E-biz Governance

Dr. David Brewer
Gamma Secure Systems Ltd
www.gammassl.co.uk
Agenda

- What is e-biz governance
- How ISO/IEC 17799 & BS 7799-2 fits
- How to apply the standards
- How to determine their effectiveness
- Particular e-biz controls
- Summary and conclusions
What is e-biz governance
Purpose

• Help organisations achieve their e-business goals
• Broadly speaking → trading profitably over Internet
Relation to Corporate Governance

• e-biz governance closely related to Corporate Governance, which:
  – Seeks to put in place all management controls necessary to achieve an organisations mission
  – Manage risk
  – Assure effective control
  – Seek improvements where appropriate
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’.
Cornerstones of the Approach

• Risk Management
• PDCA Model
  – Plan
  – Do
  – Check
  – Act
e-biz Context

- Not only usual business risks but also –
  - Rapidly Changing IT/Internet Risks
  - Need to cope with multiple legal jurisdictions
How ISO/IEC 17799 & BS 7799-2 fits
e-biz Risks

• Usual business risks plus:
  – Lots of IT
  – Internet
  – On-line payment
  – Possible on-line fulfilment
  – Multi-legal jurisdictions

• All covered by ISO/IEC 17799
Risk Management

• e-biz governance requires:
  – Need to access risks
  – Take action
  – Monitor
  – Reassess
  – Take further action as necessary

• All covered by BS 7799-2:2002
How to apply the standards
Apply BS 7799-2:2002 in the Usual Way

- Establish Information Security Forum
- Agree ISMS Scope and ISMS Policy
- Perform Risk Assessment
- Agree Risk Treatment Plan
- Implement Controls
- Monitor Effectiveness
- Act as necessary

PLAN  DO  CHECK  ACT
But…

• e-biz is more than IT
• e-biz is more than information
  – Stock
  – Money
  – Health & Safety

• Some tips
  – Impacts to consider
  – Events to consider
Impacts to Consider

- Adverse press coverage
- Court action (criminal and civil)
- Loss of revenue
- Increased costs
- Loss of current business
- Loss of future business
Events to Consider

• Theft (of stock and information)
• Acts of God, vandals and terrorists
• Duplicate deliveries, failure to deliver
• Distribution of offensive material
• Breach of contract, regulations, law
• Fraud
• IT failure
• Hacking (e.g. DOS attacks)
• Disclosure
How to determine their effectiveness
Methods and Metrics

• Methods:
  – Internal audits
  – Management reviews
  – Testing (penetration, role playing …)

• Metrics
  – Controls in place, working
  – Real incidents, test results
  – Time to detect versus time to fix
Particular e-biz controls
## Analysis of Real SOA

<table>
<thead>
<tr>
<th>Policy</th>
<th>Event #</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Policy</td>
<td>x</td>
</tr>
<tr>
<td>Organisational Security</td>
<td>x x x x x</td>
</tr>
<tr>
<td>Asset Classification and Control</td>
<td>x</td>
</tr>
<tr>
<td>Personnel Security</td>
<td>x</td>
</tr>
<tr>
<td>Physical and Environmental Security</td>
<td>x x x x x</td>
</tr>
<tr>
<td>Communications and Operations Management</td>
<td>x x x x x x x x x</td>
</tr>
<tr>
<td>Access Control</td>
<td>x x x x x x x x</td>
</tr>
<tr>
<td>System Development and Maintenance</td>
<td>x x x x x x x x</td>
</tr>
<tr>
<td>Business Continuity Management</td>
<td>x x x x x x</td>
</tr>
<tr>
<td>Compliance</td>
<td>x x x x x</td>
</tr>
</tbody>
</table>
Distribution of Offensive Material

- **Risk:** Orders that are placed over the Internet require the input of the delivery address. The delivery address could contain offensive remarks.

- **Controls:**
  - A.10.2.1 Input data validation
  - A.10.2.4 Output data validation
Legal (UK)

- **Risk:** breach of:
  - Data Protection Act 1998
  - Electronic Commerce Act 2000
  - Regulation of Investigative Powers Act 2000
  - Copyright, Designs and Patents Act 1988
  - Companies Act 1985
  - Official Secrets Act 1989
  - Freedom of Information Act 2000

- **Controls:** A.4, A.7 – A.12
Hacking

• **Risk:** It may be possible for some unknown person to access the internal networks remotely and read data, modify it, introduce malicious programs and cause other damage. Customer facing web sites may be attacked.

• **Controls:** A.4, A.8, A.9, A.11
Summary and conclusions
Summary

• We have explained:
  – What e-biz governance is
  – How ISO/IEC 17799 and BS 7799-2 fit in

• We have shared our thoughts on:
  – Particular e-biz related events and impacts
  – Associated controls
Conclusions

• e-biz governance involves
  – Risk Management
  – PDCA

• ISO/IEC 17799 provides a comprehensive list of appropriate controls

• BS 7799-2:2002 provides the risk management/PDCA framework