Implementing ISO/IEC 27001

Computer Security Week 30th November 2006

Dr. David Brewer
Gamma Secure Systems Limited
www.gammassl.co.uk

Agenda

- ISMS standards
- Implementation strategies
- Fast track
- Case Studies
- Summary

ISO/IEC 27001 is a management system standard

ISO/IEC 17799 (27002) is a catalogue of controls you might use

Other standards concern guidance, metrics, risk assessment and certification
The ISMS Standards

ISO/IEC 27001

Information Security Management Systems - Requirements

- 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

The Deming Cycle

PLAN

- ISMS Improvements
- Preventive Action
- Corrective Action

DO

- Management Review
- Internal ISMS Audit

CHECK
ISO/IEC 17799

- Security Policy
- Organising Security
- Asset Management
- Human Resources Security
- 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

Caveat

- Covers physical, environmental and personal security, compliance with the law etc, but ...

- ... IT component focuses on IT platforms

- There is very little on business applications

- Nevertheless scope of ISO/IEC 27001 is everything concerning information security, including the business applications

- If you want, use another AIL
Accredited Certification

- International mutual recognition
- Conformance means all required management processes and applicable controls are in place and working

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
International Take-up

ISMS Registrations by Continent

Implementation Strategies
Risk as a Function of Time

- Risk changes with time
- New/improved controls are used to mitigate the risk
- Residual risk must be within the risk appetite
  - Else you stop work while things are fixed
  - Or risk appetite must be increased

Residual risk must be within the risk appetite

Strategies

- Build a brand new system
  - Aim to comply with ISO/IEC 17799
  - Carry out the Risk Assessment/Treatment and determine the controls from that
- Go with what you have today
- Start-up - usually 2
**Strategy 1 – New (17799)**

- Develop brand new policies and procedures according to ISO/IEC 17799

**Upside**
- *Looks fantastic*

**Downside**
- *Can take a long time (1½ - 2 years)*
- *Control might be counter-cultural or over-the-top*
- *Too much documentation that nobody reads*
- *Risk assessment might be meaningless*
- *Scope for plenty of non-conformities*
- *Management system process often get forgotten*

---

**Strategy 2 – New (Tailored)**

- Develop brand new policies and procedures driven by actual needs

**Upside**
- *Custom made*

**Downside**
- *May still take a long time (6 - 18 months)*
- *Scope for non-conformities while new controls are bedded in*
- *Management system process may get forgotten*
**Strategy 3 – Now**

- Just document the controls as they are now

**Upside**
- Very quick (3 – 4 months)
- Focus is on the management system processes
- Use the management system to manage change

**Downside**
- Writing down what you do now can be soul destroying
- Must accept that weak controls represent an acceptable risk
- Some scope for non-conformities if actual practices are indefensible or corrective actions not in place

---

**Which is Best?**

- Strategy 1 is a hiding to nothing
- Strategy 2 and 3 are compatible, but why wait?
- Apply 3, the use it to create 2
ISO 9001 Experience

- Early implementations typically Strategy 1
  - Quality managers documented nice to have systems
  - Lots of non-conformities
  - Lots of retrospective activity prior to audits
- Now frowned upon by assessors
- Best advice “just document what you do”
- It’s then into the continuous improvement cycle

The Fast Track Approach
(see http://www.gammassl.co.uk/topics/ics/FTISMS.pdf for an open specification)

[Strategies 2 and 3]
Overview

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

Role Model
Role Model

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

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.
- 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 19.1.3</td>
<td>Add C4 and G3 see DFR</td>
</tr>
<tr>
<td>MSR Action 19.3</td>
<td>Produce new H</td>
</tr>
<tr>
<td>New ISMS Standard</td>
<td>ISO/IEC 27000 Make the sense</td>
</tr>
<tr>
<td>MSR Action 19.17</td>
<td>Add new risk (C)</td>
</tr>
<tr>
<td>Extend MS to cover DFRs</td>
<td>Create and add the Sales and Marketing Practice and add the Sales and Marketing variations to the MS records. 05/10 As at 05/10:</td>
</tr>
</tbody>
</table>
Which Means ...

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

- 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

Don’t like what you do now, think it a non-acceptable risk in the near future, or just want a look ‘n see - just put on the To-Do-List with an appropriate priority.

Overarching and Subordinate ISMSs
ISMS Policy

- Statements to cover the requirements of the standard
- The boss wants it done that way
- Policy requirements set by a higher authority (e.g. Group HQ), as a result of their risk assessment (perhaps)
- Local policy requirements (e.g. to link to HR policy/procedures, quality policy/procedures ...)
- Statements to reduce effort later (policy does not explain why, whereas risk assessment does), e.g. "good password practice shall be followed"

Overarching & Subordinate ISMSs

- Hierarchy of ISMSs
- Superior set policy for subordinate

Determine overall effectiveness

Top Level RTPs | High level policy statements | Overarching ISMS | Subordinate ISMS | Common Controls | Subordinate RTPs | Subordinate Specific Controls

©Gamma Secure Systems Limited, 2006
Event-driven Risk Treatment Plans

What is the risk?

- Proportionality → controls should be commensurate with the risk
- Decide which of the 133 controls in Annex A are applicable

Risk Treatment Plans

- Don't lose sight of why you are doing this

Choose the appropriate controls

Select the controls

Avoid the risk
Accept the risk
Transfer the risk
Mitigate the risk
Treat the risk

What shall we do?

Proportionality → controls should be commensurate with the risk
Decide which of the 133 controls in Annex A are applicable
Tell it Like a Story

- Predicated on “Time Model”
- Repeats the question “what if it doesn’t work”
- Expressed in business terms in language everyone can understand

Typical IS Events and Impacts

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

- 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

Covers all 133 controls
Example RTP (1)

- Acts of God for a library (early 1900s - no IT)
  - Threat agents: fire, flood, cyclone, vermin
  - Assets: building, staff, books
  - Impacts: inability to carry out some or all of the business of being a library

Example RTP (2)

- Can we prevent the event?
  - Fire? Possibly: state what we do, e.g. no smoking, lightning conductors, ..
  - Flood? Library on top of a hill, 2000 feet above sea level, no history of flooding: acceptable risk
  - Cyclone? No
  - Vermin? Not cost effective
Example RTP (3)

- Fire – suppose preventive measure does not work, can we detect it?
  - Yes - smoke detectors, but this is 1905 so perhaps rely on sense of smell
  - Can we put it out? We can try - buckets of sand to hand, plenty of people, spare buckets, a full well and staff well trained (volunteer fire people)
  - What if we fail? Evacuate (save the staff), write a news report

Example RTP (4)

- Cyclone – can we detect it?
  - Yes, very windy
  - What do we do? Close the shutters, take the most valuable books into the cellar and hide
  - What if the building collapses?
  - No problem, there is an escape route, well maintained used by smugglers of old

- Vermin – can we detect them?
  - Yes, regular inspection
Example RTP (5)

- What if all fail (including flood)?
  - Well we are not the only library on the island
  - There are copies of the most important books held in a mountain vault
  - There are libraries overseas
  - We are insured

- What if that fails? That is an acceptable risk

THE END OF THE STORY

Skeleton ISMS

Parts for you to complete

Version control

Covers every requirement of ISO/IEC 27001


**Skeleton ISMS**

- Built-in facility for document control
- Space to define scope and context
- Prototype policy
- Provision for RTPs
- Virtually complete SOA (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

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 (IS) is vital to the success of any organisation. It is therefore crucial that IS policies are clearly written to ensure that sensitive data is protected against loss, damage or exploitation. This policy sets out in a clear and concise way how the IS management is to be carried out. The policy covers the following areas:

- DEFINITIONS
- PURPOSE
- POLICY
- MANAGEMENT RESPONSIBILITY
- RESOURCES
- MEASURES
- AUDITING
- RECORDS
- DOCUMENTATION

The purpose of the IS policy for Gamma Secure Systems Limited is to manage and control the risk of information being lost, damaged or exploited.

PERSONNEL POLICIES

All personnel are expected to comply with this policy and are responsible for implementing the policy in their own work and in their workgroups. Any personnel who breach this policy are subject to immediate disciplinary action. Any personnel who breach this policy are subject to immediate disciplinary action.

Skeleton ISMS

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

RISK ASSESSMENT AND RISK TREATMENT
APPROACH

The risk assessment is performed manually.

For each risk assessed, the impact of the risk is determined. The risk is then assigned to a category of 'High', 'Medium', or 'Low'. The risk is then assigned to a category of 'High', 'Medium', or 'Low'.

Risks are then prioritised and can be assessed by the project team. The project team can then plan the risk mitigation actions.
Skeleton ISMS

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

There is a facility for recording training and awareness activities for all staff

Just amend/reference what you do
Skeleton ISMS

- Page on Metrics/Incident Handling
- Uses time theory
- Incident is occurrence of impact

**ISMS METRICS AND INCIDENT HANDLING**

**INTRODUCTION**

This page introduces and explains the concepts 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 ISMS. We explain that all incidents are the combination of external and internal factors. We also introduce the concept of the impact grid, which is used to analyze the potential impact of incidents.

**TIME THEORY**

Fundamental Principle

The fundamental time theory principles:

- Incident is an occurrence of impact
- Impact is a composite of external and internal factors

Visual representation: Impact grid

**Incident**

- Type
- Controls
- Impact

**Consistency**

- Data integrity
- Data accuracy

**Procedure**

- Audit
- Inspections
- Monitoring

**Compliance**

- Standards
- Regulations
- Compliance

**An internal ISMS audit schedule**

- Procedure, proforma report and checklist (ensures compliance when completed)

**INTERNAL ISMS AUDIT**

- Schedule
- Audit
- Inspection
- Monitoring
- Compliance

**Internal ISMS Audit Report and Checklist**

- Department
- Completed by

©Gamma Secure Systems Limited, 2006
Skeleton ISMS

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

**MANAGEMENT REVIEW**

**Schedule**

<table>
<thead>
<tr>
<th>Step</th>
<th>Date 1</th>
<th>Date 2</th>
<th>Date 3</th>
<th>Date 4</th>
<th>Date 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>2</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>3</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>4</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>5</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**ISMS Management Review Checklist**

- Department: 
- Completed by: 
- Meeting data: 
- Review Inputs: 
The following review inputs have been made available to the meeting:
  - Internal ISMS Audit reports and any other security audit reports

Skeleton ISMS

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

**TO DO LIST**

This table below lists those actions identified in the risk assessment that need to be documented in order to support the compliance with acceptable standards. Significant actions that are ISMS audits should also be included here. Add new actions to the top if not shown.

**RECORDS AND DOCUMENT CONTROL**

**CONTROL OF ISMS RECORDS**

ISMS records comprise:

- The Internal ISMS Audit Reports, completed checklists and theses
- The incident logs
- RECORDS AND DOCUMENTS OF ACTIONS THAT ARE EFFECTIVE OR EFFECTIVE OR PERFORMANCE OF THE ISMS, e.g. compliance

Their purpose is to assist management in ensuring the effectiveness of the system to meet objectives of the organization, particularly to ensure compliance and to ensure that remain in the control for the distribution, storage, protection, retrieval, and documentation. They are documented in accordance with the ISMS requirements.
Conformance with Standard

INDEX


4 Information security management system

4.1 General requirements

4.1.1 Establish the ISMS

a) Define the scope of the ISMS

b) Define an ISMS policy

c) Framework

d) Business, legal, regulatory and contractual requirements

e) Strategic organisational and risk management

f) Risk evaluation criteria

g) Management approval

h) Define the risk assessment approach of the organisation

CASE STUDIES
Mauritius

- Civil service-wide roll out
- Treasury, Civil Status, Passport & Immigration, Social Security, GOC, ...
- Plus a civil service-wide ISMS
- Drive towards being a cyber island of quality
- Has significantly increased security awareness – essential for a cyber-culture
- Just under 4 months from start to finish

Middle East

- Telecommunications * Petroleum
- Scope – just the IT department
- Need to take care because the ISMS is not responsible for everything
- Facilitating increased awareness and tuning of policies to business requirements (i.e. not just following ISO/IEC 17799 blindly, especially where the guidance is inappropriate
- Telecomm – 3 weeks to build
- Petroleum – 8 weeks to build
Eastern Europe

- Air traffic control

Business (air traffic control) excluded as subject to international regulations, so just IT component

- Just started

United Kingdom

- Fully integrated management system
- ISO 9001
- ISO/IEC 27001
- Finance
- Health and Safety
- Sales and Marketing (opportunity exploitation)

- ISO/IEC 27001 component built in 6 days
Summary

- Different strategies – go with what you have today is the best
- Fast track method works well
  - Won’t forget anything
  - Tell it like a story
  - To-Do-List for managing continual improvement, etc
  - Scalable
  - Build times: 2 few days to a few weeks
- But different organisations pose different challenges
- Built on world wide experience in many contexts
Implementing ISO/IEC 27001

Computer Security Week 30th November 2006

Any Questions?

Dr. David Brewer
Gamma Secure Systems Limited
www.gammassl.co.uk

©Gamma Secure Systems Limited, 2006