Information Security Management
ISO/IEC 27001 and Internal Control

Dr. David Brewer
Mr. William List, CA, hon FBCS
Themes

- Information Security Management Systems (ISMS)
- BS 7799-2 migration to ISO/IEC 27001
- COSO Audit and Risk Management
- How this all fits together
- How it can be done in practice
Agenda

- Introduction to Information Security Management Standards
- Relation with other standards, laws and regulations
- Methodology
- Commercial application
- Case study
The ISMS Standards

- ISO/IEC 27001 is a management standard – e.g. let’s party. It tells you what to do

- ISO/IEC 17799 is a supermarket of good things to do

- Certification, performed by an accredited certification body in accordance with EA7/03, is against 27001 – is the party OK?
International standardisation

- BS 7799-2:2002
- ISO/IEC 17799:2005
- Annex B of BS 7799-2
- Current work on metrics
- EA7/03

- ISO/IEC 27001:2005
- ISO/IEC 27002:2007
- ISO/IEC 27003
- ISO/IEC 27004
- IAF document
ISO/IEC 27001
Information Security Management Systems - Requirements
ISO/IEC 27001

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
- ISMS Improvements
- Preventive Action
- Corrective Action

Do
- Management Review
- Internal ISMS Audit

Check

This is the Deming cycle
Risk Treatment Plans

- Policy
  - Risk Assessment (RA)
  - Risk Treatment Plan (RTP)
- Scope
- Statement of Applicability (SOA)
- Operate Controls
- Awareness Training
- Manage Resources
- Prompt Detection and Response to Incidents
- MS Improvements
- Preventive Action
- Corrective Action
- Management Review
- Internal Audit
c) Define the risk assessment approach of the organization.

1) Identify a risk assessment methodology that is suited to the ISMS, and the identified business information security, legal and regulatory requirements.

2) Develop criteria for accepting risks and identify the acceptable levels of risk. (see 5.1f)).

The risk assessment methodology selected shall ensure that risk assessments produce comparable and reproducible results.

NOTE: Some methodologies are discussed in IT Security and Management — Techniques for the management of IT Security.

There are different methodologies for risk assessment

- assets
- threats
- vulnerabilities
- impacts
ERM Defined:

“... a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.”

A Choice of Approach

■ Thousands of calculations
  ➢ Asset * Threat * Vulnerability
  ➢ Some methods simplify this with tables
  ➢ But if asset = 0, risk = 0
  ➢ Asset value depends on event and impact

■ Does the Board understand the results?
With events and impacts, they do 😊

Why not start with these
Event Identification

- Differentiates risks and opportunities.
- Events that may have a negative impact represent risks.
- Events that may have a positive impact represent natural offsets (opportunities), which management channels back to strategy setting.
Statement of Applicability
Statement of Applicability (SOA)

- Go through all 133 controls
- Say whether applicable or not

Policy statements
  (could be imposed by higher authority)

Risk assessment
risk treatment plan

Link back
A.x.x.x Clause
A.x.x.y Clause

YES, policy xyz, events, abc
see reference
N/A reason

Link forward
normative
to procedure manuals etc.

informative

©Gamma Secure Systems Limited, Wm List & Co., 2006
Management Reviews

- Policy
- Risk Assessment (RA)
- Risk Treatment Plan (RTP)
- Statement of Applicability (SOA)
- Operate Controls
- Awareness Training
- Manage Resources
- Prompt Detection and Response to Incidents
- Scope
- MS Improvements
- Preventive Action
- Corrective Action
- Management Review
- Internal Audit
The RTP owners periodically take stock of the ISMS – is it effective?

**INPUTS**
- Results of ISMS audits and reviews
- Incident reports
- Suggestions and feedback
- New techniques, products and procedures
- Preventive/Corrective Actions
- Risk Assessment
- Results from effectiveness measurements
- Previous management review actions
- Changes affecting the ISMS
- Recommendations for improvement

**OUTPUTS**
- ISMS improvements
- Updated risk assessment
- Modified controls/procedures
- Resource requirements
- Effectiveness measurement improvements

And what about the future?
Effectiveness - Metrics

- 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
ACT

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

There are numerous requirements concerning metrics and incident handing.

4.2.3 Monitor and review the ISMS

The organization shall do the following.

a) Execute monitoring and review procedures and other controls to:
   1) promptly detect errors in the results of processing;
   2) promptly identify attempted and successful security breaches and incidents;
   3) enable management to determine whether the security activities delegated to people or implemented by information technology are performing as expected;
   4) help detect security events and thereby prevent security incidents by the use of indicators; and
   5) determine whether the actions taken to resolve a breach of security were effective.

b) Undertake regular reviews of the effectiveness of the ISMS (including meeting ISMS policy and objectives, and review of security controls) taking into account results of security audits, incidents, effectiveness measurements, suggestions and feedback from all interested parties.

c) Measure the effectiveness of controls to verify that security requirements have been met.
Metrics

- Need to assess effectiveness of ISMS
- Guidance will be in ISO/IEC 27004 – still under development

Interpreting the Results

- Perfect
- On target
- Below target, but close
- Way below target

1 - %CFES = \( \frac{TCFES}{TC} \times 100 \)
where TCFES = \( \Sigma \) co-workers who have received training in security, and TC = Total no. of co-workers

F – PFS = \( \frac{IPF}{TIS} \times 100 \)
where IPF = \( \Sigma \) Security incidents caused by lack of training, and TIS = Total no. of security incidents

1 - %SPSM = \( \frac{TSP}{TSA} \times 100 \)
where TSP = \( \Sigma \) Information systems protected from malware, and TSA = Total number of systems threatened by malicious software

Detect event in sufficient time to prevent or mitigate impact
ISO/IEC 17799
Code of Practice for Information Security Management
ISO/IEC 17799

- Security Policy
- Organising Security
- Asset Management
- Human Resources
- Physical and Environmental Security
- Communications and Operational Management
- Access Control
- Information Systems Acquisition, Development and Maintenance
- Information Security Incident Management
- Business Continuity Management
- Compliance

• Roles and responsibilities
• Screening
• Terms and conditions of employment
• Prior to employment
• During employment
• Termination or change of employment
Certification
Certification

Guidelines for Certifying and Registering ISMS

Mutual Recognition Procedures

Accredits Certification Bodies

Assesses ISMS, awards certificates in conformance with ISO/IEC 27001:2005

ISMS

ISO/IEC 27001:2005

Accreditation Body

Accreditation Body

Accreditation Body

EA7/03
Certification Audit

- Compliance with standard
- No material deficiencies in design
- No material deficiencies in operation
- NOT effectiveness or efficiency
COSO Audit

- Opine on Management’s view that controls OK
- Design OK
- Operations OK
- Deficiency = Nonconformity
- Evidence > certification audit
International Take-up

ISMS Registrations by Continent

Growth of ISMS Registrations World Wide

- Rest of the world
- Europe
- Asia
- Europe

January 2006
Benefits
Benefits

■ Reduction in insurance premium paid for project
■ New customers
■ Avoided customer penetration testing
■ Security become a team effort, including managers, everyone more aware
■ Documentation corresponds to reality
■ Corporate internal audit very happy
■ Management is in charge
Transition to ISO/IEC 27001
UKAS Transition Statement

- Up until 23 July 2006 audits 7799 or 27001
- After 27001 only
- Non-conformities against 27001 must be cleared by 23 July 2007
- Accredited BS 7799-2 certificates will be invalid after 23 July 2007
Conversion 7799 to 27001

- Many minor changes
  - prompt detection of errors, events and impacts ...

- SOA changes
  - Shuffle of controls
  - Small number additions/deletions

- Gamma’s CB (BSI) wanted to see the conversion plan

- Main changes
  - Introduced measurement

Agreed Action

Editorial Changes

Search for BS 7799 throughout web and versions:
- replace "ISO 15408 and BS 7799" Business Objectives. Also in 04 W change folder names (and DCR tit: ISO9001 Compliance" to "ISO9000"
- change navigation bar "Standards" replace "BS 7799 Control" in the 2 version 5.0
- remove SOA 2002 from the Site I change the file name "bs7799 (<< change the file name "ISO9001 Co"
- replace BS 7799-2:2002 with ISO 17799:2005 where appropriate)

1. Standards (AN), (SN)
2. Scope (AN), (SN)
3. Business Risks (AN), (SN)
4. Check (AN), (SN)
5. Records (AN), (SN)
RELATION WITH OTHER STANDARDS, LAWS and REGULATIONS
Corporate governance & internal control

- ... 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

![Diagram]

- Mission
- Business Objectives
- Business Risks
- Applicable Risks
- Internal Controls
- Review

act

©Gamma Secure Systems Limited, Wm List & Co., 2006
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.
SOX implementation

- SEC - Securities and Exchange Commission
- PCAOB - Public Company Accounting Oversight Board
- COSO - Committee of the Sponsoring Organisations of the Treadway Commission
- ISACA - Information Systems Audit and Control Association
- CobiT - Control objectives for Information and related technologies
- ITGI - IT Governance Institute
COSO ERM

Internal Control - Integrated Framework

Entity objectives can be viewed in the context of four categories:

- Strategic
- Operations
- Reporting
- Compliance

Slide created by the Institute of Internal Auditors

©Gamma Secure Systems Limited, Wm List & Co., 2006
ERM considers activities at all levels of the organization:

- Enterprise-level
- Division or
- subsidiary
- Business unit processes
COSO ERM

The eight components of the framework are interrelated …
Basel II

- Extends credit/market risk provisions of Basel 1 to operational risk
  - The risk of direct or indirect loss resulting from inadequate or failed internal processes, people and systems, or from external events

- Encourages establishment of effective internal control to release Tier 1 capital

- Can you demonstrate effective control to satisfaction of the regulators?

- You will need to be able to measure effectiveness
Internal Control

A WORD OF WARNING

In US Only financial reporting

In UK Everything

In INDIA Rule 49 Financial reporting + risk management

Definitions differ around the world!
Information Security

- ISO/IEC 15408 “Common Criteria” – IT security product evaluation
- Various technical standards: encryption, intrusion detection, biometrics, smart cards, etc.
- Laws and regulations: company acts, data protection acts, laws concerning cryptography and digital signatures, Sarbanes-Oxley, Basel, various cyber laws...

Does the product possess vulnerabilities that an attacker can exploit to harm the information the product is intended to protect?
Relationship

- ISO/IEC 27001 is a management standard

- It is the glue, whereby management can:
  - ensure compliance with laws and regulations
  - marshal the benefits of technical standards
METHODOLOGY

The Advanced Web-based Internal Control Management System Methodology (AWICMSM)
Methodology

- ISMS is just part of Internal Control
- Measuring effectiveness – the TIME theory
- Events and Impacts – tell it like a story
- The SOA is just an “AIL” – alternative ideas list
- Integrated Management Systems
The “TIME” Theory
Event-Impact Relationship

■ There is a fundamental principle of internal control (and thus ISMS):

“… 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, \( C_{BA} \)

\[ \begin{align*}
\text{Money (£)} & \quad \text{Time} & \quad T_E & \quad T_W & \quad T_M & \quad T_F \\
F & & & & & P
\end{align*} \]
Fundamental Model (in time)

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

Time

Money (£)

$T_E$, $T_D$, $T_F$, $T_W$
Types of Control

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

■ 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

■ Reactive
  - Identify that the impact has occurred and invoke appropriate actions to recover (or mitigate) the situation
## 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>
Measurement
ISMS Requirement

There are numerous requirements concerning metrics and incident handing.

4.2.3 Monitor and review the ISMS

The organization shall do the following.

a) Execute monitoring and review procedures and other controls to:

   1) promptly detect errors in the results of processing;
   2) promptly identify attempted and successful security breaches and incidents;
   3) enable management to determine whether the security activities delegated to people or implemented by information technology are performing as expected;
   4) help detect security events and thereby prevent security incidents by the use of indicators; and
   5) determine whether the actions taken to resolve a breach of security were effective.

b) Undertake regular reviews of the effectiveness of the ISMS (including meeting ISMS policy and objectives, and review of security controls) taking into account results of security audits, incidents, effectiveness measurements, suggestions and feedback from all interested parties.

c) Measure the effectiveness of controls to verify that security requirements have been met.
We Can Measure Things...

1. \[1 - \%CFES = \left(\frac{TCFES}{TC}\right) \times 100\]
   where \(TCFES = \sum\) co-workers who have received training in security, and \(TC = \) Total no. of co-workers

2. \[F - PFS = \left(\frac{IPF}{TIS}\right) \times 100\]
   where \(IPF = \sum\) Security incidents caused by lack of training, and \(TIS = \) Total no. of security incidents

3. \[1 - \%SPSM = \left(\frac{TSP}{TSA}\right) \times 100\]
   where \(TSP = \sum\) Information systems protected from malware, and \(TSA = \) Total number of systems threatened by malicious software

Extracts from New ISO Work Item on ISMS metrics
Interpreting the Results

- Perfect
- On target
- Below target, but close
- Way below target
What Have We Measured?

- Performance
- Whether on track for a given target
- Identifying areas for improvement
- All of these are valid, but are they really a measure of ISMS effectiveness?
- How do I know the ISMS is working?
This is How ...

Good design should ensure that ISMS detects all events in sufficient time...

If not there will be an incident

May need to take action

---

Statement of Applicability (SOA) •
Operate Controls •
Awareness Training •
Manage Resources •
Plan & Rehabilitation Response to Incidents •

PLAN

ACT

DO

CHECK

Need other checks as well

---

©Gamma Secure Systems Limited, Wm List & Co., 2006
Incidents?

- Safe found unlocked ✓ possible unauthorised disclosure
- Blue death ❌ usually no impact
- Hard disc crash ❌ ditto
- Adware virus ✓ possible unauthorised disclosure
- Fox hunting protestors ✓ adverse press coverage
Definition of an Incident

“… an occurrence of an impact… “

NOT the occurrence of a threat or vulnerability
A Practical Proposition (1)

**ISMS METRICS AND INCIDENT HANDLING**

- Deal with incidents and metrics together
- There is a page that does this ("ISMS Metrics and Incident Handling")
- Uses definition *incident = occurrence of impact*
- Metric is just the time metric
- Can add others if needed
- There is a template incident handling procedure
A Practical Proposition (2)

- Fill in an impact record and log it to record:
  - The event, together with a reference to the RTP
  - The impact
  - The values of $T_E$, $T_D/T_M$, $T_F$ and $T_W$ (see ISMS Metrics and incident Handling section of skeleton)
  - The value of $I_P$ (and if possible the cost of the existing controls)

- Monitor these records at:
  - Management meetings
  - ISMS audit visits

<table>
<thead>
<tr>
<th>Date</th>
<th>Event</th>
<th>RTP</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table: Impact Log

- Impact ID Description
- Fixed

Here is the blank record
UK Bank

Use of time theory for Basel II

©Gamma Secure Systems Limited, Wm List & Co., 2006
Tell it Like a Story
So What Makes 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

- Can be tiered
Approach

- Performed by risk owners – the Board
- Tell it like a story
- Business events and impacts
- Public methodology
  - Good plot
  - Happy ending

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 malicious 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 or all of our business**, see E5.1, E5.2, E5.3, E5.4
- Possible unwanted **disclosure of sensitive information** (e.g. Groups F, K), see E5.2
- Possible **court action against our company for breach of the Data Protection Ac**

The threat is the **hacker**.

**Risk E5.1** A hacker could bring about our inability to carry out some or all of our business, see E5.1, E5.2. The first line of defence against such an attack is the firewall. The ISP provides the user of whether this firewall is always correctly configured, or if it is under attack. Not acceptable risk because there is a second line of defence, which lies in hardening the

"Hotfix and service pack upgrades.” However:
Events and Impacts

Expressed in business terms, they are what worry people.

The event: an aircraft engine fails on take-off.

Impacts:

- Potential loss of life
- Dissatisfied customers
- Increased costs
Typical IS Events and Impacts

- Theft
- Acts of God, vandals and terrorists
- Fraud
- IT failure
- Hacking
- Denial of service
- Disclosure
- Breach of the law

- Adverse press coverage
- Organisation ceases trading
- Inability to carry out all or some of its business
- Loss of customer confidence
- Loss of revenue
- Increased costs
- Prosecution
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, E, 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.
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.
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.

Risk S x  All the other issues
Alternative Ideas Lists
The AIL Concept

- Policy/RTPs should have identified all controls, but has anything been overlooked?
- What do other people do?
- What do they do that applies to us?
- If it applies do we do it?
- This is just what the SOA is
- SOA = “Alternative Ideas” List (AIL)
- It is a “safety net”
Multiple AILs

In reality there are multiple AILs

ISO/IEC 17799:2005 is just one such list, but there are many others, corresponding to:

- CobiT
- COSO/ITGI
- Quality assurance (ISO 9001)
- Environmental protection
- Financial accounting
- Different lists for different legal jurisdictions
- Etc.
Extract of ITGI Guidance

Mapping of CobiT to PCAOB IT general controls

<table>
<thead>
<tr>
<th>CobiT Control Objective Heading</th>
<th>PCAOB IT General Control Heading</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Acquire or develop application software.</td>
<td>Program Development</td>
</tr>
<tr>
<td>2. Acquire technology infrastructure.</td>
<td>Program Changes</td>
</tr>
<tr>
<td>3. Develop and maintain policies and procedures.</td>
<td>Computer Operations</td>
</tr>
<tr>
<td>4. Install and test application software and technology infrastructure.</td>
<td>Access to Programs and Data</td>
</tr>
<tr>
<td>5. Manage changes.</td>
<td></td>
</tr>
<tr>
<td>6. Define and manage service levels.</td>
<td></td>
</tr>
<tr>
<td>7. Manage third-party services.</td>
<td></td>
</tr>
<tr>
<td>8. Ensure systems security.</td>
<td></td>
</tr>
<tr>
<td>9. Manage the configuration.</td>
<td></td>
</tr>
<tr>
<td>10. Manage problems and incidents.</td>
<td></td>
</tr>
<tr>
<td>11. Manage data.</td>
<td></td>
</tr>
<tr>
<td>12. Manage operations.</td>
<td></td>
</tr>
</tbody>
</table>
### IT Strategic Planning

<table>
<thead>
<tr>
<th>Question</th>
<th>Yes</th>
<th>No</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Has management prepared strategic plans for IT that align business objectives?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Figure 23—Application Control Objectives for the Sales Cycle</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Illustrative Control Objectives</td>
<td>Financial Statement Assertions</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Orders are processed only within approved customer credit limits.</td>
<td>Valuation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Orders are approved by management as to prices and terms of sale.</td>
<td>Validity</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Orders and cancellations of orders are input accurately.</td>
<td>Valuation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Order entry data are transferred completely and accurately to the shipping and invoicing activities.</td>
<td>Valuation</td>
<td>Completeness</td>
<td></td>
</tr>
<tr>
<td>All orders received from customers are input and processed.</td>
<td>Completeness</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Only valid orders are input and processed.</td>
<td>Validity</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Invoices are generated using authorized terms and prices.</td>
<td>Valuation</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
ISO 9001:2000 AIL

Applicable/non-applicable requirements under 6 major headings (Section 7 of ISO 9001)

- Planning of Product Realisation
- Customer Related Processes
- Design and Development
- Purchasing
- Product and Service Provision
- Control of Monitoring and Measuring Devices
Integrated Management Systems
Overall Model

Superposition of UK Audit Practices Board model and ISO/IEC 27001

PLAN

- Mission
- Business Objectives
- Policy
- Business Risks
  - Applicable/non-applicable risks
  - Risk Treatment Plans
  - AILs
  - SOAs
  - Safety net

ACT

- Act
  - Corrective action
  - Preventive action
  - Improvements

DO

- Control Processes
- Operational Processes
  - Manage resources
  - Training, competence, awareness
  - Prompt reaction to incidents

CHECK

- Review
  - Internal audit
  - Management review
  - Routine checks, etc.
Integrated Management Systems

- One MS, one audit, many standards
- BSI call it the shape of the future
- Gamma has one

BSI call it the shape of the future

Gamma has one

BS 7799-2

And ISO 9001

And ...

©Gamma Secure Systems Limited, Wm List & Co., 2006
Taking it from the Top

**Mission**

**Business objectives**

**Business risks**

<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*), ... doing work and not making a profit.</td>
<td></td>
</tr>
<tr>
<td>Trading risk</td>
<td>... changes in trading positions when prices move adversely. ... our money and other assets not being worth as much as they ought.</td>
<td></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. ... being unable to sell what the market wants.</td>
<td></td>
</tr>
<tr>
<td>Existence risk</td>
<td>... the fact that we exist. ... spending money unnecessarily.</td>
<td></td>
</tr>
</tbody>
</table>

**RTPs**

*Risks Concerning Non-Applicable Risks*

It is possible that a non-applicable risk becomes an applicable risk.

All assets could be affected, but primarily Assets Groups 2, 3...

**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 range from 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 authority or in error. All IT based assets could be affected (Groups 2, 3, 4, ...)

The implications of such events are:

- Possible inability to carry out some or all of Gamma's business, see Sec. 4.4.
- Sec. 4.4.2, 4.4.3, 4.4.5, 4.4.6
- Possible unauthorized disclosure of Gamma classified data, see Sec. 4.4.2, 4.4.3, 4.4.5, 4.4.6
- Possible loss of data, see Sec. 4.4.2, 4.4.3, 4.4.5, 4.4.6

The principal threats are backup failure, errors, utility failure, software failure and...
There are two parts to internal control:
Processes/procedures for
- “doing the work” (Part 1)
- “ensuring the work is done properly” (Part 2)

Part 2 are the controls (Events, Impacts and RTPs)

What about Part 1?
Opportunities and Benefits

- The converse of events and impacts
- Have Opportunity Exploitation Plans (OEPs) rather than RTPs
- Similar “time” theory

Anticipated benefits:
- Possible favourable customer perceptions, see A1.1a, A1.1b, A1.1c, A1.1d, A1.1e
- Illicitator (delete R1, M)

Reaping the benefit

Loosing the opportunity
Enhanced PDCA Framework
Summary

■ Unified methodology

■ ISMS is part of internal control ...

■ ... but is also the engine that drives it

■ Time theory: RTPs and OEPs

■ AIL safety net

■ Facilitates creation of an integrated management system
COMMERCIAL APPLICATION
Overview of an Approach

- Classroom/on-the-job training, throughout at least one PDCA cycle
- Role Model
- To-Do-List concept
- Skeleton ISMS
- Event-impact RTPs
- Integrate with existing internal control structures
- Marshal existing procedures/records

AV/OMSM projects are conducted as a series of phases with intervening gaps. 4-6 months
Role Model
Role Model

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

Acts to reduce risk to acceptable level

Provide feedback/ request policy enhancements

Policies

Set organisation-wide policy

Direct

Owns/looks after

Advise

Advise

Advise

Audit

Certify

Instruct and monitor

Acts to reduce risk to acceptable level

Owning

Provides management information

Direct

Advise

Advise

Train

Use

Information

ISMS Advisors

ISMS Administrator

ISMS Trainer

Information users

ISMS

Certification Auditors

Internal ISMS Auditors

Policy Makers

ISF

ISMS Advisors (optional)

Policy Makers

©Gamma Secure Systems Limited, Wm List & Co., 2006
The To-Do-List Concept
The “To-Do-List” Concept

- Management standards, including ISO/IEC 27001 insist that the 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” Concept

Management standards, including ISO/IEC 27001 insist that the management processes must be in place.

## 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>MSR Actions 19.11/ 19.13</td>
<td>Add G4 and G5 RTPs, in anticipation of adding S&amp;M AIL. See CRF.</td>
<td>051031</td>
<td>051031</td>
</tr>
<tr>
<td>MSR Action 19.3</td>
<td>Produce new Holiday Practice.</td>
<td>051130</td>
<td></td>
</tr>
<tr>
<td>MSR Action 19.17</td>
<td>Add new risk (ORP11) concerning under resourcing.</td>
<td>051130</td>
<td>As at 051101: 1. Presented for review</td>
</tr>
<tr>
<td>Extend MS to cover OEPs</td>
<td>Create and add the Sales and Marketing Practice; and add the Sales and Marketing reviews to the MS records.</td>
<td>051130</td>
<td>As at 051103:</td>
</tr>
</tbody>
</table>

©Gamma Secure Systems Limited, Wm List & Co., 2006
Non Conformities

A non-conformity "is the absence of, or failure to implement and maintain, one or more required management system elements, or a situation which would, on the basis of objective evidence raise significant doubt as to the capability of the ISMS to achieve the security policy and objectives of the organisation."

This definition comes from EA7/03
Which Means...

is the absence of, or failure to implement and maintain, one or more required management system elements

**Missing/failed ISMS infrastructure component**

or a situation which would, on the basis of objective evidence raise significant doubt as to the capability of the ISMS to achieve the security policy and objectives of the organisation

**Missing/failed Applicable controls leading to significant doubt ...**
Which means …

Management standards, including ISO/IEC 27001, insist that the 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”
- Can have entries in progress
- Entries will be corrective, preventive or improving in nature
- There should be evidence that any risk is being managed

<table>
<thead>
<tr>
<th>Reference</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSR Actions 19.11/19.13</td>
<td>Add G4 and G5. See CRF.</td>
</tr>
<tr>
<td>MSR Action 19.3</td>
<td>Produce new HMS.</td>
</tr>
<tr>
<td>New ISMS Standard</td>
<td>ISO/IEC 27001. Make the necessary changes.</td>
</tr>
<tr>
<td>MSR Action 19.17</td>
<td>Add new risk (051010).</td>
</tr>
<tr>
<td>Extend MS to cover OEPs</td>
<td>Create and add the Sales and Marketing Practice; and add the Sales and Marketing reviews to the MS records.</td>
</tr>
</tbody>
</table>

1. Presented for review

051130 | As at 051103:
Skeleton ISMS
Skeleton ISMS

INTRODUCTION

Objective

This document is <<COMPANY>>’s “Information Security Management System” (ISMS) to empower <<COMPANY>> to manage its information assets.

<<Note: if this document does not contain the internal audit results, please check the latest version.>>

Contents

This document defines the scope of the ISMS and contains the ISMS Audit, Risk Assessment and Risk Treatment Plan and presents the ISMS Audit Report and Checklist. The ISMS Audit Report and Checklist are based on ISO/IEC 27001:2005. The ISMS Audit Report and Checklist are based on Version 2.0 of this document. It details the processes and procedures for training and auditing of the ISMS Audit, Management Review and ISMS improvement processes.
Skeleton ISMS

- Built-in facility for document control
- Space to define scope and context
- Prototype policy
- Provision for RTPs
- Virtually AILs (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
- Records
- Compliance index
Skeleton ISMS

■ There is space to define the ISMS scope, just as it will appear on the 27001 certificate

■ And to define the ISMS context
Skeleton ISMS

■ There is a prototype ISMS policy

■ Most words are there to ensure compliance with the standards

■ Some to simplify production of the SOA

■ Customise with reference to relevant corporate policies

---

ISMS POLICY

RISK MANAGEMENT

Information Security Controls shall be selected on the basis of a risk assessment, which shall be carried out at regular intervals. The effectiveness of these controls shall be monitored and adjusted as necessary to reduce the business risk to an acceptable level and ensure that security continues to fulfill <<COMPANY>> requirements. Management shall adjust the overall set of Security Controls by relaxing the individual controls, strengthening them or exchanging them with more effective controls, or adding/deleting controls as appropriate.

ASSETS

Assets, including information, business systems and applications, shall have identified Business Owners who are responsible for determining the level of acceptable risk and implementing the ISMS Policy and associated Security Controls. Assets shall be protected according to the business impacts that might result if their confidentiality, integrity or availability were to be compromised.

---

PERSONNEL POLICIES

All staff (including directors) should be trustworthy and be responsible for implementing the ISMS Policy and Security Controls within their business areas. Unauthorised disclosure, destruction, theft or damage of/to any asset in contravention of the Security Controls by any employee shall be regarded as cause for appropriate disciplinary action.

©Gamma Secure Systems Limited, Wm List & Co., 2006
Skeleton ISMS

- Provision to develop RTPs
- The standard eight plus any others

RISK ASSESSMENT AND RISK TREATMENT APPROACH

The risk assessment is performed manually.

- Identifies a variety of events (or sources). Each event describes how a threat might violate the security of the identified assets to cause some impact. (Click here to see <<COMPANY>>’s assessment of the severity of these impacts.) The analysis thus takes account of the vulnerabilities that a threat agent may exploit, in the context of existing controls, in order to compromise an asset.

- For each impact, within the context of that event, the risks are assessed and a risk treatment plan is developed to reduce the risk to an acceptable level.

- Each event is then considered in turn, identifying:
  - The assets that may be affected

RISKS CONCERNING xxxxxx

<<DESCRIBE THE EVENT AND SO DOING REFER TO THE ASSETS. They are listed here with the correct links (to footnotes), so just delete. Of course, this list needs to be amended if the asset table is changed. If you delete an asset there is no need to change the labelled. Beware of the bookmarks if you do>>


<<Note all the impacts listed in the adverse impact summary are listed here. Delete those that do not apply. At the end of each line (where it says “see”) put a reference to the risk, e.g. see D1.3, or S4.3a). Delete the Possible/Probable as appropriate.

Impact

- Adverse press coverage
- Company goes to the wall/Quire
- Court action against << COMPANY >>
- Court action against an employer
- Failure to prosecute
- Inability to carry out some or business
- Loss of all forms of data and information
- Loss of customer confidence

RTP TEMPLATE

©Gamma Secure Systems Limited, Wm List & Co., 2006
Skeleton ISMS

- SOA with hyperlinks to the standard eight events and policy statements
- Skeleton included links to common policies and procedures

The following color coding is used:

- This Security Control is not applicable for the reasons given
- This Security Control is applicable and is a << COMPANY >> policy requirement.
- The specified Security Control is in place.
- The specified Security Control is in the process of being designed.

PHYSICAL AND ENVIRONMENTAL SECURITY

Secure Areas

The objective of these controls is to prevent unauthorised physical access, damage and interference to the organisation’s premises and information.

<table>
<thead>
<tr>
<th>Annex A Control</th>
<th>Applicability</th>
</tr>
</thead>
</table>
| A.4.1.1 Physical security perimeter | 9.1.2 Security and key control (daily) 
| A.4.1.2 Physical entry controls | 9.1.2 Security and key control (daily) 
| A.4.1.3 Securing offices, rooms and facilities | See 9.1.2 Security and key control (daily) 
| A.4.1.4 Protecting against external and environmental threats | See the risk treatment plan for this event |
Skeleton ISMS

- There is a facility for recording training and awareness activities for all staff
- Just amend/reference what you do

TRAINING AND AWARENESS

It is an ISMS Policy requirement that << COMPANY >> also ensures that all relevant personnel are aware of their information security activities and how they contribute to the implementation and maintenance of the Information Security Management System (ISMS). WHERE THESE ARE DOCUMENTED >>:

- Determining the necessary competencies for personnel;
- Providing competent training and, if necessary, education;
- Evaluating the effectiveness of the training provided;
- Maintaining records of education, training, skills, and competencies.

<< COMPANY >> also ensures that all relevant personnel are aware of their information security activities and how they contribute to the implementation and maintenance of the Information Security Management System (ISMS). WHERE THESE ARE DOCUMENTED >>:

- AM: Joe corrupted the hard disc
- Told to recover by evening
- Started to retype in all the software programmes
- PM: (In tears) admitted he had failed
- Asked what he had done previous evening
- Answered “I took a backup”
- Joe learnt the hard way of the value of backups
- The real value is, of course, in their restoration
- Take regular backups
Skeleton ISMS

Page on Metrics/Incident Handling

Uses time theory

Incident is occurrence of impact

ISMS METRICS AND INCIDENT HANDLING

INTRODUCTION

This page identifies and explains the metrics that we use to determine the effectiveness of our ISMS, and how we handle incidents.

We start by explaining the fundamental time theory and how it is used in developing the RTPs. We conclude that an incident is the occurrence of an impact and give instructions for dealing with incidents.

TIME THEORY

Fundamental Principle

The fundamental time metric/principle:

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

is illustrated in Figures 1(a) and 1(b).

Impact Log

List impact occurrence in reverse chronological order.

<table>
<thead>
<tr>
<th>Impact ID</th>
<th>Description</th>
<th>Fixed</th>
</tr>
</thead>
</table>

Date | Event | RTP | Impact |
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>T_e</td>
<td>T_d</td>
<td>T_m</td>
<td>T_r</td>
</tr>
</tbody>
</table>

Commentary

Agreed action | Date executed

Use qualitative measures for time and cost metrics if quantitative measures are not available or would be misleading due to imprecision.
Skeleton ISMS

- An internal ISMS audit schedule
- Procedure, proforma report and checklist (ensures compliance when completed)
Other audits

- Extant internal audit activities
  - COSO, CobiT etc

- Technical audits: Penetration tests, Vulnerability assessments etc

- Customer audits

- External audit
Skeleton ISMS

- Initial management review schedule
- Procedure and checklist (for the meeting secretary, which also ensures compliance when completed)

**MANAGEMENT REVIEW**

**Schedule**

ISF Management Review Meetings are planned to take place every <<3 months/6 months/year appropriate>>, in accordance with the following schedule:

|------|----------|----------|----------|----------|----------|

**ISMS MANAGEMENT REVIEW CHECKLIST**

**Department:**

**Completed by:**

**Meeting date:**

**Review Inputs**

The following review inputs have been made available to the meeting:

- Internal ISMS Audit reports and any other security audit reports

©Gamma Secure Systems Limited, Wm List & Co., 2006
Skeleton ISMS

- Procedure for dealing with preventive, corrective actions and improvements
- To-Do-List
- Record and document control section for all ISMS records

TO DO LIST

The table below lists those actions identified in the risk assessment that need to be converted unacceptable risks into acceptable risks. Significant actions arising from ISMS Audits should also be included here. Add new entries to the top of the list change control.

<table>
<thead>
<tr>
<th>Reference</th>
<th>Action</th>
<th>Target Date</th>
<th>Completion Date</th>
</tr>
</thead>
</table>

RECORDS AND DOCUMENT CON

CONTROL OF ISMS RECORDS

ISMS records comprise:

- The Internal ISMS Audit Reports, completed checklists and the audit report
- The minutes and completed checklists of the Management Review meeting
- The incident log (GIVE REFERENCE)
- LIST ALL OTHER RECORDS OF ACTIONS/EVENTS THAT CONSTITUTE EFFECTIVENESS OR PERFORMANCE OF THE ISMS, e.g. completed checklists

Their purpose is to assist management in ensuring the effectiveness of the controls needed for the identification, storage, protection, retrieval, and documentation of ISM records. These controls take a particular role in avoiding fraudulent modification and ensure that remain effective. Their purpose is to assist management in ensuring the effectiveness of the controls needed for the identification, storage, protection, retrieval, and documentation of ISM records. These controls take a particular role in avoiding fraudulent modification and ensure that remain effective.
Conformance with Standard

INDEX

ISO/IEC 27001:2005 Requirement

4 Information security management system

4.1 General requirements

4.2 Establishing and managing the ISMS

4.2.1 Establish the ISMS

a) Define the scope of the ISMS

b) Define an ISMS policy

1) framework

2) business, legal, regulatory and contractual requirements

3) strategic organizational and risk management

4) risk evaluation criteria

5) management approval

6) Define the risk assessment approach of the organisation

Cross-reference

Introduction
Scope
ISMS Policy
ISMS Policy
ISMS Policy
ISMS Policy
ISMS Policy
Risk Assessment
Summary
What Makes the Approach Fast

- Classroom/on-the-job training, throughout at least one PDCA cycle
- Role Model
- To-Do-List concept
- Skeleton ISMS
- Event-impact RTPs
- Integrate with existing internal control structures
- Marshal existing procedures/records

- Addresses all the issues:
  - Scope, Policy, Risk Assessment/Treatment, SOA, Gap Analysis, ...

- Skeleton means that everything that needs to be done only once is done only once

- Facilitates a well organised project

- Instils confidence to succeed in participants

- Creates information security awareness
CASE STUDY
The Civil Service of Mauritius

- Small island off the southeast coast of Africa in the Indian Ocean
- 2,000 km from Durban, 6000 km from Perth, 9700 km from London
- Area: 1865 km²
- Population: 1.2 m
- Multi-cultural society (66% Indian, 31% African & European, 3% Chinese)
- Free & compulsory education
- Bilingual (English, French)
- 90% literacy rate
- Free health services
- Sub Tropical Climate (19°C - 29°C)

Source: Ministry of IT & Telecommunications, Mauritius
The Mission

■ Develop ICT as the 5th Pillar of the Economy

■ Critical success factors include information security, as well as leadership, legislation, infrastructure, e-culture, marketing, etc.

■ Drivers:

➢ Security seen to be an IT issue
➢ Lack of information security awareness
➢ Greater emphasis on technical controls rather than management controls
➢ Risk management fairly new to many organizations

Source: Ministry of IT & Telecommunications, Mauritius
The Information Security Journey

- Establish Steering Committee and plans (2001)
- Government approval of plans (2002)
- Invite tenders for consultancy (2002)
- Consultancy project to train staff and take four “pilots” through to certification (2003)
- Rollout to all other Ministries and Departments (2004-6)
# Project Timescales

**Start of Training**  \[ 4 \text{ months} \]

<table>
<thead>
<tr>
<th>Month</th>
<th>Oct</th>
<th>Nov</th>
<th>Dec</th>
<th>Jan</th>
<th>Feb</th>
<th>Mar</th>
<th>Apr</th>
<th>May</th>
</tr>
</thead>
<tbody>
<tr>
<td>Project week</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>11 week gap</td>
</tr>
</tbody>
</table>

- Phase 1 (Planning/promotion)
- Phase 2 (Training/project initiation)
- Phase 3 (Project finalisation)
- Phase 4 (Publicity)
- Certifications completed
- Formal end of project

**ISMSs Certified**
Approach

- ISMS built by people who will own it
- Training to ALL involved with the ISMS
- Use of Skeleton ISMS to ‘fast track’ creation of actual ISMS manual

- Stylised approach to creating RTPs, based on events and impacts
- To-Do-List to manage implementation of improvements and additional security requirements
Pilot Implementation Framework

■ Steering Committee

■ Pilot Site Information Security Forum
  ➢ **Ministry of Social Security** *(Contributions, Benefits, ...)*
  ➢ **Passport & Immigration Office** *(passport, residence permit, visa, border control, ...)*
  ➢ **Civil Status Office** *(Birth, Death, Marriage registration, ...)*
  ➢ **Treasury Department** *(Govt. Accounting System, Budget monitoring, pensions, ...)*
  ➢ Head or Deputy as Project Leader
  ➢ Team *(Head and/or Deputy, Senior Officers)*

■ ISMS Advisors/Consultants

■ Internal ISMS Auditors
Training Programme

Coverage

- BS 7799-2 and Methodology
- Risk Treatment Plans
- ISMS Skeleton
- Internal ISMS Auditing
- Computer Assisted Audit Techniques

Audience

- Pilot ISMS Development Teams
- Management
- ISMS Advisors
- Internal ISMS Auditors

On-the-Job Training
Skeleton ISMS Manual

INTRODUCTION

Purpose

This document is <<State name of Department (note you System (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 SOA 2:2002. The SOA refers to other relevant processes and requirements.

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 BS 7799-2:2002
Risk Treatment Plans

Departments chose “departmental specific” events and worked on those first

- D1 -
- D2 -
- D3 -
- D4 -

- S1 - Theft
- S2 - Acts of God, vandals and terrorists
- S3 - Regular fraud
- S4 - IT failure
- S5 - Hacking
- S6 - Denial of service attacks
- S7 - Disclosure
- S8 - Breach of the Law

Adverse press coverage
Court action against the Department
Court action against an officer of the Department
Failure to prosecute
Inability to carry out some or all of the Department’s business
Loss of all forms of data and information
Loss of citizen confidence
Loss of revenue
Loss of the monetary value of
Method of Working

- Teams worked largely on their own with support from:
  - The new ISMS Advisors
  - The Consultants

- Starting with the “business” events worked well

- The traditional RTPs ran smoothly as Senior Management now knew what questions to ask
To-Do-Lists

- Each created a To-Do-List
- These did not prove a bar to certification
- Demonstrated information security management
- The ISMS owners made these decisions

Source: Ministry of IT & Telecommunications, Mauritius
Auditing and Certification

Internal Auditing

Mandatory

IT Security Unit/Dept Internal Auditors
Desktop Audit
Implementation Audit

External Auditing

Desirable

Mauritius Standards Bureau
“Certification”

©Gamma Secure Systems Limited, Wm List & Co., 2006
Feedback

**BEFORE**
- Resource Availability
- Expertise of ISMS Team
- Commitment of Senior Management
- Tight Schedule
- Lack of confidence

**AFTER**
- Security Awareness
- Higher Confidence
- Security Culture
- Empowerment
- Improved Security
- Enriching experience
- Feeling of Satisfaction

*Source: Ministry of IT & Telecommunications, Mauritius*
Observation

By involving very senior staff in developing the RTPs

- They own the information security problem
- They lead from the top
- They believe in its importance
- Their immediate staff know that
- It is a powerful way of creating awareness
Institutional Framework

PMO

Other ministries

Ministerial Security Officers Committee

PMO Security Division

IT Security Unit

Overarching ISMS RTPs for central policies (Registry, Personnel, Finance, ...)

Central Skeleton ISMS

Subordinate ISMSs (Ministries Depts)

Prioritisation of Sites

Certification

Marketing & Promotion

ISO/IEC 17799 as National Standards

Source: Ministry of IT & Telecommunications, Mauritius

©Gamma Secure Systems Limited, WmList & Co., 2006
Current Status

- Rollout to other Ministries and Departments proceeding to plan

- It is clear that the training worked

- To a large extent it was marshalling what the Departments already had, rather than inventing something new
SUMMARY
Summary

- ISO/IEC 27001, risk driven PDCA management system standard
- Methodology: time theory governing effectiveness, places ISMS at heart of internal control
- RTP method allows senior management to own the information security problem
- Extensible using AILs and OEPs to cover whole of internal control
- Practical implementation
- Skeleton ISMS
- Practical experience
- Methodology can be taught and applied easily by others
Further Information

The papers referred to in this presentation can be found at www.gammassl.co.uk/topics/ics/html.
Information Security Management
ISO/IEC 27001 and Internal Control

Dr. David Brewer
Mr. William List, CA, hon FBCS

©Gamma Secure Systems Limited, Wm List & Co., 2006