Security - Who is in charge? - The users? Or the system?

William List
www.gammassl.co.uk
w.list@ntlworld.com
Agenda

- Introduction
- Internal Control and Corporate Governance
- Time Metrics
- Risk Treatment Plans
- Overview of the 7799 Standards
- Fast Track ISMS
- Results
- An Exercise
- Summary and conclusions
Introduction
We all live in an insecure world

Nothing is really secure
Old Threats

- Breakdowns
- Mistakes
- Thieves
- Fraudsters
- Terrorists - bombers
- Acts of God - flood, fire, etc
New Threats

- Hackers - spammers
- Viruses
- Impersonation - pfishing
- Bugs and gremlins in the systems
Traditional Solution

Secure the perimeter of the computer (system)
And elsewhere for E-Commerce
e-Business Structure

WWW
Call Centre
Shop Front
Kiosk

Internet Technology (delivery platform)

CRM Profile

Work Flow

Middleware

Marketing
Sales
Service
Finance
Distribution

Customer
TYPICAL EC ARCHITECTURE

- Internet
- E-Commerce server
- Web Server
- Authorisation & Settlement Server
- Mainframe
  - Accounting
  - Fulfillment
  - ERP
  - ERM
  - EDI
- Database & Data warehousing
- Content building tools
- Product Catalog
- Router
- Consumer
- Consumer A/C
- Issuing Bank
- Merchant A/C
- Acquiring Bank

©Wm. List & Co, Gamma Secure Systems Limited, 2004
Three Tier Architectures

Backend Layer  |  Mid-tier Layer  |  Web Server Layer

Mainframe  |  E-Commerce servers  |  Load-balancing DNS

ERP System  |  Router

Catalog Database  |  Analysis and decision support interface

©Wm. List & Co, Gamma Secure Systems Limited, 2004
And we must remember that the programs are (heavily) patched and may be unstable
What is the system doing?

- Is it right?

- Is it authorised?

- Can I find out?
So what are we told?

- Rogue users compromise security
- Emails contain bad things
- Boards must be involved
Internal Control & Corporate Governance
Internal Control is an old concept
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
Audit Practice Board

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>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>
Applicable Risks

and non-applicable risks

<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>low</td>
</tr>
<tr>
<td>high</td>
<td>high</td>
</tr>
</tbody>
</table>

©Wm. List & Co, Gamma Secure Systems Limited, 2004
“... detect the event in sufficient time to do something positive about it...”
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
Why Corporate Governance

- … 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, EU directive

- 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.
Turnbull

- FTSE only (Yellow Book) requirement
- IC part

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'.
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.
Time Metrics
The Fundamental Principle

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

See http://www.gammassl.co.uk/topics/time/index.html
Parameter Definition (Time)

- Time that event occurs, $T_E$
- Time of detection, $T_D$ or $T_M$
- Time problem is fixed, $T_F$
- Time at which impact occurs (if not fixed), $T_W$
Parameter Definition (Money)

- Cost of doing business, $C_{BA}$
- Cost of internal control, $C_{ICS}$
- Impact penalty, $I_P$
- Cost of fix, $C_F$
Fundamental Model

- Revenue, $R$
- Cost of business activities, $C_{BA}$
- Cost of ICS, $C_{ICS}$

Money (£) vs. Time
Fundamental Model

![Diagram showing the relationship between revenue, cost of ICS, and cost of business activities over time.]

- Revenue, $R$
- Cost of ICS, $C_{ICS}$
- Cost of business activities, $C_{BA}$

Time $T_E$
Fundamental Model

\[ \text{Cost of ICS, } C_{\text{ICS}} \]

\[ \text{Cost of business activities, } C_{\text{BA}} \]

\[ \text{Revenue, } R \]

Money (£)

Time

\[ T_E \]

\[ T_W \]
Fundamental Model

Revenue, $R$

Cost of business activities, $C_{BA}$

Cost of ICS, $C_{ICS}$

Money (£)

Time

$T_E$, $T_W$, $T_M$
Fundamental Model

- **Cost of ICS, $C_{ICS}$**
- **Cost of business activities, $C_{BA}$**
- **Revenue, $R$**

Time: $T_E$, $T_W$, $T_M$, $T_F$
Fundamental Model

- Cost of ICS, $C_{ICS}$
- Cost of business activities, $C_{BA}$
- Revenue, $R$
- Time
- Money (£)
- TE, TW, TM, TF

©Wm. List & Co, Gamma Secure Systems Limited, 2004
Fundamental Model

Revenue, $R$

Cost of business activities, $C_{BA}$

Cost of ICS, $C_{ICS}$
Fundamental Model

Revenue, $R$

Cost of business activities, $C_{BA}$

Cost of ICS, $C_{ICS}$

$T_E$ and $T_W$
Fundamental Model

Cost of ICS, $C_{ICS}$

Cost of business activities, $C_{BA}$

Revenue, $R$

Time

$T_E$, $T_D$, $T_F$, $T_W$

Money (£)

$P$
Fundamental Model

Money (£) vs. Time

Revenue, $R$

Cost of business activities, $C_{BA}$

Points: $T_E$, $T_D$, $T_F$, $T_W$, $P$
## Continuum of Classes

<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>
Risk Treatment Plans
What is a Risk Treatment Plan?

- **Risk Treatment**: treatment process of selection and implementation of measures to modify risk [ISO Guide 73]

- Identification of risk
- Prevention of occurrence
- Detection of occurrence
- Limitation of Impact
- Recovery
What is a Good Risk Analysis?

- The senior management, as a whole can
  - understand the risks
  - together participate in determining optimum countermeasures to risk
  - allocate the overall ‘control’ spend to various risks across the whole business

- All staff concerned with design, implementation or performance of controls
  - to understand why the control is necessary
  - to determine when an implementation of a control fails to meet its objective
  - to understand how failures in a control are detected

- Enables prompt revisions to be undertaken as circumstances change or incidents occur

- NOTE The risk analysis can be in tiers if complex
Traditional risk analysis

- Identify
  - Assets
  - Threats
  - Vulnerabilities
  - Probability of incident occurring

- Estimate risk factor
  - Value of loss if risk occurs
  - Probability of risk occurring
  - Complex mathematics
Who knows

- All the threats - or their urgency
- All the vulnerabilities - in purchased software
- What are probabilities of occurrence

- So 9/11
DO THE BOARD UNDERSTAND THE RESULTS?
There must be a better way to explain the risk treatment plan
Suppose we start with what worries people
Worries

- No Sales
- No Money
- IT failed
- Fraud
- Regulators
- Bad press
- Info all to pot

Wrong product
- Competitors
- Too expensive
- No bribes
My Customers have not paid me

- Why not?
- Bad work
- Did not deliver
- Did not Invoice
- Customer broke
How to address worries

- Identify what they are
- Try to prevent
- Detect if materialised
- Limit impacts
- Recover
Recording the RTP

Tell the story:

- How I planned to save the business

For example:

- My airplane is broken - far away
- Impacts
  - Safety for crew and passengers
  - Customer satisfaction
  - Additional costs

This happen to us on BA 122 on 22nd November 2003 – read the Time Paper
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 vulnerabilities that may allow access to the internal networks remotely and read data, modify it, intro-duce or delete data. Groups such as K, L, M, N, P, R, Q, E, F, G, H, I, J, etc.

The impacts of such events are:

- Possible inability to carry out some or all of our business, see E5.1.
- Possible unwanted disclosure of sensitive information (e.g. Groups K, L, M, N, P, R, Q, E, F, G, H, I, J, etc.)
- Possible court action against our company for breach of the Data Protection Act.

The threat is the hacker.

Risk E5.1  A hacker could bring about our inability to carry out some operations on the network. The first line of defence against such an attack is the fire-wall. If the firewall is not adequately configured, or if it is up-to-date, the following are possible:

- Hotfix and service pack upgrades.

Event

- Aircraft broken down
- Bagage handler strike
- Theft
- Acts of God
- Regular Fraud
- IT failure
- Hacking
- etc

Organisation Specific

Common (but treatment might be different!)
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 ways for an attacker to access the internal networks remotely and read data, modify it, introduce new data or have it altered or be affected (Groups G, D, E, F, G, H, J, K, L, M, N, P, R).

The impacts of such events are:

- Possible inability to carry out some or all of our business, see E5.1, E5.2
- Possible unwanted disclosure of sensitive information (e.g. Groups F, G, J, K, L, M, N, P, R)
- Possible court action against our company for breach of the Data Protection Act

The threat is the hacker.

Risk E5.1

A hacker could bring about our inability to carry out some or all of our business on the network. The first line of defence against such an attack is the firewall. However, if it is not correctly configured, or it is undetectable, the risk can be high.

The second line of defence is the firewall, and for this reason we have implemented “Hotfix and service pack upgrades”. However:
Method

■ One RTP per event
■ Describe event
■ List assets that might be affected
■ Document, order applicable impacts
■ List applicable threats
■ Repeat until all impacts dealt with, and residual risk is acceptable:
  ➢ How can it happen?
  ➢ Do I prevent it?
  ➢ How do I detect it?
    ➢ No preventive measure or Preventive measure fails or Didn’t know it could happen that way
  ➢ How do I fix/recover?
Overview of the 7799 Standards
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
- ISO 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 •

PLAN

DO

ACT

CHECK

• 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
Linking the Two Standards

The Statement of Applicability (SOA):

“a document describing the control objectives and controls that are relevant and applicable to the organization’s ISMS, based on the results and conclusions of the risk assessment and risk treatment processes”

It is a certification requirement (EA7/03)
Why is it Important?

<table>
<thead>
<tr>
<th>A.3.1 Information security policy</th>
<th>BS ISO/IEC 17799:2000 numbering</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Control objective:</strong> To provide management direction and support for information security.</td>
<td>3.1</td>
</tr>
<tr>
<td><strong>A.3.1.1 Information security policy document</strong></td>
<td>3.1.1</td>
</tr>
<tr>
<td>A policy document shall be approved by management, published and communicated, as appropriate, to all employees.</td>
<td></td>
</tr>
<tr>
<td><strong>A.3.1.2 Review and evaluation</strong></td>
<td>3.1.2</td>
</tr>
<tr>
<td>The policy shall be reviewed regularly, and in case of influencing changes, to ensure it remains appropriate</td>
<td></td>
</tr>
</tbody>
</table>

- You have to say, for all 127 ISO/IEC 17799 controls, whether they are applicable or not
- If YES, why (with reference to risk assessment)
- Important because everyone uses the same laundry list
A Practical Implementation

Policy statements
(could be imposed by higher authority)

Risk assessment
risk treatment plan

Link backs

A.x.x.x Clause
A.x.x.y Clause

YES, policy xyz, events, abc
see reference

N/A reason

normative

informative

Link forward to procedure manuals etc.
Fast Track ISMS
The Vital Ingredients

- Role Model
- Skeleton ISMS Manual
- The event-impact driven RTPs (as previously discussed)
- Classroom and on-the-job training
- Various quality assurance activities
Role Model

- Information Security Forum (ISF)
- ISMS Administrator
- Internal ISMS Auditor
- ISMS Trainer
- ISMS Advisor
- Certification Auditor
- Policy Maker

Acts to reduce risk to acceptable level

Owns/looks after ISMS
Manages Policy Makers
Set Civil Service-wide policy
Provides management information
Owning
Provides feedback/ request policy enhancements
Provide feedback
Provide feedback
Provide feedback
Instruct and monitor
Use
Acts to reduce risk to acceptable level

©Wm. List & Co, Gamma Secure Systems Limited, 2004
Skeleton ISMS Manual

INTRODUCTION

Purpose

This document is "<State name of Department (note you) ISMS Manual". The purpose of the ISMS is to manage risks.

Contents

This Manual defines the scope of the ISMS and all applicable Assessment and Risk Treatment Plan and presents the Security Policy. The SOA refers to other relevant processes and procedures in support of the ISMS.

Approval and Distribution Policy

This ISMS Manual was approved by the Department on <date> and distributed according to the approval and distribution policy identified in the Risk Treatment Plan.

Covers every requirement of BS7799-2:2002
Contents

- Pages associated with the whole PDCA cycle
- Built-in facility for document control
- Space to define ISMS scope and context
- Prototype ISMS policy
- Provision for RTPs
- Virtually complete SOA (with built-in hyperlinks to policy statements and standard events)
- Facility for including training and awareness
- Internal ISMS audit proforma and checklist
- Management system review checklist
- Procedures for corrective action etc.
- To-Do-List and associated procedures
- Compliance index
The “To-Do-List”

- BS 7799-2 is a management standard – so is internal control
- Management processes must be in place, but new security processes may be required because risks change
- At any point in time:
  - Existing security procedures in place
  - Newly identified ones still-to-do
- Managed using a “To-Do-List”
The "To-Do-List"

**The To-Do-List**

<table>
<thead>
<tr>
<th>Reference</th>
<th>Action</th>
<th>Target Date</th>
<th>Comment/Completion Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extend scope of MS to include BS7799-2</td>
<td>Produce SOA</td>
<td>040402</td>
<td>040331</td>
</tr>
<tr>
<td></td>
<td>Produce scope statement</td>
<td>040402</td>
<td>040331</td>
</tr>
<tr>
<td></td>
<td>Produce context (i.e. information architecture)</td>
<td>040402</td>
<td>040331</td>
</tr>
<tr>
<td></td>
<td>Integrate checklists into current MS, modify existing MS Review practice accordingly</td>
<td>040402</td>
<td>040331</td>
</tr>
<tr>
<td></td>
<td>Produce RTPs (just the standard 8) and link with business risk analysis</td>
<td>040402</td>
<td>040331</td>
</tr>
<tr>
<td></td>
<td>Insert compliance statement from Skeleton and check all cross refs</td>
<td>040402</td>
<td>040331</td>
</tr>
</tbody>
</table>
Results
Some Results

UK Logistics Company
- Initial development of Skeleton
- First application of event-impact driven RA/RTPs
- Engaged Board
- MD in control

UK start-up
- Up to speed in a day
- 2 day brainstorm for RTPs
- First BSI visit in September

Government of Mauritius
- 4 sites “attested” by MSB
- Chiefs empowered
- Rollout to all other departments
Principle can be extended

- Overall ICS

- Including
  - ISO 9000
  - Financials
  - General management issues
Now an audience participation exercise

Identity Cards
Summary and Conclusions
Computers help people

- PCs, mobile phones, mainframes, servers etc

- Could we do without them?
  - **Volume of transactions**
  - **Speed of communications**

- Criminals are businesses too
Summary

- Information security part of internal control
- Time metrics key to effectiveness
- Event-impact driven RA/RTPs key to Board engagement
- Hypertext, web-technology Skeleton key to rapid development
- Certification successes bear this out
Security - Who is in charge? - The users? Or the system?

William List
www.gammassl.co.uk
w.list@ntlworld.com