



# Integrated Management Systems – an *IMS-Smart* productised IP-led service

Dr. David Brewer, *FBCS, MIOD*



*Certificate No. IS 85916*



*Certificate No. FS 30710*

# Agenda

---

- Introduction
- The *IMS-Smart* "productised IP-led service"
  - *Overview*
  - *Under the hood*
- Benefits
- Summary

---

# INTRODUCTION

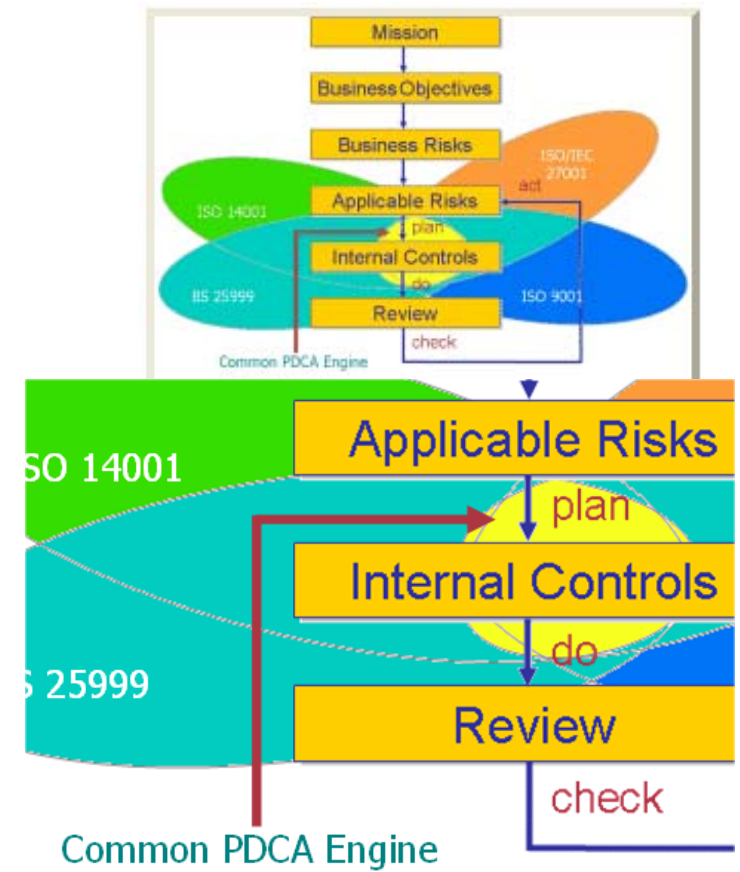
# What is *IMS-Smart*?

---

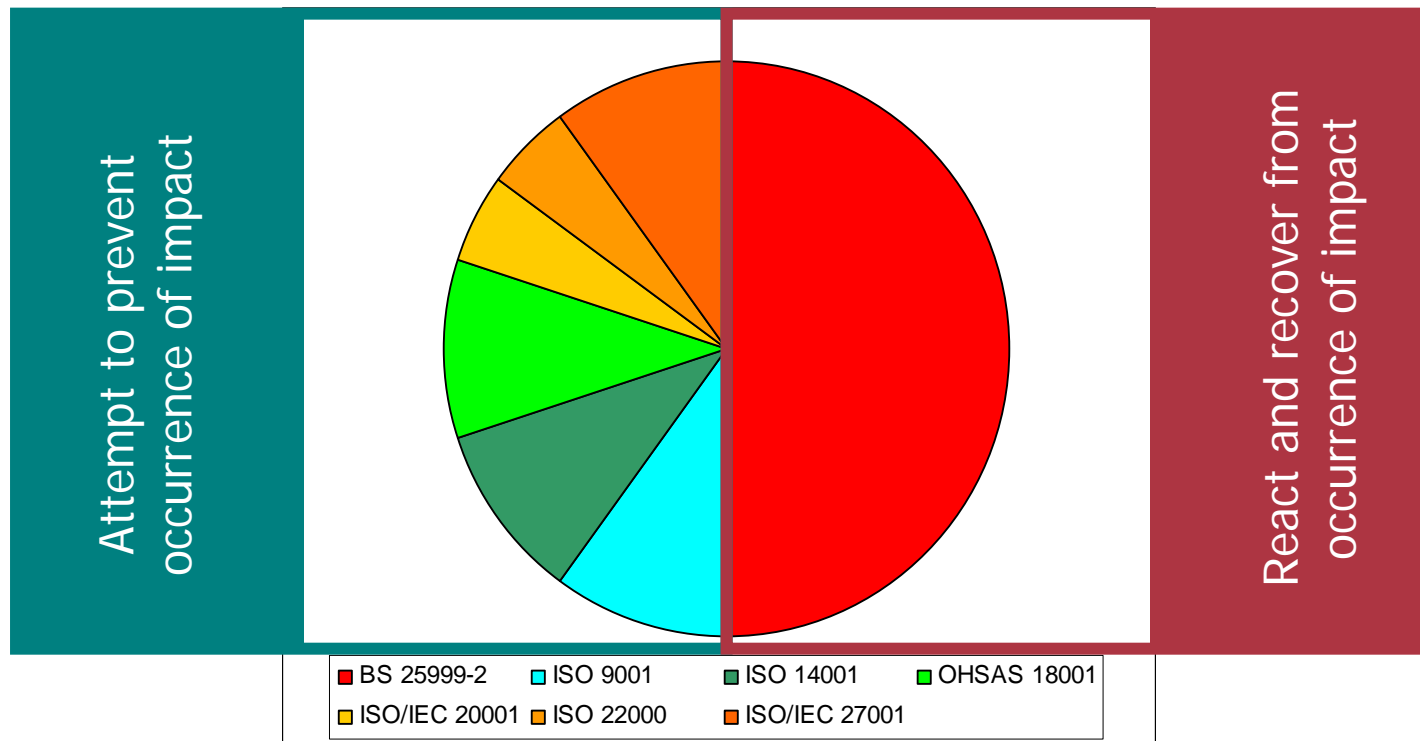
- IMS-Smart is a methodology with associated technology and productised IP-led services, including training for creating integrated management systems
- It consists of a *methodology, framework, architecture, service, training and technology*
- It is more than just ISO
- It is key to sound internal control and corporate governance

# Management system standards

- Management system = management capability
- Means to establish, police and improve your system of internal control
- Internal control is the means by which an organisation marshals its resources to achieve its objectives:
  - *Processes for doing the job*
  - *Processes for doing the job the way the boss wants it done*



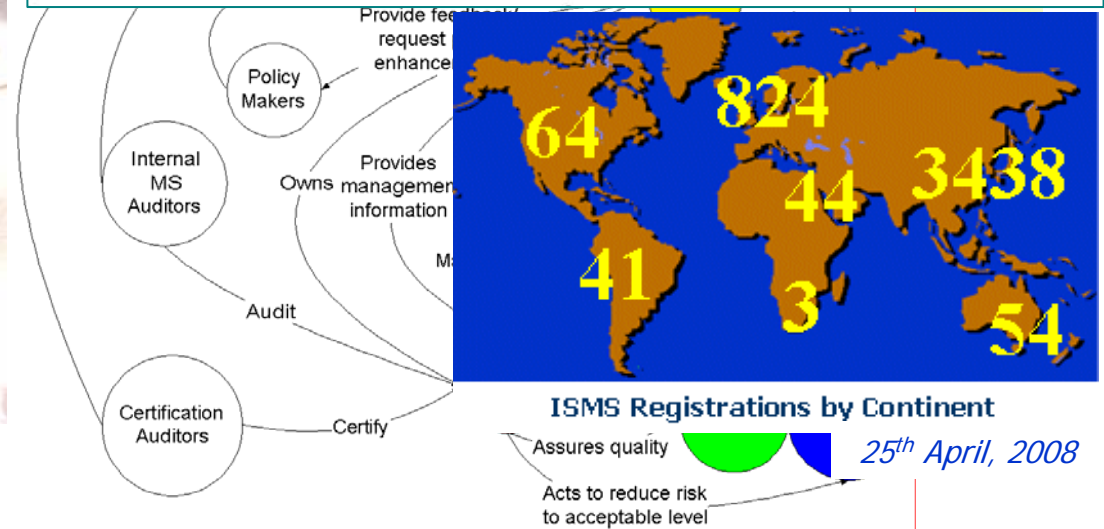
# Enter BS 25999



- BS 25999 has to deal with the triggering events of all other management systems plus one

# Market need

- Lots of management system standards
- Companies need/want to be certified
- But too many systems, audits etc
- Solution is an integrated management system
- One MS, one audit, many standards
- BSI call it the shape of the future



# Productised IP-led service

---

- Delivered by Gamma and its partners
- Created by Dr. David Brewer, a co-author of BS 7799-2 (now ISO/IEC 27001)
- Methodology for constructing and using IMS
- Encompasses Brewer-List "Time" theory (for *measuring effectiveness of internal control*)
- Tried and tested



ISO/IEC 27001

ISO 9001

BS 25999

# Tried and tested – an example

- Rolling out ISMS across all ministries and departments for Government of Mauritius

## Overarching ISMS at Cabinet Office level



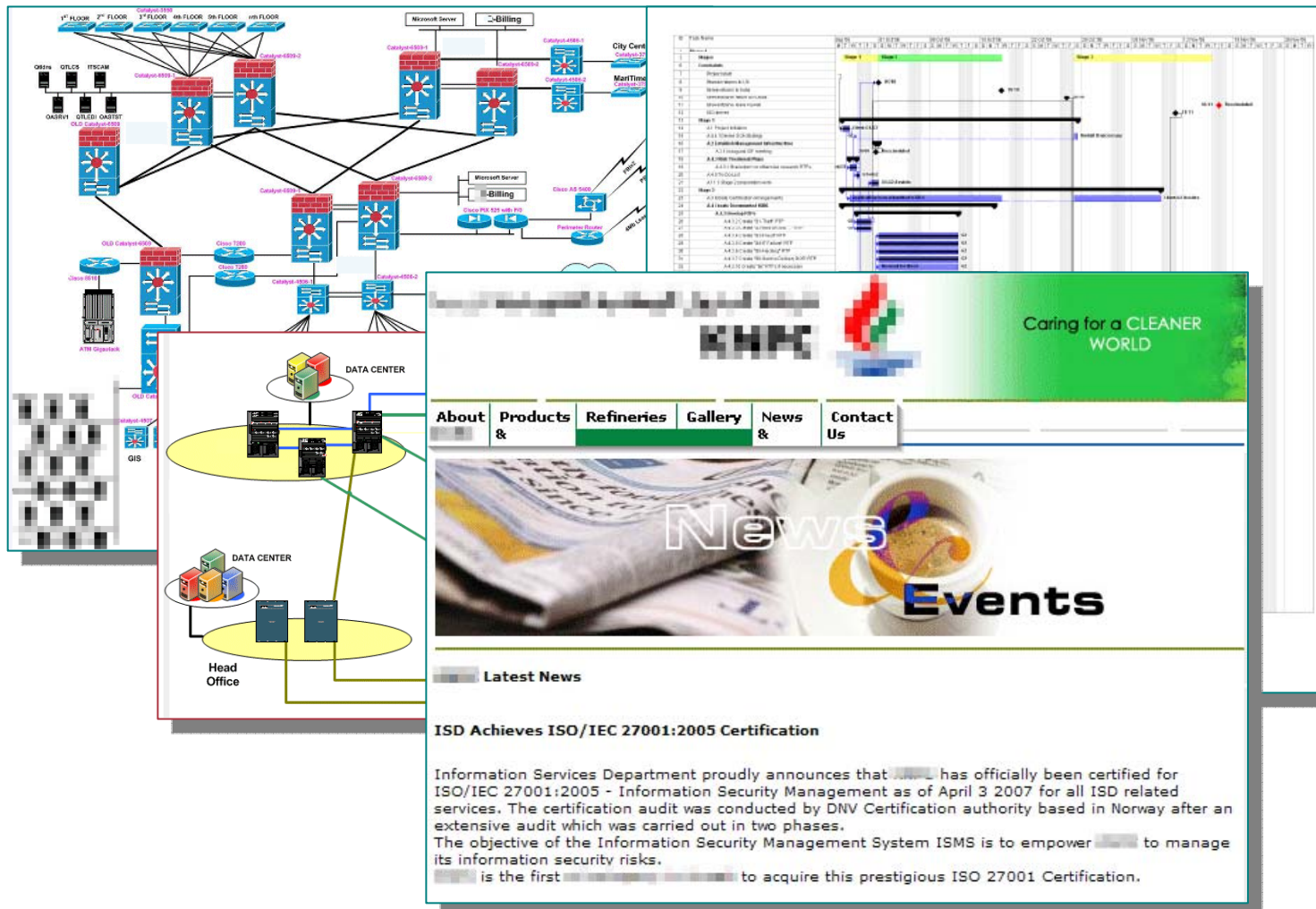
*Consultants  
trained  
selected civil  
servants to  
do the work*

Template ISMS allows promulgation of civil-service wide policies/procedure to subordinate ISMSs



Subordinate ISMS in Ministries (and various departments, e.g. Treasury, Passport & Immigration, Civil Status, Social Service, Government Online Centre, ....)

# Tried and tested – more examples



The image displays a complex network architecture and a corporate website. On the left, a network diagram shows multiple floors (1st to 6th) with various servers and switches. A central 'Microsoft Server' and 'Billing' system are connected to several 'Catalyst' switches. A 'Data Center' is also shown with multiple servers. On the top right, a network configuration table lists various parameters and settings. On the bottom right, a screenshot of a corporate website is shown, featuring a navigation menu with 'About & Products', 'Refineries', 'Gallery', 'News & Events', and 'Contact Us'. The 'News & Events' section is highlighted, showing a news article titled 'ISD Achieves ISO/IEC 27001:2005 Certification'.

**News & Events**

**Latest News**

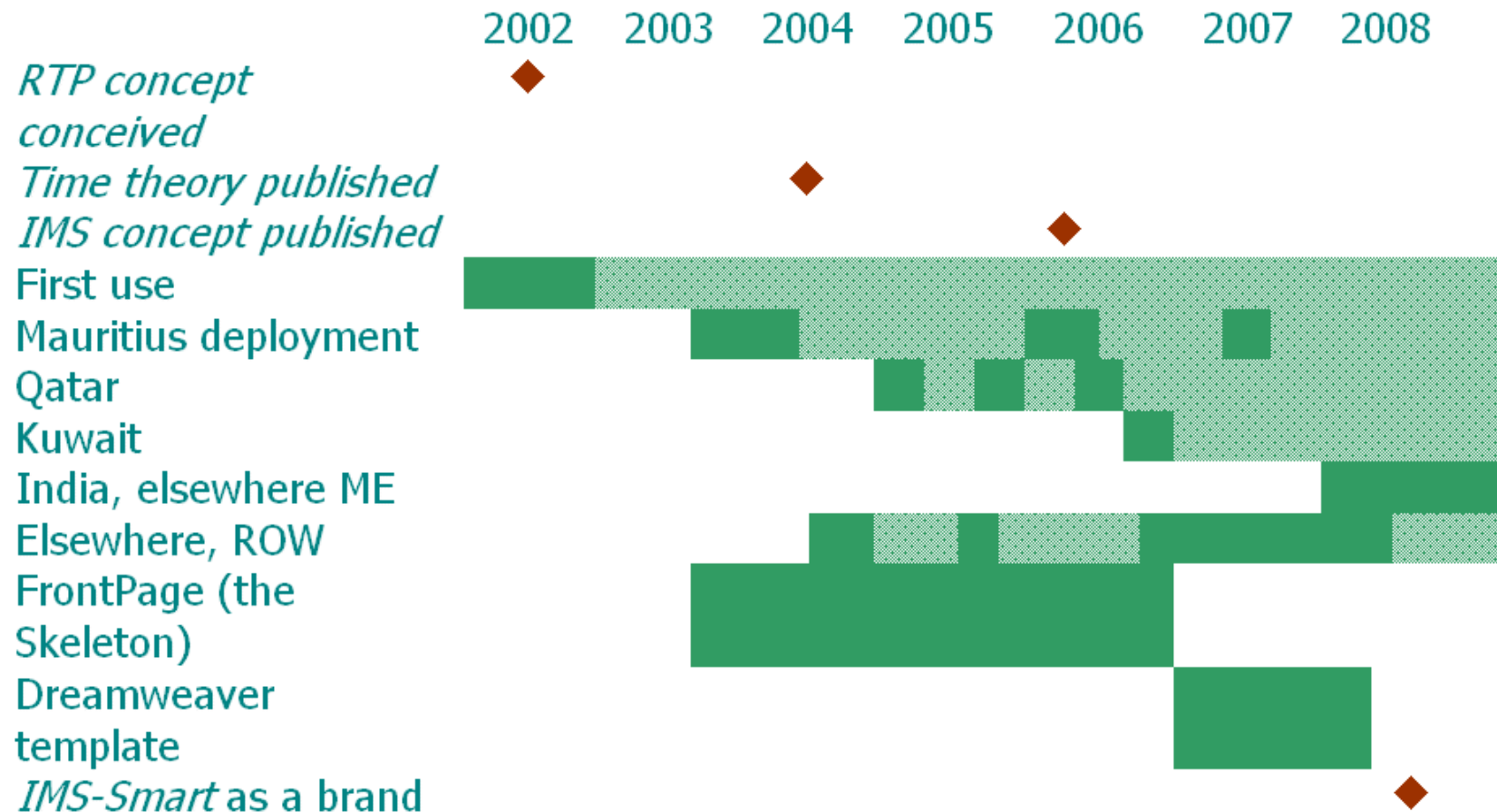
**ISD Achieves ISO/IEC 27001:2005 Certification**

Information Services Department proudly announces that ISD has officially been certified for ISO/IEC 27001:2005 - Information Security Management as of April 3 2007 for all ISD related services. The certification audit was conducted by DNV Certification authority based in Norway after an extensive audit which was carried out in two phases. The objective of the Information Security Management System ISMS is to empower ISD to manage its information security risks. ISD is the first company to acquire this prestigious ISO 27001 Certification.

---

# THE *IMS-Smart* "PRODUCTISED IP-led SERVICE"

# IMS-Smart history

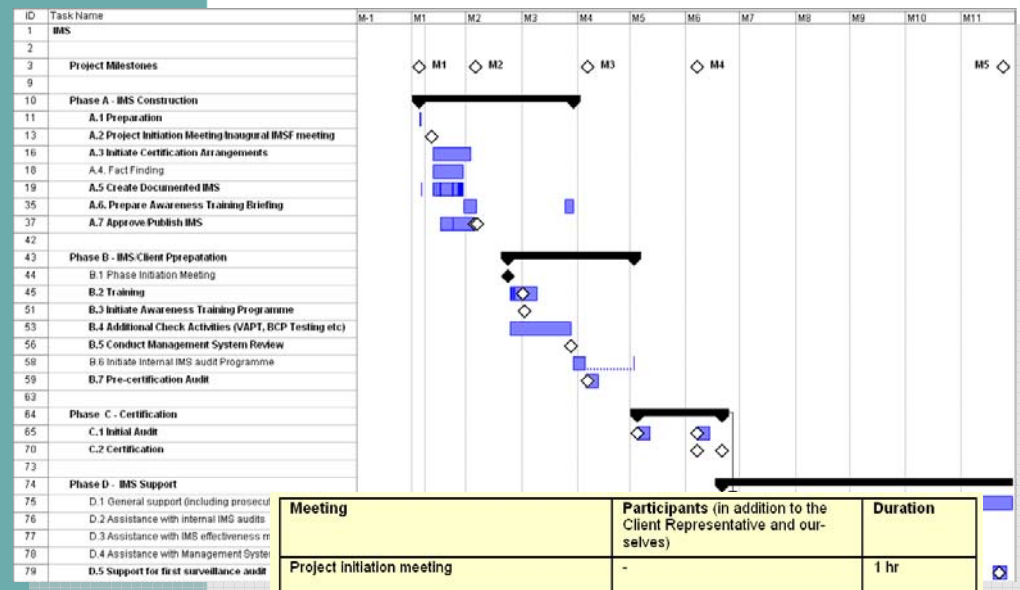


# IMS productised IP-led service

- Product specification
- Near identical IMS
- Pre-defined plan
- ISO/IEC 27001, ISO 9001, BS25999, etc
- All at once or as upgrades



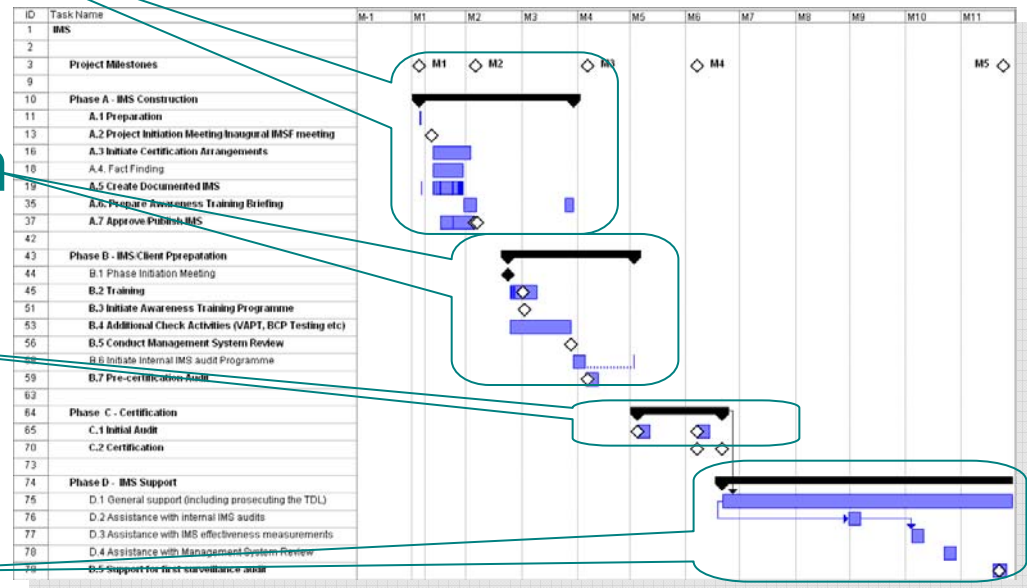
**IMS**  
Productised  
IP-led Service  
Specification



Meeting	Participants (in addition to the Client Representative and ourselves)	Duration
Project Initiation meeting	-	1 hr
Inaugural Integrate Management System Forum (IMSF) meeting	IMSF	2 hrs
IMS administrator training	IMS Implementers/ Administrators	0.5 days
IMSF Meeting to approve IMS	IMSF	1 hr
Phase Initiation meeting	-	1 hr
Phase B training	Internal IMS Auditors	1 day
On-the-job audit training (desktop)	Internal IMS Auditors	2-3 hrs
On-the-job audit training (implementation audits)	Internal IMS Auditors	1 hr per audit.
IMSF training	IMSF, Internal IMS Auditors	2 hrs
Give Awareness Seminars (one per standard)	Everyone within scope of the IMS and everyone within your organisation that you wish to invite	1 hr each
Conduct Management System Review	IMSF	3 hrs
Pre-certification audit	As agreed with the Certification Body	

# Phases

- Construct the IMS
- Prepare it and the client for certification
- Certification
- Support through the first surveillance audit

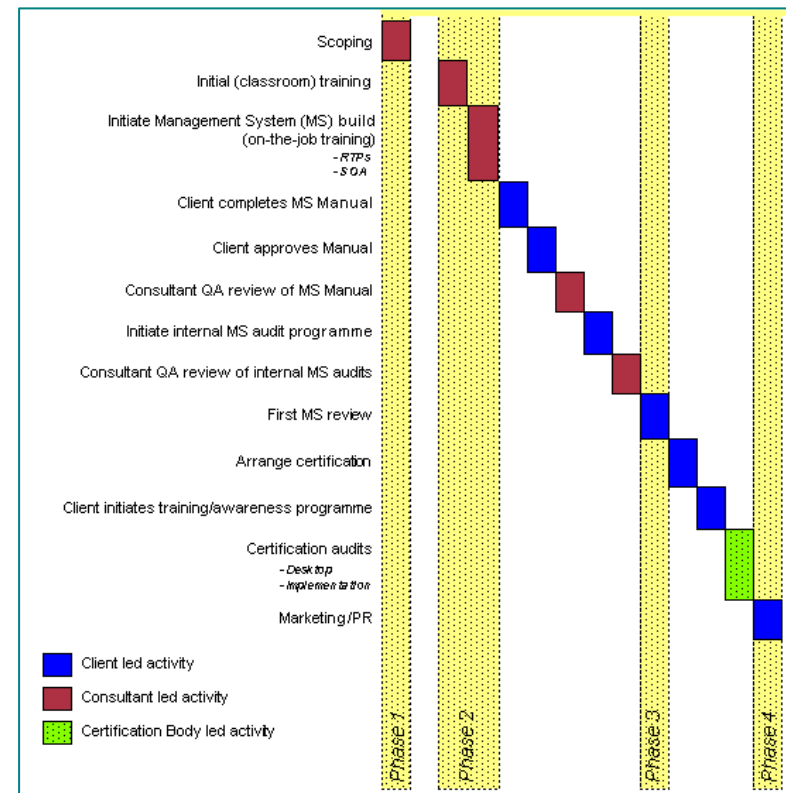


# Under the hood

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

- Solid theoretical foundation
- Event-impact RTPs
- Opportunity-benefit OEPs
- Role Model
- To-Do-List concept
- *IMS-Smart*
- Overarching/subordinate IMS

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



Project plan as actually used in Mauritius


3-6 months

# Solid theoretical foundation

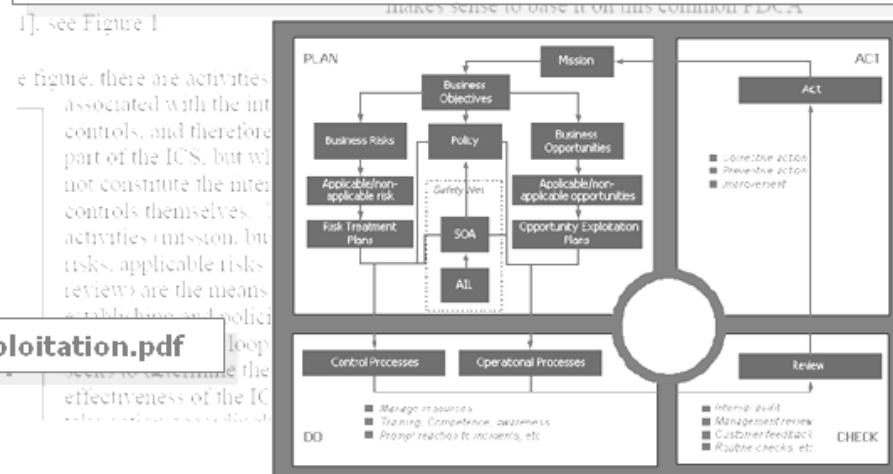
## Common PDCA framework

- Introduction
- Alternative Ideas Lists (AILs)
- Process specifications (e.g. for IMP, BCP)

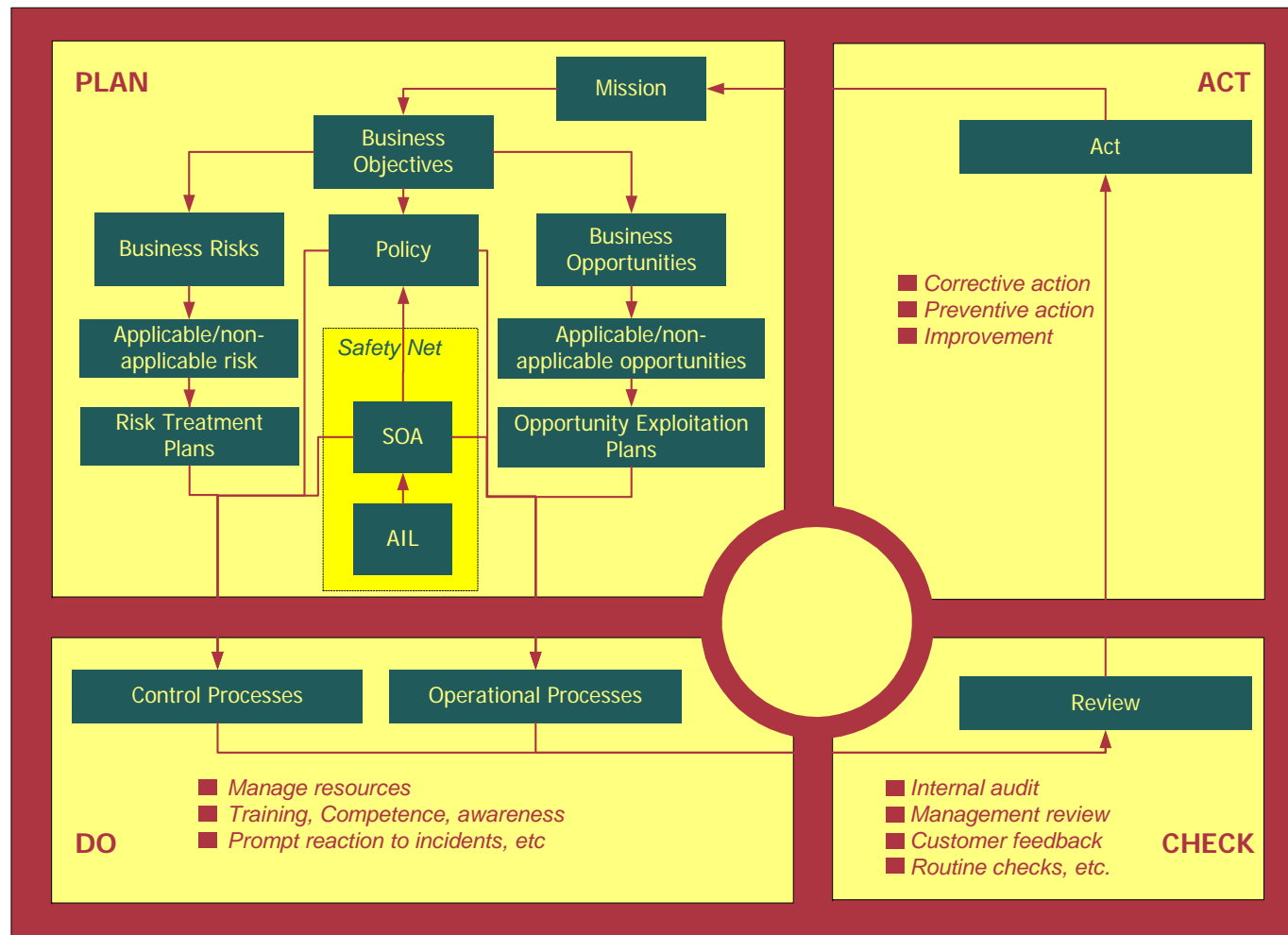
**The AIL**  
 AIL (pronounced "eye") is the French word for garlic, which for some people is used to ward off evil spirits. In our methodology, AIL stands for "Alternative Ideas List". It is usually manifest in the form of a code of good practice. Use it to identify any controls that you have inadvertently omitted when you formulated your Risk Treatment Plans. Document your results, identifying for each one whether it applies to you and why, in a "Statement of Applicability". ISO/IEC 27001 has an explicit formal requirement to do this. In other standards the AIL is implicit. For example, in ISO 9001 it corresponds to Section 7—Product Realisation.



Audit Practices Board  
 Business Risks  
<http://www.gammassl.co.uk/topics/ics/MSExploitation.pdf>  
 Applicable Risks



# Management system architecture



# The “AIL” concept

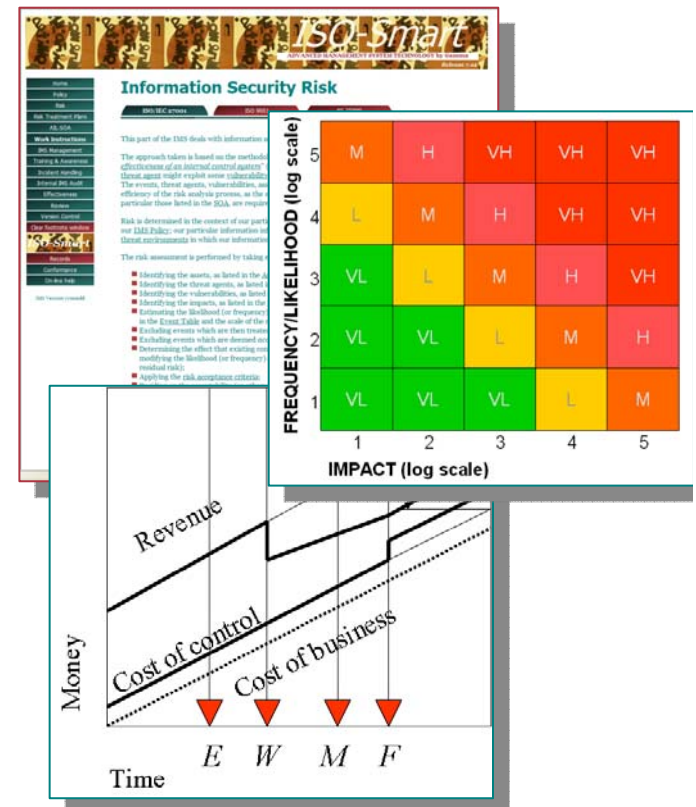
---

- RTPs and OEPs 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 Annex A (27K), §7 (9K) and CobiT are all about
- SOA  $\leftrightarrow$  “Alternative Ideas” List (AIL)
- It is a “safety net”



# Event-impact RTPs

- Risk Assessment/ Treatment process, which can be performed by executive board members
- Common to all standards
- Predicated on Modified Brewer-List Methodology
- Considers events and impacts
- Uses a “tell it like a story approach” to identify the controls



# Opportunity-benefit driven OEPs

## OPPORTUNITIES CONCERNING MARKET PRESENCE

■ The converse of events and impacts

■ Have Opportunity Exploitation Plans (OEPs) rather than RTPs

Assets exploited

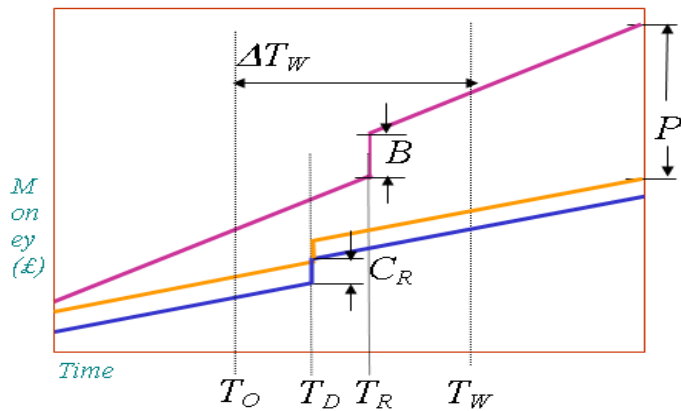
We have a range of products, some established (of which some will have just been improved), new products and the results of our own R&D projects. The Market Presence Opportunity Exploitation Plans (OEPs) focus on products that are already in market presence.

The assets that are taken advantage of are: Z1, Z2, Z3 and Z4.

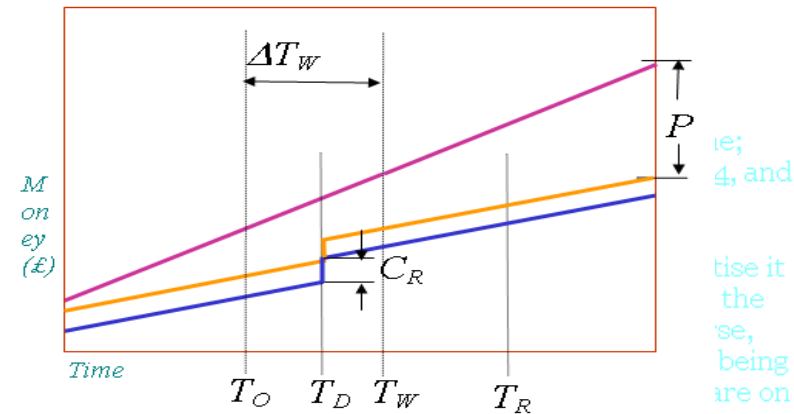
■ Similar "time" theory ■ Still aimed at Board level, etc

Anticipated benefits

The benefits are: Possible favourable customer perceptions, see [A1.1a](#), [A.1b](#), [A1.1c](#), [A1.d](#), [A1.1e](#)



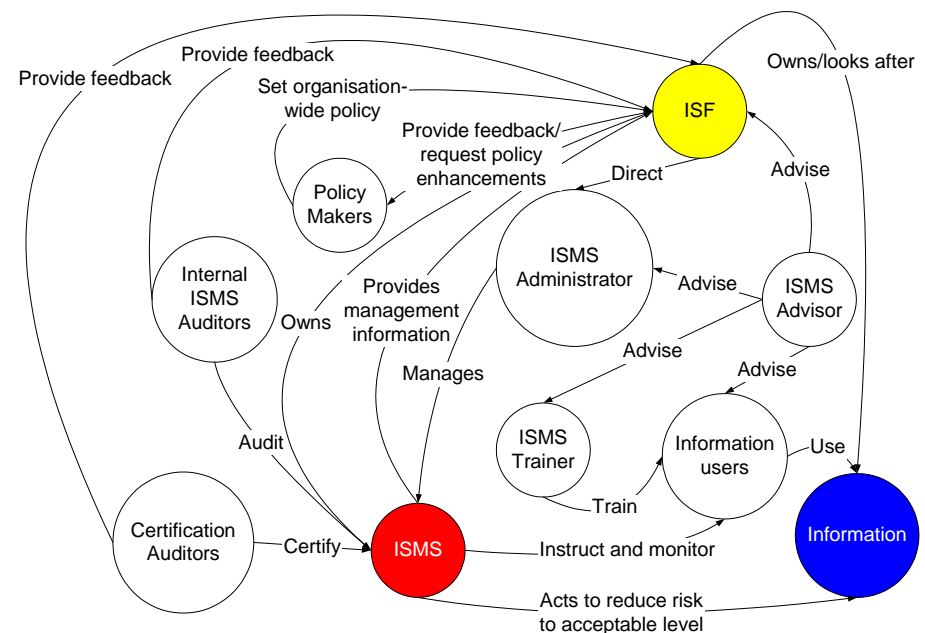
**Reaping the benefit**



**Loosing the opportunity**

# Role model

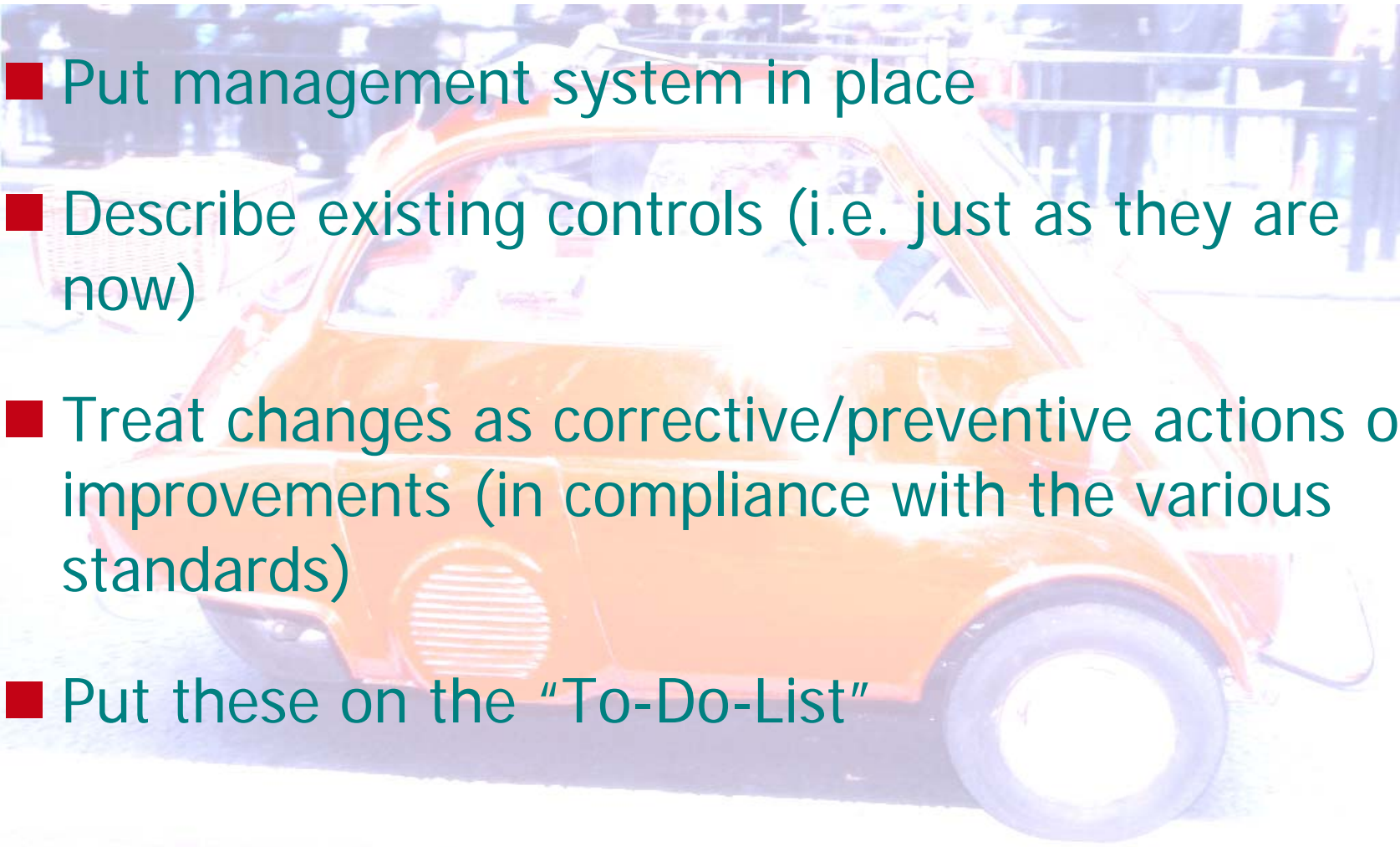
- Integrated Management System Forum (ISMF)
- IMS Implementer
- IMS Administrator
- Internal IMS Auditor
- IMS Trainer
- IMS Advisor
- Certification auditor (optional)
- Policy Maker



*Original role model as created in Mauritius, November 2003*

# The to-do-list concept

---

- 
- A semi-transparent background image of a red vintage car, possibly a Mini Cooper, parked in a public area with people and structures visible in the background.
- Put management system in place
  - Describe existing controls (i.e. just as they are now)
  - Treat changes as corrective/preventive actions or improvements (in compliance with the various standards)
  - Put these on the "To-Do-List"

# IMS-Smart technology

- Hypertext
- Ensure “desktop” conformance
- Accelerated IMS build
- Upgrade path (e.g. for revisions to ISO standards, increasing IMS scope, ...)
- On-line help facility



**IMS-Smart**  
ADVANCED MANAGEMENT SYSTEM TECHNOLOGY by Gamma  
Release 7.03

**Home**  
Policy  
Risk  
Risk Treatment Plans  
AIL-SOA  
**Work Instructions**  
IMS Management  
Training & Awareness  
Incident Management  
Internal IMS Audit  
Effectiveness  
Review  
Version Control  
Clear footnote window  
**IMS Smart**  
Records  
Conformance  
On-line help

IMS Version: yyymmdd

**Welcome**  
Welcome to Put the c  
The scope of our IM  
Put in the box the scope sentences long and apart does. An example would turn off these instructio

**Information Security Management**  
This part of the IMS deals with continual improvement. It explains how corrective and preventive action is taken and how improvements are managed. The need for such actions can arise at any time. This page explains what to do.  
The overall process is illustrated in the following diagram:

```

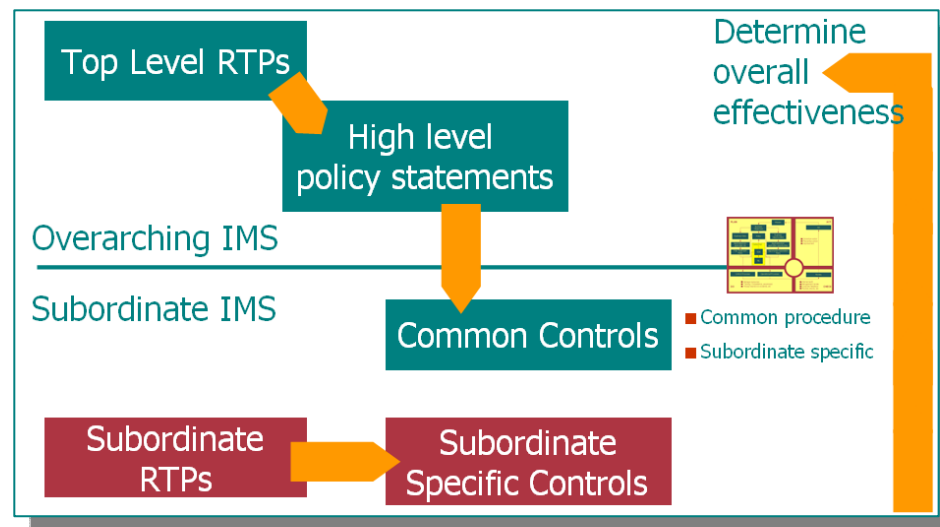
    graph TD
      Start([Start]) --> Step1[STEP 1]
      Step1 --> Step2[STEP 2]
      Step2 --> Step3[STEP 3]
      Step3 --> Step4[STEP 4]
      Step4 --> Step5[STEP 5]
      Step5 --> Step6[STEP 6]
      Step6 --> Step7[STEP 7]
      Step7 --> Step8[STEP 8]
      Step8 --> Step9[STEP 9]
      Step9 --> Step10[STEP 10]
      Step10 --> Step11[STEP 11]
      Step11 --> Step12[STEP 12]
      Step12 --> Step13[STEP 13]
      Step13 --> Step14[STEP 14]
      Step14 --> Step15[STEP 15]
      Step15 --> Step16[STEP 16]
      Step16 --> Step17[STEP 17]
      Step17 --> Step18[STEP 18]
      Step18 --> Step19[STEP 19]
      Step19 --> Step20[STEP 20]
      Step20 --> Step21[STEP 21]
      Step21 --> Step22[STEP 22]
      Step22 --> Step23[STEP 23]
      Step23 --> Step24[STEP 24]
      Step24 --> Step25[STEP 25]
      Step25 --> Step26[STEP 26]
      Step26 --> Step27[STEP 27]
      Step27 --> Step28[STEP 28]
      Step28 --> Step29[STEP 29]
      Step29 --> Step30[STEP 30]
      Step30 --> Step31[STEP 31]
      Step31 --> Step32[STEP 32]
      Step32 --> Step33[STEP 33]
      Step33 --> Step34[STEP 34]
      Step34 --> Step35[STEP 35]
      Step35 --> Step36[STEP 36]
      Step36 --> Step37[STEP 37]
      Step37 --> Step38[STEP 38]
      Step38 --> Step39[STEP 39]
      Step39 --> Step40[STEP 40]
      Step40 --> Step41[STEP 41]
      Step41 --> Step42[STEP 42]
      Step42 --> Step43[STEP 43]
      Step43 --> Step44[STEP 44]
      Step44 --> Step45[STEP 45]
      Step45 --> Step46[STEP 46]
      Step46 --> Step47[STEP 47]
      Step47 --> Step48[STEP 48]
      Step48 --> Step49[STEP 49]
      Step49 --> Step50[STEP 50]
      Step50 --> Step51[STEP 51]
      Step51 --> Step52[STEP 52]
      Step52 --> Step53[STEP 53]
      Step53 --> Step54[STEP 54]
      Step54 --> Step55[STEP 55]
      Step55 --> Step56[STEP 56]
      Step56 --> Step57[STEP 57]
      Step57 --> Step58[STEP 58]
      Step58 --> Step59[STEP 59]
      Step59 --> Step60[STEP 60]
      Step60 --> Step61[STEP 61]
      Step61 --> Step62[STEP 62]
      Step62 --> Step63[STEP 63]
      Step63 --> Step64[STEP 64]
      Step64 --> Step65[STEP 65]
      Step65 --> Step66[STEP 66]
      Step66 --> Step67[STEP 67]
      Step67 --> Step68[STEP 68]
      Step68 --> Step69[STEP 69]
      Step69 --> Step70[STEP 70]
      Step70 --> Step71[STEP 71]
      Step71 --> Step72[STEP 72]
      Step72 --> Step73[STEP 73]
      Step73 --> Step74[STEP 74]
      Step74 --> Step75[STEP 75]
      Step75 --> Step76[STEP 76]
      Step76 --> Step77[STEP 77]
      Step77 --> Step78[STEP 78]
      Step78 --> Step79[STEP 79]
      Step79 --> Step80[STEP 80]
      Step80 --> Step81[STEP 81]
      Step81 --> Step82[STEP 82]
      Step82 --> Step83[STEP 83]
      Step83 --> Step84[STEP 84]
      Step84 --> Step85[STEP 85]
      Step85 --> Step86[STEP 86]
      Step86 --> Step87[STEP 87]
      Step87 --> Step88[STEP 88]
      Step88 --> Step89[STEP 89]
      Step89 --> Step90[STEP 90]
      Step90 --> Step91[STEP 91]
      Step91 --> Step92[STEP 92]
      Step92 --> Step93[STEP 93]
      Step93 --> Step94[STEP 94]
      Step94 --> Step95[STEP 95]
      Step95 --> Step96[STEP 96]
      Step96 --> Step97[STEP 97]
      Step97 --> Step98[STEP 98]
      Step98 --> Step99[STEP 99]
      Step99 --> End([End])
  
```

The IMS was first e  
A link to the IMS reco

**Layout**  
Use the navigatio  
footnote window. T

# Overarching & Subordinate IMSs

- Needed for complex organisations (management structure)
- Hierarchy of IMSs
- Superior sets policy for subordinate
- Effectively establishes “baseline” of controls
- Subordinate may augment these to deal with greater risk
- Subordinate may deal with other risks



---

# BENEFITS

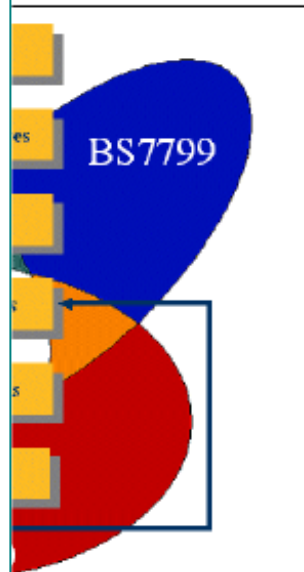
# One click away

---

- All documentation/records at your fingertips
- No hunting for documents
- No paper (99% saving)
- Reduced audit time (e.g. 4hrs down to 3½ minutes)
- Speeds up management reviews too

## Just a click away

Being a web-technology based system, navigation through the ISMS manual is by clicking on



are just parts of the tem

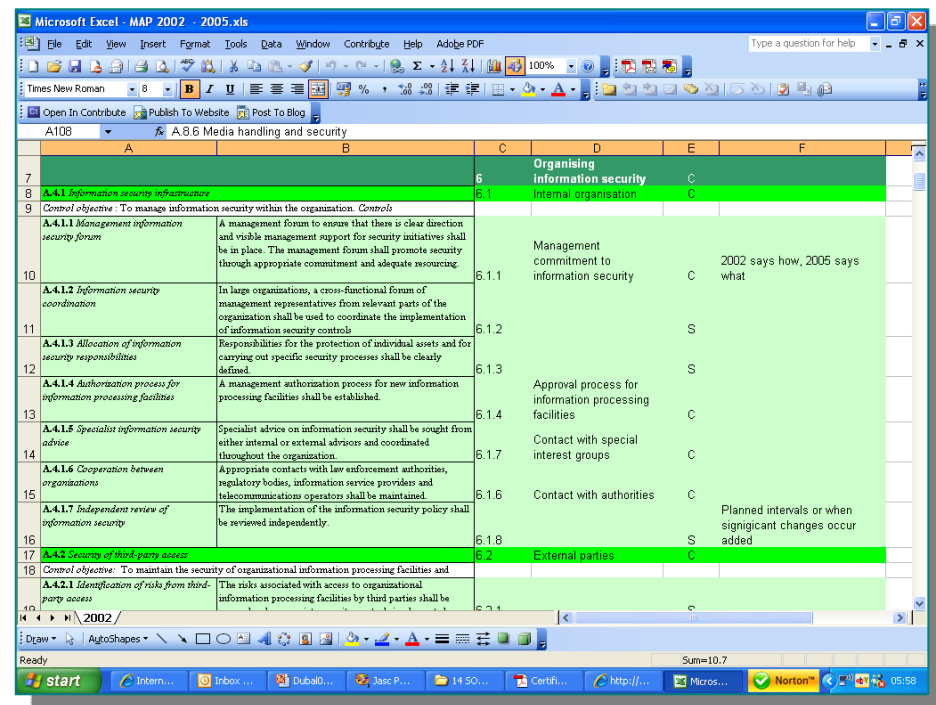
with glee.

hypertext links. In one particular sequence, I showed how internal audit observations, management system review actions, To-Do-List entries, change request forms and document control records all fitted together. In the space of a few minutes I had demonstrated how our management system had meet about 50% of the BS 7799-2 requirements. The assessor asked me another question. I clicked the hyperlink. The answer appeared in a footnote window (see [1]). Mike noticed the assessor smile

*Extract from <http://www.gammassl.co.uk/topics/ics/Certification%20v02.pdf>*

# Transitions

- Standards change every 5-6 years (ISO 9001 due later this year)
- Transitions are time-consuming
- *IMS-Smart* upgrades will shorten transition times by 2-3 months



	A	B	C	D	E	F
7			6	Organising information security	C	
8	A.4.1 Information security infrastructure		6.1	Internal organisation	C	
9	Control objective: To manage information security within the organization. Controls					
10	A.4.1.1 Management information security forum	A management forum to ensure that there is clear direction and visible management support for security initiatives shall be in place. The management forum shall promote security through appropriate commitment and adequate resourcing.	6.1.1	Management commitment to information security	C	2002 says how, 2005 says what
11	A.4.1.2 Information security coordination	In large organizations, a cross-functional forum of management representatives from relevant parts of the organization shall be used to coordinate the implementation of information security controls.	6.1.2		S	
12	A.4.1.3 Allocation of information security responsibilities	Responsibilities for the protection of individual assets and for carrying out specific security processes shall be clearly defined.	6.1.3		S	
13	A.4.1.4 Authorization process for information processing facilities	A management authorization process for new information processing facilities shall be established.	6.1.4	Approval process for information processing facilities	C	
14	A.4.1.5 Specialist information security advice	Specialist advice on information security shall be sought from either internal or external advisors and coordinated throughout the organization.	6.1.7	Contact with special interest groups	C	
15	A.4.1.6 Cooperation between organizations	Appropriate contacts with law enforcement authorities, regulatory bodies, information service providers and telecommunications operators shall be maintained.	6.1.6	Contact with authorities	C	
16	A.4.1.7 Independent review of information security	The implementation of the information security policy shall be reviewed independently.	6.1.8		S	Planned intervals or when significant changes occur added
17	A.4.2 Security of third-party assets		6.2	External parties	C	
18	Control objective: To maintain the security of organizational information processing facilities and					
19	A.4.2.1 Identification of risks from third-party access	The risks associated with access to organizational information processing facilities by third parties shall be	6.2.1		S	

Extract from Gamma's project records for transition of BS 7799-2:2002 to ISO/IEC 27001:2005

# Just one system

---

## OVERLAPS

- Some controls and therefore
- Non conformities
- Audits
- Management reviews
- Effectiveness analysis
- ....

- With several systems a lot of work, strictly speaking, has to be done several times
- This is a waste of resources
- Removal of duplicate effort – 100%

# Just one audit

---

- Having one audit saves time because of all the common elements
- In Gamma's case it's a reduction of about 80%
- Preparation used to be 2-3 days per audit, now it is virtually zero

## TYPICAL GAMMA AUDIT

### Morning

- Common management system
- Information security

### Afternoon

- Quality
- Report

---

Before IMS (9001 was paper based)

- 4 audits 1 full day each

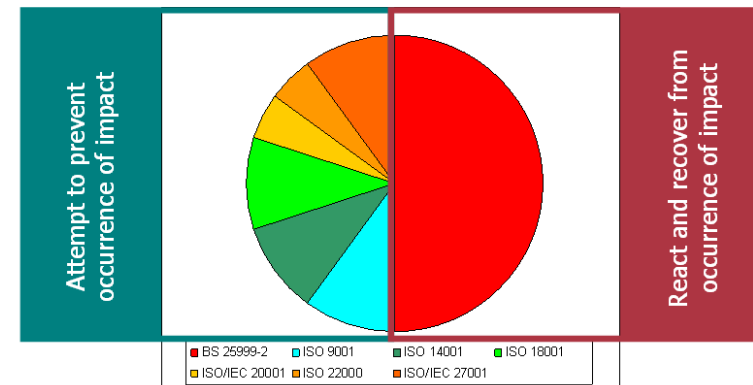
With IMS

- 1 audit of  $\frac{3}{4}$  day

# BS 25999

---

- BS 25999 on its own has to deal with all the triggering events of all the other management system standards plus one
- If all are integrated together then the means to prevent occurrence of impact is already dealt with
- Saving, for just ISO/IEC 27001 about 50% of up front consultancy effort



# But not least

---

- Ensures internal control is a line management responsibility



- Senior management takes ownership → better company with sound corporate governance

---

# SUMMARY

# Summary

---

- Productised IP-led service
- Buy just like an off-the-peg suit or a car, rather than “consultancy”
- Many satisfied customers
  - *Large complex organisations*
  - *Small organisations*
  - *Start-ups*
  - *Established companies, etc., etc.*
- More than just ISO – a key ingredient for sound internal control and corporate governance

---

# Integrated management systems – a productised IP-led service



Dr. David Brewer, FBCS, MIOD