Integrated Management Systems

New Delhi, 16 February 2008
Dr. David Brewer
You're in charge. That's what you think!

William List, CA, FBCS
40 years in computer audit

[Roadshow image with text and photos]

David Brewer
PhD in experimental atomic physics

Secure Matrix

©Gamma Secure Systems Limited, 2008
Agenda

- Internal control
- “Tell it like a story”
- The “Time” theory
- Alternative ideas lists
- A unified theory
- The current state of the art – PIPS
Internal control
**Initial quest**


- Enter the UK Audit Practices Board’s guidance on internal control and the requirements of Turnbull, OECD, Sarbanes-Oxley, EU directive, …
Putting on my CEO hat...

A taxonomy of risk

<table>
<thead>
<tr>
<th>Primary Risk Category</th>
<th>Definition: the risk of loss arising from ...</th>
<th>Associated Operational Risk: the inadequacy or failure of internal processes, people and systems that results in a risk of ...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Project risk</td>
<td>... default by a creditor (which will usually be a customer).</td>
<td>... doing work and not making a profit.</td>
</tr>
<tr>
<td>Market risk</td>
<td>... the market will not pay what we have to pay for the materials and other assets not</td>
<td></td>
</tr>
<tr>
<td>Existence risk</td>
<td>... the fact that we exist as a business.</td>
<td></td>
</tr>
</tbody>
</table>

The creditor defaults

1. Invoice not raised
2. Work outside contract
3. Unacceptable quality
4. Overheads too high
5. Unable to complete the job
6. 10. Delivery too late
Putting on my CEO hat...

### CREDIT RISK

<table>
<thead>
<tr>
<th>Primary Risk Category</th>
<th>Definition: the risk of loss arising from ...</th>
<th>Associated Operational Risk: the inadequacy or failure of internal processes, people and systems that results in a risk of ...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Project risk</td>
<td>... default by a creditor (which will usually be a customer).</td>
<td>... doing work and not making a profit.</td>
</tr>
<tr>
<td>Trading risk</td>
<td>... changes in trading positions when prices move adversely.</td>
<td>... our money and other assets not being worth as much as they ought.</td>
</tr>
<tr>
<td>Market risk</td>
<td>... the market refusing to buy what we have to offer at the price we wish to sell it.</td>
<td>... being unable to sell what the market wants.</td>
</tr>
<tr>
<td>Existence risk</td>
<td>... the fact that we exist.</td>
<td>... spending money unnecessarily.</td>
</tr>
</tbody>
</table>

### MARKET RISK

- 1
- 2
- 3
- 4

### OPERATIONAL RISK

©Gamma Secure Systems Limited, 2008
So it is an acceptable risk to loose £5000. What if you loose £5001?
“Tell it like a story”
Dealing with the MD

- “What are your information assets?”
- “What are your threats?”
- “What are your vulnerabilities?”
- “What are your concerns?”
Event-impact RTPs

- Considers events and impacts
- Uses a “tell it like a story approach” to identify the controls
- Threats, vulnerabilities and assets drop out of the analysis
- Understood by senior civil servants
- Most effective at engendering awareness
Common sense prevails

- How do you prevent the event?

- If can’t or prevent fails, how do you detect it and prevent impact?

- If can’t or detect/prevent fails, how do you react to the impact?

Read the paper 😊
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

ISO 9001:2000 Requirement

4. Quality management system
   - 4.1 General requirements
     - Establish a documented Quality Management System
     - Quality process identification
     - Sequence and interaction of quality processes
     - Criteria and methods to ensure effectiveness
     - Ability to operate, monitor and improve
     - Outsourcing

Control Structures

©Gamma Secure Systems Limited, 2008
When BA 122 aborted take-off on 22 November 2003, we found ourselves in the midst of a real RTP.
The “Time” theory
Event-Impact Relationship

There is a fundamental principle of internal control (and thus ISMS):

“… detect the event in sufficient time to do something positive about it… “

See http://www.gammassl.co.uk/topics/time/index.html
Fundamental Model (too late)
Fundamental Model (in time)
# Control Spectrum

<table>
<thead>
<tr>
<th>Class</th>
<th>Ability to detect the event and take recovery action</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Prevents the event, or detects the event as it happens and prevents it from having any impact</td>
<td>Preventive</td>
</tr>
<tr>
<td>2</td>
<td>Detects the event and reacts fast enough to fix it well within the time window</td>
<td>Detective</td>
</tr>
<tr>
<td>3</td>
<td>Detects the event and just reacts fast enough to fix it within the time window</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Detects the event but cannot react fast enough to fix it within the time window</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Fails to detect the event but has a partially deployed BCP</td>
<td>Reactive</td>
</tr>
<tr>
<td>6</td>
<td>Fails to detect the event but does have a BCP</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Fails to detect the event and does not have a BCP</td>
<td></td>
</tr>
</tbody>
</table>
And what if it doesn’t work?
Alternative Ideas Lists
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 was first to call it the shape of the future

©Gamma Secure Systems Limited, 2008
But are they designed that way?

Information Security Management Systems – Requirements (27001)

- Scope
- Policy
- Risk Assessment (RA)
- Risk Treatment Plan (RTP)
- Statement of Applicability (SOA)
- Operate Controls
- Awareness Training
- Manage Resources
- Prompt Detection and Response to Incidents

The Deming Cycle

- Plan
- Do
- Check
- Act

Ensuring information security is always appropriate to your business
But are they designed that way?

Quality Management Systems – Requirements (9001)

Scope • Policy • Exclusions •
Operate Controls • Awareness Training •
Manage Resources • Customer feedback •

QMS Improvements • Preventive Action • Corrective Action • Management Review • Internal QMS Audit

The Deming Cycle

Ensuring customer satisfaction and product conformity

©Gamma Secure Systems Limited, 2008
But are they designed that way?

Business Continuity Management Systems – Requirements (25999)

- Scope
- Policy
- Business Impact Analysis
- Risk Assessment/ Risk Treatment
- Business continuity plans
- Exercises
- Awareness Training
- Manage Resources
- Incident Response
- BCMS Improvements
- Preventive Action
- Corrective Action
- Management Review
- Internal BCMS Audit

Ensuring business continuity

©Gamma Secure Systems Limited, 2008
Enter the “AIL”

- Policy/RTPs 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 the SOA is about
- SOA ↔ “Alternative Ideas” List (AIL)
- It is a “safety net”
Multiple AILs

- In reality there are multiple AILs
- ISO/IEC 27002:2005 is just one such list, but there are many others, for example:
  - CobiT
  - Section 7 of ISO 9001

ISO 9001:2000 AIL

- Planning of Product Realisation
- Customer Related Processes
- Design and Development
- Purchasing
- Product and Service Provision
- Control of Monitoring and Measuring Devices
Common PDCA framework

Information Security Management + Quality Management

Scope • Policy • Risk Assessment (RA) • Risk Treatment Plan (RTP) • Operate Controls • Awareness Training • Manage Resources • Customer feedback • Prompt Detection and Response to Incidents • ISMS Improvements • Preventive Action • Corrective Action • Management Review • Internal ISMS Audit

The Deming Cycle

PLAN
DO
CHECK

©Gamma Secure Systems Limited, 2008
And an AIL for each standard

Information Security Management + Quality Management

• Security Policy
• Asset Management
• Human Resources Security
• Physical and Environmental Security
• Communications and Operational Management
• Access Control
• Information Systems Audit Management
• Exclusions
• Business Continuity Management
• Compliance

Statement of Applicability (SOA)

PLAN
ACT

The Deming Cycle

DO
CHECK

©Gamma Secure Systems Limited, 2008
Overall Model

Superposition of UK Audit Practices Board model and ISO/IEC 27001
But internal control has two parts - you have only dealt with the second. What about the first?
A unified theory
Test of the AIL concept using Ries and Trout’s 22 immutable laws of marketing:

- Only six laws are controls
- What are the other 18?

Answer: things concerned with the first part of internal control
Opportunities and Benefits

- **The converse of events and impacts**

  We have a range of products, some established (of which some will have just been introduced), as well as an outcome of the result of a range of NPD products. The market is up to opportunity particular way of selling our products by generating market presence.

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

- **Have Opportunity Exploitation Plans (OEPs) rather than RTPs**

- **Assets exploited**

- **Similar “time” theory**

  Benefits are:

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

  - Money (£)

  - Time

  - \( T_O \), \( T_D \), \( T_R \), \( T_W \)

  - \( \Delta T_W \)

  - \( P \)

  - \( B \)

  - \( C_R \)

- **Anticipated benefits**

- **Reaping the benefit**

- **Loosing the opportunity**

©Gamma Secure Systems Limited, 2008
Enhanced PDCA Framework

PLAN

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

DO

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

ACT

- Act
- Corrective action
- Preventive action
- Improvement

CHECK

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

©Gamma Secure Systems Limited, 2008
I am in charge
The current state of the art - PIPS
Over the years...

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

Project plan as actually used in Mauritius

3-6 months
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

- Put management system in place
- Describe existing controls (i.e. just as they are now)
- (Means certain prerequisites apply)
- Treat changes as corrective/preventive actions or improvements (in compliance with the various standards)
- Put these on the “To-Do-List”
- There are other strategies, but some, like the Vasa, are doomed at the outset
Template IMS

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

RTP concept conceived
Time theory published
IMS concept published
First use
Mauritius deployment
FrontPage (the Skeleton)
Dreamweaver template
Productised IP-led service (PIPS)

- Delivered by Secure-Matrix
- Created by Gamma
- Facilitates rapid construction of an IMS
- Facilitates upgrades to accommodate new and revised standards, etc…
Well - maybe
Integrated Management Systems

Thank you for listening

New Delhi, 16 February 2008
Dr. David Brewer

©Gamma Secure Systems Limited, 2008