IT FACULTY ROADSHOW

You’re In Charge - That’s what you think!
You’re In Charge - That’s what you Think!

William List & Dr. David Brewer
www.gammasssl.co.uk
w.list@ntlworld.com  dbrewer@gammasssl.co.uk
Agenda

- Introduction
- Internal control and corporate governance
- Risk treatment plans (RTPs)
- Time metrics
- Introduction to Management System Standards
- Fast Track ISMS
- Results
  - An Example of a fully integrated ICS covering all business risks
- Summary and conclusions
Today

- Business is dependent on IT
- IT is complex - even on a PC
- Who really understands the systems?
- Do IT controls fit in with the business?
- How does the Board engage with IT?
Practical Issues

- Is information security part of internal control or something different?
- Engaging the Board (some think it is only an IT issue)?
- Ensuring RA reflects business objectives
- How do you measure effectiveness?
Our Objective

“Tell it like a story” RTPs

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

All business risks are covered

Just the right level of control – not too much, not too little

Management system to establish and police ICS

“Fast Track” takes the drudgery away
What we have also done

- Built an ICS management system template in hypertext
  - *Will use Gamma as an example*

- Linked MS to detailed procedures also in hypertext

- All admin matters built in to template
Corporate Governance
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, environment 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.
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.
Audit Practices Board

This is their advice:

1. Mission
2. Business Objectives
3. Business Risks
4. Applicable Risks
5. Internal Controls
6. Review

**Only Applicable Risks?**

**Note the Deming cycle**
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)
Running a business

Processes for

- Selling the product
- Making the product
- Occupying premises
- Employing people
- Keeping the records

Later

- Reporting externally
- Multiple jurisdiction issues
Some Examples of controls

- Management accounts
- Double entry bookkeeping
- Bank reconciliations
- Access Controls
- Business recovery
“… 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
Too many controls?

- Think of all perils
- Put in a control
- Overlap?
- Create more to combat incidents
- Create more to placate auditors
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 RTP?

- 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 treatment can be in tiers if complex
Applicable Risks

and non-applicable risks

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

Area of applicable risk

©Wm. List & Co, Gamma Secure Systems Limited, 2004
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
DO THE BOARD UNDERSTAND THE RESULTS?
Worries

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

Wrong product
- Competitors
- Too expensive
- No bribes
How to address worries

- Identify what they are
- Try to prevent
- Detect if materialised
- Limit impacts
- Recover
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 ways to access the internal network remotely and read data, modify it, introduce it, be affected. (Groups: E, F, G, H, 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
- Possible unwanted disclosure of sensitive information (e.g. Groups E, F, G, H, 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. The first line of defence against such an attack is the firewall, whether it be hardware or software. If it is unacceptably configured, or if it is unacceptably positioned, then the second line of defence may be software or hardware firewalls. This line of defence is flawed if it is not adequate, or if it is not supported by other controls such as “hotfix and service pack upgrades”. However:

Event

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

©Wm. List & Co, Gamma Secure Systems Limited, 2004
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 sites which access the internal networks remotely and read data, modify it, introduce viruses which could be affected (Groups C, D, E, F, G, H, I, 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 E, F)
- 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 the network. The first line of defence against such an attack is the firewall, therefore whether this firewall is always correctly configured, or it is under an acceptable risk because there is a second line of defence, which lies in “Hotfix and service pack upgrades”. However:

**Impacts**

- Adverse press coverage
- Questions in parliament
- Court action against org
- Failure to prosecute
- Unanticipated costs
- *etc*
An Example

RISKS CONCERNING IT FAILURE

We are reliant on our IT. The technology could fail for a wide variety of reasons and in a wide variety of manners. Broadly speaking, the failure will result in unavailability, loss of integrity and/or loss of confidentiality. Note that integrity also implies that information is sufficiently right for the purpose for which it is used at the time that it is used, and not just that data has been modified without authorization or in error. All IT based assets could be affected (Groups E, F, I, J, K).

The impacts of such events are:

- Possible inability to carry out some or all of our business, see S4.1a, S4.1b, S4.1c, S4.1d, S4.1e
- Possible unauthorised disclosure of protectively marked, sensitive or client sensitive information, see S4.2

The principal threats are backup failure, errors, utility failure, software failure and viruses.
An Example (continued)

**Risk S4.1a**  IT failure could be due to a power failure. The outage that could be tolerated before power/communications was restored is a few hours (the duration of the laptop batteries). This is an acceptable risk.

**Risk S4.1b**  Telecommunications could fail, denying the ability to make or receive phone calls, e-mail access and web connectivity. However, all staff have a mobile phone. All offices, including staff residences have broadband via cable, BT copper and mobile telephone facilities. Mobiles are regularly backed up. The risk of all of these failing at a time when it is imperative that communications is established is acceptable.

**Risk S4.1c**  IT failure could also be caused by a virus (as described addressed S5-risks concerning hacking) but instigated inadvertently by an authorised user rather than by a hacker. The defence is the antivirus measures that run in the background. Their failure is an acceptable risk.
An Example (continued)

Risk S4.1d  Software failure may be yet another cause, usually evidenced by the "blue death". This is countered in the first instance by making regular "save files". In the worst case it requires the regeneration of systems and data from backups. This is discussed in S1.3b and is an acceptable risk. The acceptability of risk concerning long term backup failure has been been investigated and has proved to be an acceptable risk.

Risk S4.1e  Yet another way that the IT systems may impact on the ability to carry out some or all of our business is due to a violation of integrity. Physical and logical access controls are used to prevent one user from interfering with the work of another. To counter error, regular save files using different file names is encouraged. The failure of either strategy is an acceptable risk.

Risk S4.2  Physical and logical access controls are also used to prevent unauthorised disclosure of information. The use of these controls presents an acceptable risk.

Etc
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
Risk Treatment Plans

Tell it like a story

Methodology

- Good plot
- Happy ending

Uses time metrics

Ask “what if it doesn’t work?”

Encourages well formed controls (i.e., self-policing)

Risks Concerning Hacking

The internal networks are connected to the Internet. There are also various modern access the internal networks remotely and read data, modify it, introduce maliciously be affected (Groups C, D, E, F, G, H, I, 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, E5.3, E5.4.
- Possible unwanted disclosure of sensitive information (e.g. Groups E, K), see E5.2.
- 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. The ISP is therefore whether this firewall is always correctly configured, or if it is under attack. Nevertheless, an acceptable risk because there is a second line of defence, which lies in hardening the “Hotfix and service pack upgrades”. However:
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
Fundamental Model (too late)

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

$P$
Fundamental Model (too late)
Fundamental Model (too late)

Revenue, R

Cost of business activities, C_{BA}

Cost of ICS, C_{ICS}

Time

Money (£)

T_E

T_W

P

©Wm. List & Co, Gamma Secure Systems Limited, 2004
Fundamental Model (too late)
Fundamental Model (too late)
Fundamental Model (too late)
Fundamental Model (too late)
Fundamental Model (too late)
Fundamental Model (in time)

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

Money (£) vs. Time

P
Fundamental Model (in time)

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

Time

Money (£)

$T_E$, $T_W$
Fundamental Model (in time)

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

- Time: $T_E$, $T_D$, $T_F$, $T_W$
Fundamental Model (in time)

Time

- $T_E$
- $T_D$
- $T_F$
- $T_W$

Money (£)

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

$P$
Fundamental Model (in time)

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

Time: $T_E$, $T_D$, $T_F$, $T_W$
## 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>
Example – Setting the Scene

- Small software company
- ICS relies solely on program testing and backup
- Experienced, knows what can go wrong
- Bidding for new fixed price contract (dev + maint)
- Should it have a better ICS?
Example – Experience Data

Rework required if design error detected in month $M$

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$1/20$</td>
<td>$3/20$</td>
<td>$1/4$</td>
<td>1.5</td>
<td>1.5</td>
<td>1.5</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>4.5</td>
<td>6</td>
<td>8</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

©Wm. List & Co, Gamma Secure Systems Limited, 2004
Example – Candidate ICS

Case 1 – leave ICS as it is

- Worst case detect error in M11

Case 2 – better testing techniques

- Costs more, detect error in M6, positive impact on maintenance

Case 3 – design reviews (+ training)

- Costs more, detect error in M3, some impact on maintenance

Case 4 – design reviews (with experienced programmer)

- Costs more, detect error in M3, some impact on maintenance

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/20</td>
<td>3/20</td>
<td>1/4</td>
<td>1.5</td>
<td>1.5</td>
<td>1.5</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>4.5</td>
<td>6</td>
<td>8</td>
</tr>
</tbody>
</table>

ICS#1

ICS#2

ICS#3 & 4
### Example - Results

<table>
<thead>
<tr>
<th>Event occurs</th>
<th>Profit (in some monetary unit)</th>
<th>ICS#1</th>
<th>ICS#2</th>
<th>ICS#3</th>
<th>ICS#4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>(5.5)</td>
<td>6.8</td>
<td>9.8</td>
<td>8.8</td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>9</td>
<td>8.3</td>
<td>10</td>
<td>9</td>
<td></td>
</tr>
</tbody>
</table>

The bottom line effectiveness of the four candidate ICS (fixed price)

1. No change
2. Better s/w testing
3. Design reviews
4. As 3 + experienced staff
Example – What if T & M?

But bid fixed price on maintenance if ICS#2, 3 or 4...

<table>
<thead>
<tr>
<th>ICS</th>
<th>(event occurs)</th>
<th>(no event)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Profit</td>
<td>Client pays</td>
</tr>
<tr>
<td>#1</td>
<td>12.4</td>
<td>81.9</td>
</tr>
<tr>
<td>#2</td>
<td>16.1</td>
<td>75.9</td>
</tr>
<tr>
<td>#3</td>
<td>10.3</td>
<td>68.8</td>
</tr>
<tr>
<td>#4</td>
<td>14.3</td>
<td>73.8</td>
</tr>
</tbody>
</table>

The bottom line effectiveness of the four candidate ICS for a mix of T&M (dev) and FP (man). ICS#1 T&M for both phases

1. No change
2. Better s/w testing
3. Design reviews
4. As 3 + experienced staff
Example - Conclusions

- The time to detect clearly has an effect on the overall effectiveness and the bottom line.

- The best operationally effective ICS is not necessarily the most cost effective.

- Note how cost effectiveness changes with the environment (e.g. fixed price versus time and materials).
Measuring the effectiveness of an internal control system

by Dr. David Brewer and William List, CA, Hon FBCS

The objective of this paper is to propose a methodology by which management can measure the effectiveness of the organisation’s Internal Control System (ICS). In addition the paper proposes a methodology for recording Risk Treatment Plans (RTPs), which improve the communication between risk specialists and senior management. This methodology incorporates our concepts for classifications of ICS.

The ICS is the way in which the management deploys the organisation’s resources to achieve the organisation’s objectives.

The ICS exists in two basic parts:

- Procedures to perform the work necessary to conduct the organisation’s business. These are called operational procedures.
- Procedures to ensure that the business is conducted as expected. These are called controls.

It is this second part of the ICS which this paper examines.

All organisations have an ICS. In large organisations it is formalised; in the very small
IT FACULTY ROADSHOW

You’re In Charge - That’s what you think!
Management Systems
Management Systems

- The means by which management establishes and policies its internal control system

- I.e the procedures/processes for realising the APB model

- There are ISO standards that do this

- Best fit is BS 7799-2:2002
Attributes of a Management System

Defined management systems include

- Active management involvement
- Maintenance of records
- Document control
- Evidence of performance
- To Do List of some sort

Has always been part of internal control
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?

Effective Security in tune with the business.
BS 7799-2:2002

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

This is the Deming cycle

An incident is the occurrence of an impact

©Wm. List & Co, Gamma Secure Systems Limited, 2004
I can also tell if it is working

Good design ensures that controls detect all events in sufficient time…

May need to take action

- Preventive Action
- Corrective Action
- Management Review
- Internal ISMS Audit
- ISMS Improvements

“Check” activities check the controls

If not there will be an incident
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?

| A.3.1 Information security policy |  |
| Control objective: To provide management direction and support for information security. | 3.1 |

**Controls**

| A.3.1.1 Information security policy document | A policy document shall be approved by management, published and communicated, as appropriate, to all employees. | 3.1.1 |
| A.3.1.2 Review and evaluation | The policy shall be reviewed regularly, and in case of influencing changes, to ensure it remains appropriate | 3.1.2 |

- 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
YES, policy xyz, events, abc
see reference

A.x.x.y Clause
N/A reason

informative

normative

Link forward to procedure manuals etc.
ISO/IEC 17799:2000

Provides guidance under 10 major headings
a check list for information security controls

- 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 17799:2000

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

The Blue parts apply to all management systems.

©Wm. List & Co, Gamma Secure Systems Limited, 2004
Book keeping checklist

- Ensure completeness of input
- Evidence of completeness of output
- Reconcile bank accounts
- Has ICAEW software evaluation functionality
- Etc
Accounts Preparation Checklist

- Analyse fixed assets
  - Cost: accumulated depreciation: net
- Analyse turnover: geographically
- Specify shareholdings: major: directors: etc
- Contingent liabilities
- Directors remuneration: options: etc
- Etc
Benefits

- Provides a means to realise APB model
  - Not only a means to demonstrate effectiveness
  - But also, continual improvement

- Engages the Board members

- ISO/IEC 17799 super checklist for information security, but don’t forget finance, quality etc

- Top down approach starting with corporate governance
Top Down

Corporate Governance

Internal Control

Mission
Business Objectives
Business Risks
Applicable Risks
Internal Controls
Review

Management System

Checklists/ codes of best practice

Scope • ISMS Improvements
Policy • Preventive Action
Risk Assessment (RA) • Corrective Action
Risk Treatment Plan (RTP) • Management Review
Statement of Applicability (SOA) • Internal ISMS Audit
Operate Controls • Manage Resources
Awareness Training • Prompt Detection and Response to Incidents
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) Management Forum
  
- (IS)MS Administrator

- Internal (IS)MS Auditor

- (IS)MS Trainer

- (IS)MS Advisor

- Certification /external auditor (optional)

- Policy Maker

Or simply the Board
Skeleton ISMS Manual

INTRODUCTION

Purpose

This document is <<State name of Department (note you’re doing System (ISMS) Manual”). The purpose of the ISMS is to identify and manage the risks.

Contents

This Manual defines the scope of the ISMS and all applicable Assessment and Risk Treatment Plan and presents the Scope 2:2002. The ISMS refers to other relevant processes and procedures.

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 <<State here the distribution policy for this ISMS Manual’s approved on >>.

Parts for you to complete

Covers every requirement of BS7799-2:2002 Extensible to finance, quality etc.
Contents

- Pages associated with the whole PDCA cycle
- Built-in facility for document control
- Space to define scope and context
- Prototype policy
- Provision for RTPs
- Virtually complete checklists (with built-in hyperlinks to policy statements and standard events)
- Facility for including training and awareness
- Internal 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"

BS 7799-2 is a management standard, so is... 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, with MD in control
- Balance of control spend

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

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

- ✓ Resource Availability
- ✓ Expertise of ISMS Team
- ✓ Commitment of Management
- ✓ Tight Schedule
- ✓ Lack of confidence

## Outcome

- ✓ Security Awareness
- ✓ Higher Confidence
- ✓ Security Culture
- ✓ Empowerment
- ✓ Improved Security
- ✓ Enriching experience
- ✓ Feeling of Satisfaction
An Example of a Fully Integrated ICS
Welcome to Gamma

Here you will find a guide to the wide range of our useful information on IT-related topics. The Gamma Security Evaluation Criteria (ITSEC), a hard copy of which is available from us, is a new and important tool for anyone involved in the selection and design of security solutions. We offer a wide range of information security consultancy services. We can help you to gain BS 7799-2 certification quickly using our 'Fast Track' method, and integrate quality and security into your business plan. We offer training in information security management, and will train you to train others. Our BS 7799-2 services start with establishing the business plan, and guide you throughout the process towards successful certification. We carry out a wide variety of research and strategic studies. Why not let us help you? Innovation and good value are our strengths.

You may contact us by phone, e-mail or drop us a line in our Visitor's Book, or perhaps we may meet at an event. We would be very pleased to hear from you. Click here to see our offices and learn about our partners worldwide.

©Wm. List & Co, Gamma Secure Systems Limited, 2004
Summary and Conclusions
Summary

- Internal control addresses all risks (quality, information security ... as well as financial)
- Time metrics key to effectiveness
- Event-impact driven RA/RTPs key to Board engagement
- Hypertext, web-technology Skeleton key to rapid development
- It works and you can show it works
Our Objective

“Tell it like a story” RTPs

“All business risks are covered"

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

“Fast Track” takes the drudgery away

Just the right level of control – not too much, not too little

Management system to establish and police ICS

©Wm. List & Co, Gamma Secure Systems Limited, 2004
“Take Away”

- Does your ICS address all business risks?
- Can you find out events in good time?
- Construct some RTPs
  - Not enough control?
  - Too much control?
- Are you making best use of IT in managing your ICS?
You’re In Charge -
That’s what you Think!

Questions and Discussion
IT FACULTY ROADSHOW

You’re In Charge - That’s what you think!