Agenda

- Corporate Governance
- Internal Control
- ISO/IEC 17799 and BS 7799-2
  - Could they serve as an adequate control framework?
  - Have they a wider utility?
- Prospects and Limitations
- Summary
Corporate Governance
Why

- ... a result of scandals ... investing public ... being "ripped off" ... conduct of senior executives
  - South Sea Bubble, Kruger, Salad Oil company, Equity funding, Polly Peck, Maxwell Pensions, Enron, WorldCom ...

- New laws/regulations ... anti discrimination, privacy protection, product quality etc.

- Turnbull, OECD, Sarbanes-Oxley
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'.

- The rights of shareholders and key ownership functions
- The equitable treatment of shareholders
- The role of stakeholders in corporate governance
- Disclosure and transparency
- The responsibilities of the Board

▶ *It is an important function of the board to establish internal control systems covering the use of corporate assets and to guard against abusive related party transactions.*
Sarbanes-Oxley/EC Directive

- An act “to protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the security laws, and for other purposes”

- Places heavy emphasis on internal control, e.g.
  - §404 (a) (1) state the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting.
Internal Control
What is Internal Control?

- Way in which management deploys resources to achieve the organisation's objectives

- Two basic parts:
  - Procedures to perform the work necessary to conduct the organisation's business (operational procedures)
  - Procedures to ensure that the business is conducted as expected (controls)

- It is this second part that concerns us today
This is their advice:

- Mission
- Business Objectives
- Business Risks
- Applicable Risks
- Internal Controls
- Review
# Risks – a Taxonomy

## Following Basel II

<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><strong>Project risk</strong></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><strong>Trading risk</strong></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><strong>Market risk</strong></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><strong>Existence risk</strong></td>
<td>... the fact that we exist.</td>
<td>... spending money unnecessarily.</td>
</tr>
</tbody>
</table>
## Applicable Risks

- and non-applicable risks

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>high</td>
<td></td>
</tr>
<tr>
<td>low</td>
<td></td>
</tr>
<tr>
<td><strong>low</strong></td>
<td></td>
</tr>
</tbody>
</table>

*Area of applicable risk*
Controls – Fundamentals

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

See http://www.gammassl.co.uk/topics/time/index.html
Types of Control

- **Preventive**
  - Either prevent the event from occurring or affecting the organisation, or
  - Detect the event as it happens and prevent any further activity that may lead to an impact

- **Detective**
  - Identify when some event, or events have occurred ... and invoke appropriate actions to arrest (or mitigate) the situation

- **Reactive**
  - Identify that the impact has occurred and invoke appropriate actions to recover (or mitigate) the situation
ISO/IEC 17799 and BS 7799-2

1 – What are they?
World-wide Take Up

BS 7799-2 Registrations by Continent

Growth of BS7799-2 Registrations World Wide

(c) Gamma Secure Systems Limited 2004
ISO/IEC 17799 and BS7799-2

- BS 7799 Part 2 is a management standard – e.g. let’s party. Part 2 tells you what to do
- IS 17799 is a supermarket of good things to do
- Certification is against Part 2 – is the party OK?
BS 7799-2:2002

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 •

ISMS Improvements •
Preventive Action •
Corrective Action •
Management Review •
Internal ISMS Audit •
ISO/IEC 17799:2000

Provides guidance under 10 major headings

- Security Policy
- Security Organisation
- Asset Classification and Control
- Personnel Security
- Physical and Environmental Security
- Communications and Operational Management
- Access Control
- Systems Development and Maintenance
- Business Continuity Management
- Compliance
ISO/IEC 17799 and BS 7799-2

2 – Could they serve as an adequate control framework?
Equivalent Structures

Mission

Business Objectives

Business Risks

Applicable Risks

Internal Controls

Review

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 •

• ISMS Improvements
• Preventive Action
• Corrective Action
• Internal ISMS Audit

(c) Gamma Secure Systems Limited 2004
## Gamma’s ICS Does This (2)

<table>
<thead>
<tr>
<th>Home</th>
<th>Overall MS</th>
<th>ISO 9001</th>
<th>BS 7799-2</th>
</tr>
</thead>
<tbody>
<tr>
<td>PLAN</td>
<td>Scope</td>
<td>Scope</td>
<td>Scope</td>
</tr>
<tr>
<td></td>
<td>Policy</td>
<td>Quality Policy</td>
<td>Information Security Policy</td>
</tr>
<tr>
<td></td>
<td>Business Risks</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk Treatment Plan Index</td>
<td></td>
<td>Risk Assessment</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Threats</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Assets</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Vulnerabilities</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Impacts</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Compliance</td>
<td>Exclusions</td>
<td>SOA</td>
</tr>
<tr>
<td></td>
<td>Compliance</td>
<td>Compliance</td>
<td>Compliance</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>DO</th>
<th>Summary of Internal Controls</th>
<th>Control Structures</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Projects Practice</td>
<td>Version Control Practice</td>
</tr>
<tr>
<td></td>
<td>Media Management Practice</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Terms of Reference</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Document Review Practice</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CHECK</th>
<th>Management Review (overview)</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Management System Review Practice</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Internal/External Audit and Management Review Schedule</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Management Review Index</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Management Review Checklist</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Customer Feedback (Instructions and Results)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ACT</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>To Do List</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Preventive and Corrective Action</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Improvements</td>
<td></td>
</tr>
</tbody>
</table>

(c) Gamma Secure Systems Limited 2004
Gamma’s ICS Does This (3)

Business Objectives

Business Risks

Applicable?

NO

RTP – G1

YES

RTP – G2

RTPs – S1..S8

(c) Gamma Secure Systems Limited 2004
Q. Could they serve as an adequate control framework?

A. YES
ISO/IEC 17799 and BS 7799-2

3 – Have they a wider utility?
Answer to the Question

YES

- Gamma’s ICS addresses:
  - Credit Risk
  - Trading Risk
  - Market Risk
  - Quality Risk

- As well as Information Security Risk
But ISO/IEC is just IT!

- No – it’s information security not IT security
- IT security is just the same old problem in a different guise
- Internal control activities (including everything concerning financial reporting) predominately concerns information
Does ISO/IEC Recognise This?

YES

- 10.2.1 Input Validation
- 10.2.2 Control of Internal Processing
- 10.2.4 Output Validation

Transparency and disclosure rely on integrity, availability and confidentiality – the hallmarks of ISO/IEC 17799
Prospects and Limitations
Fast Track to Internal Control

- Guidance and standards exist in the public domain (although a small fee applies to some)
- A skeleton ISMS manual is available
- Standards, theory and practice of RTPs is available
- Shrink-wrapped?
  - Almost
  - All ICS have to be customised to organisation
  - Need management involvement and resources

(c) Gamma Secure Systems Limited 2004
Skeleton ISMS Manual

INTRODUCTION

Purpose

This document is the System (ISMS) Manual. The purpose of the ISMS is to identify and manage risks.

Contents

This Manual defines the scope of the ISMS and all applicable Assessment and Risk Treatment Plan and presents the St 2:2002. The SOA refers out to other relevant processes as required.

This manual details the processes and procedures for training, Internal ISMS Audit, Management Review and ISMS improvement.

Approval and Distribution Policy

This ISMS Manual was approved by the Department on 23/03/2003. It covers all risks identified in the Risk Treatment Plans.

Checklists

INTERNAL ISMS AUDIT REPORT and CHECKLIST

Covers every requirement of BS7799-2:2002
Stylised RTPs

Business driven risk assessment/treatment using events and impacts → making it all worthwhile

Organisation Specific

- One of my aircraft has broken down
- Theft
- Acts of God
- Regular Fraud
- IT failure
- Hacking
- etc

Common (but treatment might be different!)

- Possible inability to carry out some or all of the business, see F5.
- Possible unwanted disclosure of sensitive information (e.g. Groups F, K), see E5.
- Possible court action against the organisation for breach of the Data Protection Act, see E5.

The threat is the hacker.

Risk E5.1 A hacker could bring about the inability of the company to carry out an attack on the network. The first line of defence against such an attack is the firewall and it is therefore necessary to have it correctly configured to be an acceptable risk at the network level. The second line of defence is the firewall policy for "Hotfix and Service Pack upgrades". However:
Stylised RTPs

Business driven risk assessment/ treatment using events and impacts → making it all worthwhile

RISKS CONCERNING HACKING

The internal networks are connected to the Internet. There are also various methods to access the internal networks remotely and read data, modify it, introduce malware, etc. This will be affected (Groups G, D, F, H, J, K, L, M, N, P, R).

The impacts of such events are:

- Possible inability to carry out some part of the business, see E5.
- Possible unwanted disclosure of sensitive information (e.g. Groups F, K), see F2.
- Possible court action against for breach of the Data Protection Act.

The threat is the hacker.

**Risk E5.1** A hacker could bring about the inability of to carry out a planned attack on the network. The first line of defence against such an attack is the firewall, which does not know therefore whether this firewall is always correctly configured. It is considered to be an acceptable risk because there is a second line of defence in place in line with the IT policy for “Hotfix and service pack upgrades.” However:

Impacts

- Adverse press coverage
- Questions in parliament
- Court action against dep
- Failure to prosecute
- Unanticipated costs
- etc
Limitations

- **Buy and forget?**
  - *NO*
  - *Risks may be common but treatment is not*
  - *PDCA cycle requires requires continuous resource*
  - *Fast track requires senior management involvement*

- **Extension to other standards**
  - *Not a problem*
  - *Conceived as part of a whole*

- **Conclusion**
  - *The “Sky” is the limit*
Summary
Summary

- Corporate governance is a modern day imperative

- Demands an effective internal control system

- BS 7799-2 provides a coherent framework

- Information risk is more than just IT (and is captured by ISO/IEC 17799)

- Fast track methods are available, but management involvement is imperative
Thank you

I will take questions in the panel later