Integrated Management Systems

Dr. David Brewer, *FBCS, MIOD*
Agenda

- Introduction
- Theoretical framework
- Practical experience
- Current state-of-the-art
- Benefits
- Summary
INTRODUCTION
What is a management system?

- 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
Above all

- Management system = management capability
- Albeit supported by documentation and records
- Perhaps in conformance with one or more management system standards, e.g. ISO 9001, ISO 14001, OHSAS 18001, ISO/IEC 20001, ISO 22000, ISO/IEC 27001, …
- But ISO doesn’t cover everything
- Must aim at Executive Board
Enter BS 25999-2

BS 25999 has to deal with the triggering events of all other management systems plus one
A perspective on Basel

Event loss types (Basel II)

KEY

- **Within scope of ISO/IEC 27001 and Annex A controls**
- **Within scope but not included in Annex A**
- **Outside scope**

©Gamma Secure Systems Limited, 2008
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

Secure Matrix

©Gamma Secure Systems Limited, 2008
THEORECTICAL FRAMEWORK
Roadmap

Internal control

“Tell it like a story”

The “Time” theory

Alternative ideas lists

A unified theory

Both co-authors of BS 7799-2:2002

William List, CA, FBCS
40 years in computer audit

David Brewer
PhD in experimental atomic physics

©Gamma Secure Systems Limited, 2008
Management system architecture

PLAN

- Business Objectives
- Policy
- Business Opportunities
- Applicable/non-applicable risk
- Applicable/non-applicable opportunities
- Risk Treatment Plans
- Opportunity Exploitation Plans
- Safety Net
- SOA
- AIL

DO

- Manage resources
- Training, Competence, awareness
- Prompt reaction to incidents, etc

ACT

- Act
- Corrective action
- Preventive action
- Improvement

CHECK

- Internal audit
- Management review
- Customer feedback
- Routine checks, etc.

©Gamma Secure Systems Limited, 2008
Event-impact RTPs

- Risk Assessment/Treatment process, which can be performed by executive board members
- Common to all standards
- Considers events and impacts
- Uses a “tell it like a story approach” to identify the controls
- Integrated with effectiveness measurement
Opportunity-benefit driven OEPs

The converse of events and impacts

Have Opportunity Exploitation Plans (OEPs) rather than RTPs

Similar “time” theory

Still aimed at Board level, etc

We have a range of products, some established (of which some will have just been improved), new products and the results of ongoing R&D products. The Market
is driving us to grow and exploit opportunities, to position our products in the
market presence.

The assets that are taken advantage of are: 21, 22, 23 and 24.

Possible favourable customer perceptions, see A1.1a, A.1b, A1.1c, A1.1d, A1.1e

Reaping the benefit

Loosing the opportunity

©Gamma Secure Systems Limited, 2008
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 ↔ “Alternative Ideas” List (AIL)
- It is a “safety net”
PRACTICAL EXPERIENCE
History

RTP concept conceived
Time theory published
IMS concept published
First use
Mauritius deployment
Qatar
Kuwait
India, elsewhere ME
Elsewhere, ROW
FrontPage (the
Skeleton)
Dreamweaver template
IMS-Smart
Mauritius

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

Overarching ISMS at Cabinet Office level

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

Consultants trained selected civil servants to do the work

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

ISO Achieves ISO/IEC 27001:2005 Certification

Information Services Department proudly announces that GSS 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 DIN 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 GSS to manage its information security risks.

GSS is the first to secure this prestigious ISO 27001 Certification.
Figure 1: Overall timescales
Timescales

- Mauritius – 4 months
- Gamma – 4 months
- Qatar – 4 months
- Kuwait – 7 weeks

Fast Track IMS

At an information security conference on 29 April 2004 there were gasps of awe from the audience as we announced that four clients of ours based in that country had achieved ISMS attestation in less than four months each from a standing start. Gamma’s own ISMS took three months to build and be certified, with much of that being spent waiting for a convenient slot in BSI’s and Gamma’s busy schedules.

How can we do this?

The answer lies in our “fast track” approach to building Integrated Management Systems, of which an ISO/IEC 15001 ISMS is just a component.
CURRENT STATE-OF-THE-ART
Productised IP-led service

- Packaged as a PIPS for both consultancy and training
- **IMS-Smart**
- Delivered by Gamma and Secure Matrix
- Created by Dr. David Brewer, a co-author of BS 7799-2 (now ISO/IEC 27001)
- Tried and tested

* Under development

©Gamma Secure Systems Limited, 2008
Under the hood

- Classroom/on-the-job training, throughout at least one PDCA cycle
- Solid theoretical foundation
- Event-impact RTPs, etc
- Role Model
- To-Do-List concept
- Overarching/subordinate IMS

IMS-Smart

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

SecureMatrix

Project plan as actually used in Mauritius

3-6 months

©Gamma Secure Systems Limited, 2008
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

©Gamma Secure Systems Limited, 2008
The to-do-list concept

- 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”
Overarching & Subordinate ISMSs

- Needed for complex organisations (management structure)

- Hierarchy of ISMSs
  - 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

©Gamma Secure Systems Limited, 2008
IMS-Smart

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

©Gamma Secure Systems Limited, 2008
Greater sophistication

- Just 3 RTPs covers the whole of the 133 controls in ISO/IEC 27001 Annex A
- The risk square
- Applied to ISO 9001, again three families, actually allows you to derive your necessary quality processes

<table>
<thead>
<tr>
<th>ISO 9001/2008 Requirement</th>
<th>Cross-reference</th>
<th>Control Structures</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1 General requirements</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Establish a documented Quality Management System</td>
<td>Plan</td>
<td>Welcome</td>
</tr>
<tr>
<td>Quality process identification</td>
<td>Internal</td>
<td>Audit</td>
</tr>
<tr>
<td>Sequence and interaction of quality processes</td>
<td>Check</td>
<td>Check</td>
</tr>
<tr>
<td>Criteria and methods to ensure effectiveness</td>
<td>Do</td>
<td>Do</td>
</tr>
<tr>
<td>Ability to operate, monitor and improve</td>
<td>Review</td>
<td>Review</td>
</tr>
<tr>
<td>Outsourcing</td>
<td>Policy</td>
<td>Policy</td>
</tr>
</tbody>
</table>

Vulnerability exploitation: An attacker exploits a security vulnerability to cause the undesirable disclosure of information, fraud or denial of service. The attacker could be an authorised user of our IT, whereby they abuse their authority and do things that they should not. If the attacker is not an authorised user of our IT they might attempt to masquerade as an authorised user. Perhaps the attacker can gain access to our IT by some other means, or simply eavesdrop. The focus of this RTP is towards the creation of a healthy security culture backed by sound technical security. The RTP also recognises the dynamic nature of this particular threat environment.

IT failure: Our IT fails because of a hardware or software malfunction. The malfunction can be brought about in a variety of ways, such as lack of power, adverse operating conditions (fire, flood etc.), unreliability and specification/design/implementation errors. The focus is on making sure that the IT works and is available for use.

Dispossession: A physical container of information is dispensed. Typical containers are documents, envelopes, briefcases, laptops, desktops, servers, PDAs, mobile phones, cameras, magnetic tapes, CDs, DVDs, USB sticks etc. Dispossession
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 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

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

©Gamma Secure Systems Limited, 2008
Just one system

- 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%

OVERLAPS
- Some controls and therefore
- Non conformities
- Audits
- Management reviews
- Effectiveness analysis
- …
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 ¾ 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 upfront 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

- Integrated management systems – PDCA engine to drive internal control

- *All* of it – not just risk management or ISO standards

- Holistic approach aimed at Executive Board

- Tried and tested, packaged as a PIPS for consultancy and training
Integrated management systems

Thank you for listening

Dr. David Brewer, FBCS, MIOD
www.gammasl.co.uk