Is IT Governance Enough?

by Dr. David Brewer

Gamma Secure Systems Limited
Diamond House, 149 Frimley Road
Camberley, Surrey, GU15 2PS +44 1276 702500
dbrewer@gammassl.co.uk
www.gammassl.co.uk
The Question

IT security practitioners have long realised that it is essential to align information security with the needs of the business. With the advent of the OECD guidelines on corporate governance and, in the UK, the Turnbull Report, the IT professionals see that "corporate governance and IT governance can no longer be considered separate and distinct disciplines". But does this view merely reinforce this distinction? To address the real business requirement is IT governance enough?
Agenda

- Corporate governance, OECD Guidelines and Turnbull?
- Internal Control Structures and Business Objectives
- Work of the IT Governance Institute
- COBIT and ISO/IEC 17799 / BS 7799-2
- The "gaps"
- How BS 7799-2:2002 helps fill the gaps

(c) Gamma Secure Systems Limited, 2002
Corporate governance, OECD Guidelines and Turnbull?
Corporate Governance

How to run your business to meet your mission

- Safeguarding stakeholders’ interests
- Ethos
- Processes

OECD Principals for Corporate Governance
- For corporate organisations
- Fairness to stakeholders

Turnbull
- 100 FTSE only (Yellow Book)

Even if not mandatory, gives good advise and guidance

7799 Goes Global
Internal Control Structures and Business Objectives
The internal control requirements of the Combined Code

**Principle D.2** of the Code states that ‘The board should maintain a sound system of internal control to safeguard shareholders’ investment and the company’s assets’.

**Provision D.2.1** states that ‘The directors should, at least annually, conduct a review of the effectiveness of the group’s system of internal control and should report to shareholders that they have done so. The review should cover all controls, including financial, operational and compliance controls and risk management’.

**Provision D.2.2** states that ‘Companies which do not have an internal audit function should from time to time review the need for one’.
Business Objectives

- Customer knows about product
- Customer buys product
- Able to make and deliver product at “right” price/quality
- Etc….
Specific Risks

- Customer buys from competition
- Customer doesn’t buy anything
- Cannot supply
- Costs too high for adequate gross margins
- Etc. . .
Common Risks

- Acts of God
- Error
- Fraud
- Hacking
- Bad records
- Theft
- Etc….

(c) Gamma Secure Systems Limited, 2002
Work of the IT Governance Institute
To achieve success in this information economy, enterprise governance and IT governance can no longer be considered separate and distinct disciplines

Board Briefing on IT Governance

Board Briefing on Information Security Governance

COBIT (Control Objectives for IT)
COBIT and ISO/IEC 17799 / BS 7799-2
COBIT

- Code of practice, like 17799

- Wider brief
  - Planning and organisation
  - Acquisition and implementation
  - Delivery and support
  - Monitoring

- Embraces “Plan, Do, Check, Control”

- 3rd Edition, a family of products
COBIT

Executive Summary

Framework
with high level control objectives

Management Guidelines

Detailed Control Objectives

Audit Guidelines

Implementation Tool Set
COBIT & 17799/7799-2

- Can’t be certified to COBIT
- Can be certified to BS 7799-2

Some more detail

Concise ISMS specification
Nothing Covers Everything

- Good reason for why BS 7799-2:2002 integrates with other management system standards

- But there are still gaps
The “Gaps"
Biases and Not Enough

- Confidentiality
- Integrity
- Platform Security
- Business Applications
- IT risks
- Business Context
- Prevention
- Detection

➢ Inability of testing big systems & the unknown vulnerability

7799 Goes Global
How BS 7799-2 fills the gaps
Get the I(S)MS Structure Right
Standards are Just a Perspective

MANAGEMENT REQUIREMENTS

3.1 General

The organisation shall establish and maintain a documented ISMS. This shall address the assets to be protected, the organisation's approach to risk management, the control objectives and controls, and the degree of assurance required.

3.2 Establishing a management framework

The following steps shall be undertaken to identify and document the control objectives and controls:

- The information security policy shall be defined.
- The scope of the ISMS shall be defined. The boundaries shall be defined in terms of the characteristics of the organisation, its location, assets and technology.
- An appropriate risk assessment shall be undertaken. The risk assessment shall identify the threats to assets, vulnerabilities and impacts on the

INTRODUCTION

From an information security perspective, there are a number of concerns that fall out immediately from our business risk and vulnerabilities that could exploited by various threats, which, if successful, could result in:

- Direct financial loss
- Loss of reputation
Controls/Risks are Many-Many
Know When There is a Problem

- E.g. when non-applicable risks become applicable!

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>high</td>
<td>Area of applicable risk</td>
</tr>
<tr>
<td>low</td>
<td>high</td>
</tr>
</tbody>
</table>

- Low Impact
- High Likelihood

(c) Gamma Secure Systems Limited, 2002
Take a Fresh Look at PDCA

Detect

Prevent

Contain

Recover

Do

Check

Plan

Act
Ask the Right Questions

- “How worried are you if a hacker gets into the system?”

- “How concerned would you be if competitor X got hold of your trade secret Y?”

- “Would you be more or less concerned if there were in excess of £L million of unpaid invoices overdue by M months?”
Ask the Right Questions

- “How worried are you if a hacker gets into the system?”
- “How concerned would you be if someone got hold of your trade secrets?”
- “Would you be more or less able to pay your bills if you were in excess of £L million overdue by M months?”

- If office dead, what do we do now?
- Our recovery plan fails!
- If big error (fraud), who finds it?
- Can customer find website?
- Information on website OK?
- Our sales are way off - why?
Pay Attention to Applications

- Work out what controls you need in the business applications

- Then work out how platform security can help

- I(S)MS metrics:
  - How long does it take to find out the problem?
  - Is there sufficient time to fix it?
Summary
Summary

- Rather than educate the Board (ITGovlnst approach), teach IT the business priorities
  - Risk questions in overall business context
  - Emphasis on how do you know its wrong
  - Applications before platforms

- BS7799-2:2002 – the kernel on which to build
  - Risk-based management standard
  - Concise PDCA-based specification with guidance
  - Certifiable
  - Integrates well with other standards
The Answer to the Question

Better to teach the business priorities to the information technologists, and consider security from the application perspective. The big ones (Bearings, Enron, …) are all application issues. There should only be corporate governance. “This” governance and “that” governance merely clouds the issue. Internal Controls are the processes that implement the mission. Controlling everything is impossible and too expensive. Who can ever think of all the risks anyway. Therefore we need risk analysis to establish priorities. PDCA then takes over and BS 7799-2:2002 is a good place to start.