three are cars but are designed with different operational objectives in mind
- Don’t worry about documentation/records, it’s the people that count
- If the Jag was to be chauffeur-driven it would have a longer wheel base
- A management system is a managing capability, not just a documentation/record set
- The project must deliver that managing capability
- Therefore it is the operational people that need to be trained
- Ideally they should be involved in the build

Security requirements

- In *99.99%* of cases you are reverse engineering conformance out of existing out of an existing context
- SOA is a good place to start – just document what is being done
- To do otherwise you will build a Vasa:

- Instead build bubble cars and grow them into spaceships

Continual improvement (section 8 of 27K)

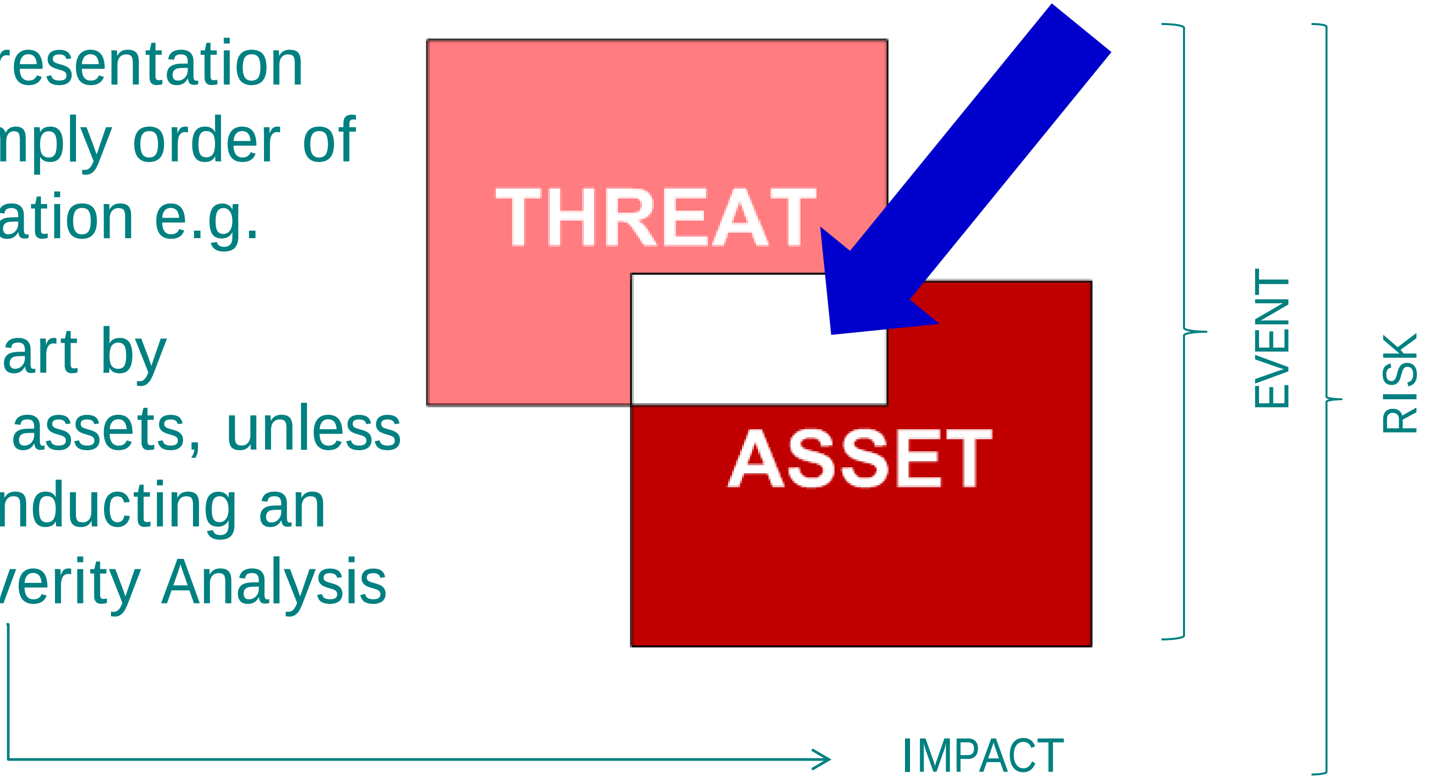
Risk appetite

- If analysis exposes unacceptable risks, they must be treated immediately:
  - *Knowingly accept the risk (and minute it)*
  - *Avoid risk by ceasing operations (in that area)*
  - *Introduce/modify controls to:*
    - ❑ *Reduce frequency/likelihood of occurrence*
    - ❑ *Reduce severity of consequence*
- Remember you are exposed throughout the time it takes to treat the risk
- All applicable controls must be operational

Risk assessment

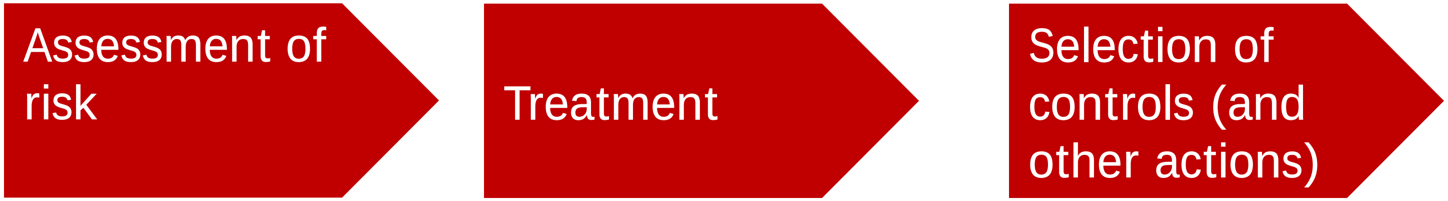
- ISO/IEC 27001 is a specification
- Order of presentation does not imply order of implementation e.g.
- DO NOT start by identifying assets, unless you are conducting an Impact Severity Analysis

Vulnerability associated with the asset that the threat has the capability of exploiting



Risk assessment/ treatment

- Remember:

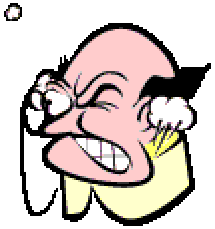

Assessment of risk

Treatment

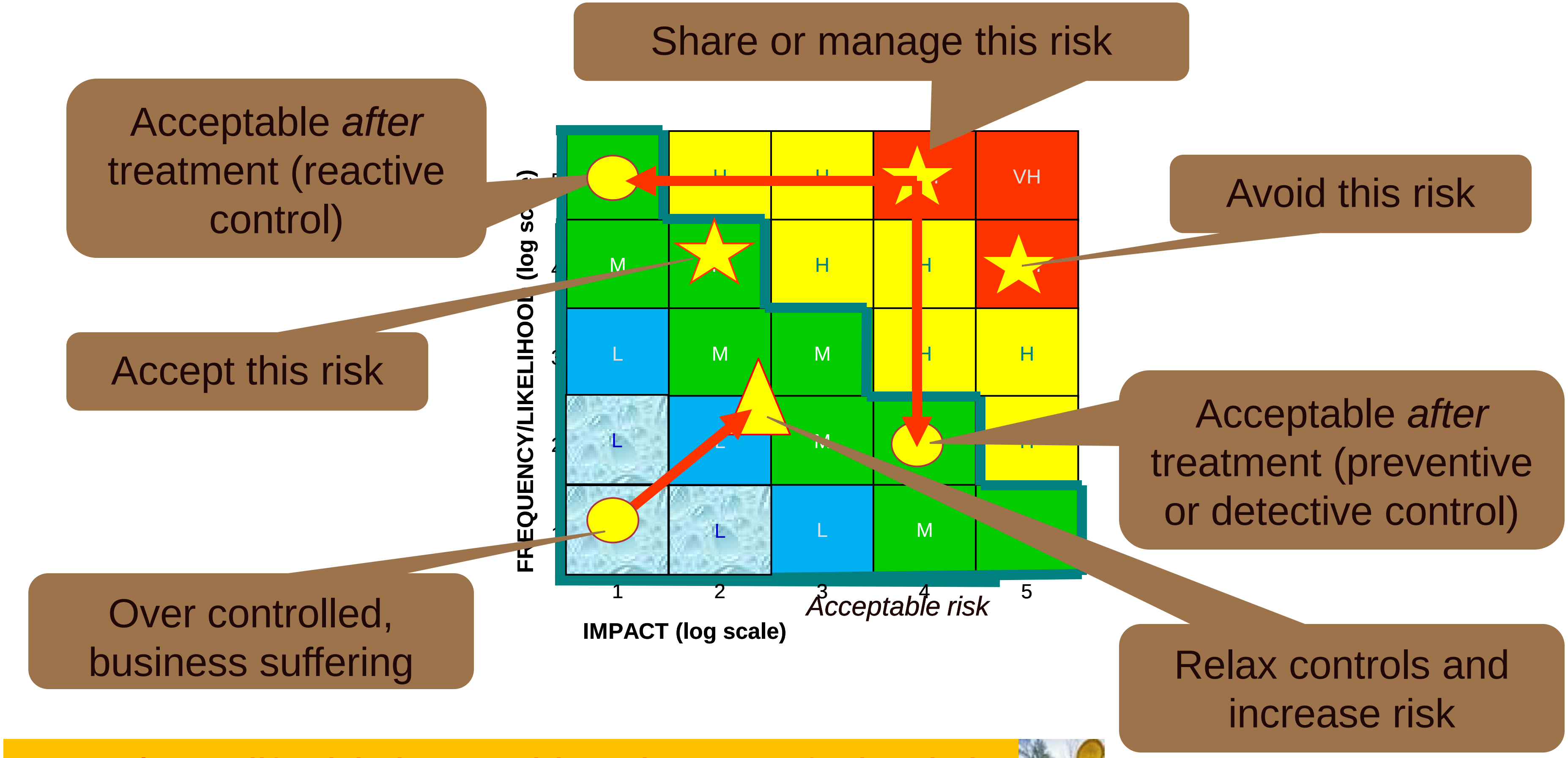
Selection of controls (and other actions)

- If you are bogged down in numbers and/or management does not understand it, something is seriously wrong

“I spent £25,000 on a risk assessment. The trouble is, my MD doesn’t understand any of it”



Risk treatment



Share or manage this risk

Acceptable *after* treatment (reactive control)

Avoid this risk

Accept this risk

Acceptable *after* treatment (preventive or detective control)

Over controlled, business suffering

Relax controls and increase risk

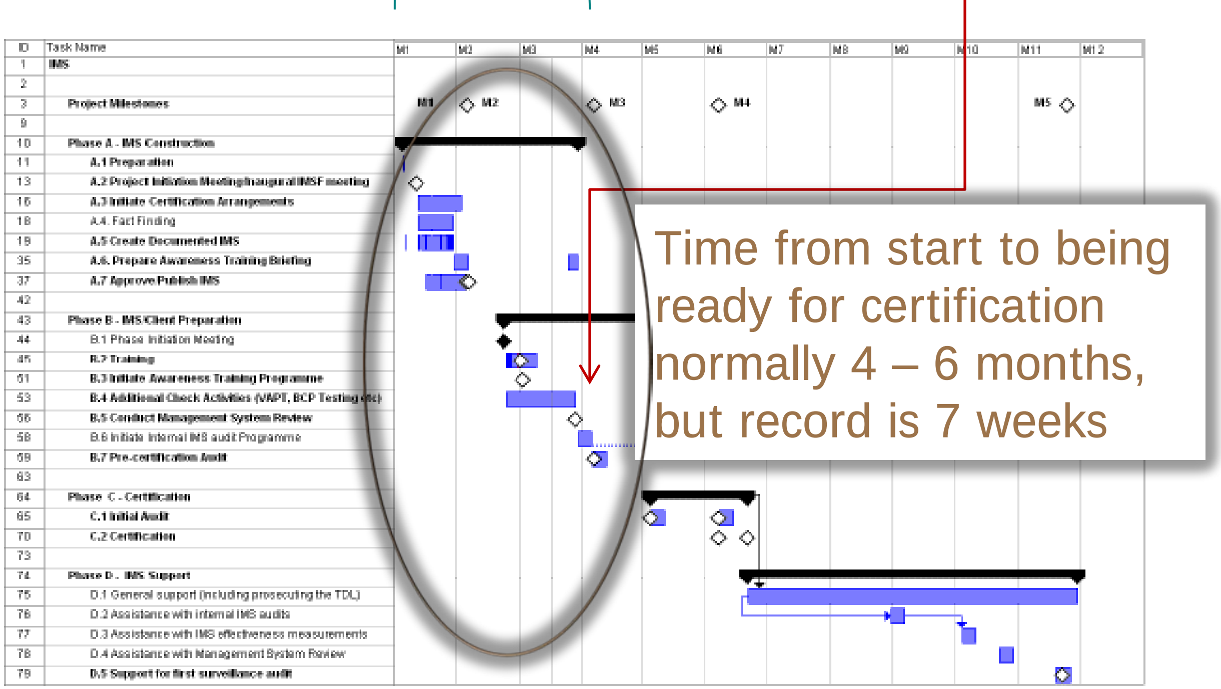
Controls modify risk (ISO Guide 73). Most of what is in ISO/IEC 27002 are NOT controls. At best they are parts of controls. Some are actually groups

Project plan

- Here's mine

Scope of 27003

ISMS operational about here



ID	Task Name
1	IMS
2	
3	Project Milestones
9	
10	Phase A - IMS Construction
11	A.1 Preparation
13	A.2 Project Initiation Meeting/Inaugural IMSF meeting
16	A.3 Initiate Certification Arrangements
18	A.4. Fact Finding
19	A.5 Create Documented IMS
35	A.6. Prepare Awareness Training Briefing
37	A.7 Approve/Publish IMS
42	
43	Phase B - IMS/Client Preparation
44	B.1 Phase Initiation Meeting
45	B.2 Training
51	B.3 Initiate Awareness Training Programme
53	B.4 Additional Check Activities (VAPT, BCP Testing etc)
56	B.5 Conduct Management System Review
58	B.6 Initiate Internal IMS audit Programme
59	B.7 Pre-certification Audit
63	
64	Phase C - Certification
65	C.1 Initial Audit
70	C.2 Certification
73	
74	Phase D - IMS Support
75	D.1 General support (including prosecuting the TDL)
76	D.2 Assistance with internal IMS audits
77	D.3 Assistance with IMS effectiveness measurements
78	D.4 Assistance with Management System Review
79	D.5 Support for first surveillance audit

Time from start to being ready for certification normally 4 – 6 months, but record is 7 weeks

- See http://www.ims-smart.com/PIPS/index.php

Conclusions

Conclusions

- ISO/IEC 27003 addresses an important component of creating an ISMS managing capability
  - *Does not address operational issues*
  - *Assumes a particular paradigm*
  - *Perhaps does not go far enough*
- Is it helpful – Yes
- Is it a substitute for an expert - No

ISO/IEC 27003

The Millennium Lovers, Port Louis, Mauritius

(ISMS Implementation Guidelines)

Any Questions?

Certificate No. IS 85916

Certificate No. FS 30710