Rolling out ISO/BS (1)7799 in the Real World

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

- Introduction
- Overview of the 7799 standards
- Practical issues
- Internal control and corporate governance
- Time metrics
- Risk treatment plans (RTPs)
- Fast Track I SMS
- Results
  - An Example of a fully integrated ICS covering all business risk, including quality and information security
- Summary and conclusions
Overview of the 7799 Standards
World-wide Take Up

BS 7799-2 Registrations by Continent

Growth of BS7799-2 Registrations World Wide

©Wm. List & Co, 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?

Effective Security in tune with the business
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

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?

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

<table>
<thead>
<tr>
<th>Controls</th>
<th>BS ISO/IEC 17799:2000 numbering</th>
</tr>
</thead>
<tbody>
<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
YES, policy xyz, events, abc see reference

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

Link forward to procedure manuals etc.
A Practical Implementation

Policy statements
(could be imposed by higher authority)

Risk assessment
risk treatment plan

Link backs

normative

Link forward to procedure manuals etc.

A.x.x.x Clause
YES, policy xyz, events, abc
see reference

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

©Wm. List & Co, Gamma Secure Systems Limited, 2004
A Practical Implementation

Policy statements
(could be imposed by higher authority)

Link backs

Risk assessment
risk treatment plan

YES, policy xyz, events, abc
see reference

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

A.x.x.x Clause

informative

normative

Link forward to procedure manuals etc.
Practical Issues
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
- Tediousness of creating SOA, volumes of documentation/records etc
- Costs, resources and time to set up and administer, certification etc
- How do you measure effectiveness?
What We Have Done

1. Is information security part of internal control or something different?
2. Engaging the Board (some think it is only an IT issue)?
3. Ensuring RA reflects business objectives
4. Tediousness of creating SOA, volumes of documentation/records etc
5. Costs, resources and time to set up and administer, certification etc
6. How do you measure effectiveness?
What We Have Done

1. Is information security part of internal control or something different?
2. How do you measure effectiveness?
3. Engaging the Board (some think it is only an IT issue)?
4. Ensuring RA reflects business objectives
5. Tediousness of creating SOA, volumes of documentation/records etc
6. Costs, resources and time to set up and administer, certification etc
What We Have Done

Time Paper

- **Internal control**
- **Time & cost metrics**
- **Event-impact driven RTPs**

Fast Track ISMS paper

Results

1. Is information security part of internal control or something different?
2. How do you measure effectiveness?
3. Engaging the Board (some think it is only an IT issue)?
4. Ensuring RA reflects business objectives
5. Tediousness of creating SOA, volumes of documentation/records etc
6. Costs, resources and time to set up and administer, certification etc
Internal Control & 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 etc.

- Turnbull, OECD, Sarbanes-Oxley, EU directive
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'.

- 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.
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:
## Risks – a Taxonomy

### Following Basel II

<table>
<thead>
<tr>
<th>Primary Risk Category</th>
<th><strong>Definition:</strong> the risk of loss arising from ...</th>
<th><strong>Associated Operational Risk:</strong> 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>Area of applicable risk</td>
</tr>
<tr>
<td>high</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>X</td>
</tr>
<tr>
<td>low</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>X</td>
</tr>
<tr>
<td>low</td>
<td>X</td>
</tr>
<tr>
<td>low</td>
<td>X</td>
</tr>
<tr>
<td>low</td>
<td>X</td>
</tr>
<tr>
<td>low</td>
<td>X</td>
</tr>
<tr>
<td>high</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>X</td>
</tr>
<tr>
<td>high</td>
<td>X</td>
</tr>
</tbody>
</table>

©Wm. List & Co, Gamma Secure Systems Limited, 2004
Controls – Fundamentals

“… 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
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 (too late)

Revenue, $R$

Cost of business activities, $C_{BA}$

Cost of ICS, $C_{ICS}$

Money (£)

Time

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

Money (£)

Time $T_E$ $T_W$

Revenue, $R$

Cost of business activities, $C_{BA}$

Cost of ICS, $C_{ICS}$

$P$

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

Revenue, $R$

Cost of ICS, $C_{ICS}$

Cost of business activities, $C_{BA}$

Money (£)

Time

$T_E$

$T_W$

$T_M$

$P$
Fundamental Model (too late)

<table>
<thead>
<tr>
<th>Time</th>
<th>Revenue, R</th>
<th>Cost of business activities, C_{BA}</th>
<th>Cost of ICS, C_{ICS}</th>
</tr>
</thead>
<tbody>
<tr>
<td>TE</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TW</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TM</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TF</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

![Diagram showing the relationship between money ($) and time (T_E, T_W, T_M, T_F) with lines representing revenue (R) and cost of business activities (C_{BA}).]
Fundamental Model (too late)

- Revenue, $R$
- Cost of business activities, $C_{BA}$
- Time: $T_E$, $T_W$, $T_M$, $T_F$
- Money (£)

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

Money (£)

Time

Revenue, R

Cost of business activities, C_{BA}

Cost of ICS, C_{ICS}

P
Fundamental Model (in time)

- Revenue, $R$
- Cost of business activities, $C_{BA}$
- Cost of ICS, $C_{ICS}$
- Time, $T_E$, $T_W$
- Money (£), $P$
Fundamental Model (in time)

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

Time: $T_E, T_D, T_F, T_W$

Money (£)
Fundamental Model (in time)

Money (£) vs. Time

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

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

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

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

$P$
# 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>
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

<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>Top Level Design</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>Module Design</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>Coding/Unit Tests</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>Integration Tests</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>Acceptance Tests</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>

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></td>
<td>$\frac{1}{20}$</td>
<td>$\frac{3}{20}$</td>
<td>$\frac{1}{4}$</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>
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

<p>| | | | | | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>10</td>
<td>11</td>
</tr>
<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>
</tr>
</tbody>
</table>
Example - Results

<table>
<thead>
<tr>
<th>Event occurs</th>
<th>Profit (in some monetary unit)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ICS#1</td>
</tr>
<tr>
<td>Yes</td>
<td>(5.5)</td>
</tr>
<tr>
<td>No</td>
<td>9</td>
</tr>
</tbody>
</table>

The bottom line effectiveness of the four candidate ICS (fixed price)
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.
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).
What Else is in the Paper

- Background
- True stories
- Classes and categories
- Operational effectiveness
- Cost effectiveness
- Measuring improvement
- Risk treatment plans
- Conclusions
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
DO THE BOARD UNDERSTAND THE RESULTS?
Who knows

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

- So 9/11
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
RISKS CONCERNING HACKING

The internal networks are connected to the Internet. There are also various more sophisticated methods to access the internal networks remotely and read data, modify it, introduce faults etc. e.g. E5. Possible hackers, e.g. N, L, N, P, R.

The impacts of such events are:

- Possible inability to carry out some or all of the business, see E5.
- 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 legislation.

The threat is the hacker.

Risk E5: A hacker could bring about the inability of the organisation to carry out business on the network. The first line of defence against such an attack is the firewall and it is not known therefore whether this firewall is always correctly configured to be an effective barrier. The second line of defence is the organisation's 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 means to access the internal networks remotely and read data, modify it, introduce malware or be affected (Groups C, D, E, F, G, H, J, K, L, M, N, P, R).

The impacts of such events are:

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

The threat is the [redacted].

Risk E5.1 A hacker could bring about the inability of [redacted] to carry out a particular attack on the network. The first line of defense against such an attack is the firewall. The [redacted] 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 defense, viz. adherence with the IT policy for “Hotfix and service pack upgrades”. However:

Impacts

- Adverse press coverage
- Questions in parliament
- Court action against org
- Failure to prosecute
- Unanticipated costs
- etc
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?
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
Skeleton ISMS Manual

INTRODUCTION

Purpose

This document is <<State name of Department (note you System (ISMS) Manual”. The purpose of the ISMS is ensure risks.

Contents

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

Approval and Distribution Policy

This ISMS Manual was approved by the Department on <<State here the distribution policy for this ISMS Manual.>>

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

- 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
Results

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

**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

**Specialist UK IS consultancy**
- Fully integrated ICS/MS
- Certified ISO 9001:2000
- Certified BS 7799-2:2002
Information Security Seminar  
on 29 April 2004  
at La Petite Cannelle,  
Domaine Les Pailles

- **Session I: Opening**
  - 9:00 - 9:30  Registration
  - 9:30 - 9:40  Welcome address by Mrs Aubeelack, PS, Ministry of IT & Telecommunications
  - 9:40 - 10:00  Opening address by Honourable D. Jocha, Minister of IT & Telecommunications

- 10:00 - 10:15  Introduction to ISO/IEC 17799 Security Standards by Dr Brewer / Mr List
- 10:15 - 10:30  Implementing ISO/IEC 17799 Security Standards in the Civil Service by Dr Brewer / Mr List

- **Session II: Implementing ISO/IEC 17799 Security Standards - The Pilot Sites Experience**
  - 10:45 - 11:00  The Contributions Branch
  - 11:00 - 11:15  The Civil Status Division
  - 11:15 - 11:30  The Treasury Department
  - 11:30 - 11:45  The Passport & Immigration Office

- **Session III: Certification**
# Overall Timescales

<table>
<thead>
<tr>
<th>Project week</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>
<th>13</th>
<th>14</th>
<th>15</th>
<th>16</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial training/supervision</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>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISMS manual completed</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>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Quality assurance</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>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Internal audit programme initiated</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>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Training/awareness programme initiated</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>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Certification audits</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>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- 4 months from standing start to *attestation*
- Senior management now own the problem, discovered subtle problems in current business procedures
- RTPs + Skeleton were key
- 2 hr desktop audit gained unbelievable confidence in methodology
- ½ - 1 day MSB audits (and they got faster)
An Example of a Fully Integrated System –
Gamma Secure Systems Limited
ISO 9001 + BS 7799-2 certified
Welcome to Gamma

Here you will find a summary of useful information on ISO/IEC 17799, BS 7799-2 and the Common Criteria, and a host of other interesting information security topics ranging from reprogrammable smart cards to internal control and corporate governance.

We offer a broad range of information security consultancy services. We can help you gain BS 7799-2 certification quickly using our 'Fast Track' method, and integrate quality and security into your internal control system. We offer training in information security management, and will teach you to train others. Our Common Criteria services start with establishing the business plan, and guide you throughout the process to successful certification. We carry out a wide variety of research and strategic studies. Why not let us help you? Innovation and great 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 world-wide.

STOP PRESS
Gamma is now BS 7799-2 certified. Click here to read all about it.

RISKS CONCERNING NON-APPLICABLE RISKS
It is possible that a non-applicable risk becomes an applicable risk.

All assets could be affected, but primarily Asset Groups Y and Z.

RISKS CONCERNING IT FAILURE
Gamma is reliant on its IT. The technology could fail for a wide variety of reasons and in a wide variety of manners. Broadly speaking, the failure will render infeasible, 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 1, 2, 4, 5, 6).

The impacts of such events are:
- Possible inability to carry out some or all of Gamma's business, see E1A.
- Possible unauthorized disclosure of sensitive information, see E1A.
- Possible unauthorized alteration of sensitive information, see E1A.
- Possible denial of service, see E1A.

©Wm. List & Co, Gamma Secure Systems Limited, 2004
# Development History

<table>
<thead>
<tr>
<th>Date</th>
<th>APB</th>
<th>Paperless</th>
<th>Basel</th>
<th>RTPs</th>
<th>QMS</th>
<th>ISMS</th>
<th>Certification</th>
</tr>
</thead>
<tbody>
<tr>
<td>JUN 2001</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAR 2003</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAY 2003</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td>9001:2000</td>
</tr>
<tr>
<td>APR 2004</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>JUL 2004</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓ BS 7799-2</td>
</tr>
</tbody>
</table>

- Upgrade to BS 7799-2 took 6 days of effort

- Future – add in metrics
Benefits

- ICS key to mission success
- Everything is just “one click away”
- No bureaucracy
- Firm management control on attainment of business objectives and business risk management
- One ICS, one MS, one certification audit, two standards
Summary and Conclusions
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