ISO/IEC 27001: Case Study – Data Centre Implementation

Dr. David Brewer, FBCS, MIOD

Conference of IT Heads of Banks, RBI, CAB, Pune 22 September 2007
Agenda

- General facts
- Strategy
- Approach
- Results
- Conclusions
GENERAL FACTS
Four data centres
Milestones

- M1 – Contract award
- M2 – ISMS approved
- M3 – Ready for certification
- M4 – Recommended for certification
- M5 – Fully operational
Project plan

- Build (M1-M3) 7 weeks
- M4 3 months later (dependent upon certification body constraints)
- M5 at first surveillance visit
STRATEGY
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

There will be little/no evidence of related security incidents
Strategies

- Build a brand new system
  - Aim to comply with ISO/IEC 27002
  - 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 (27002)

- Develop brand new policies and procedures according to ISO/IEC 27002

- 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*

---

As the controls are “new” no one knows what to do, so the auditor is likely to find that they are not followed. They will take time to bed in.

Vasa: sank in 1628 within 1 mile of the start of her maiden voyage
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
APPROACH
Overview

- Classroom/on-the-job training, throughout at least one PDCA cycle
- Event-impact RTPs
- Role Model
- To-Do-List concept
- Template ISMS
- Overarching/subordinate ISMS
- Integrate with existing internal control structures
- Marshal existing procedures/ records
- Combine with ISO 9001
- Combine with CVa, etc

3-6 months
Role Model
Role Model

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

©Gamma Secure Systems Limited, 2007
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, 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 Host Security Plan.</td>
</tr>
<tr>
<td>New ISMS Standard</td>
<td>ISO/IEC 27001, make the necessary security enhancements.</td>
</tr>
<tr>
<td>MSR Action 19.17</td>
<td>Add new risk (as in CRF).</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

©Gamma Secure Systems Limited, 2007
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” which 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 to improve - just put on the To-Do-List with an appropriate priority.
Template ISMS
Template ISMS

- Consultants’ productivity aid to speed the ISMS build process and ensure nothing is omitted

- Two current forms:
  - *Microsoft Word document*
  - *Adobe Dreamweaver web site*

- On the case study we used:
  - *Microsoft FrontPage web site*
Covers every requirement of ISO/IEC 27001

INTRODUCTION

Objective

This document is the Information Security Department. The objective of the ISMS is to ensure that all security policies and procedures are followed.

Contents

This document defines the scope of the ISMS and includes the Risk Assessment and Risk Treatment Plan and presents ISMS ISO/IEC 27001:2005. The SOA refers out to other sections.

It details the processes and procedures for training, ISMS Audit, Management Review and ISMS improvement.

It includes all the ISMS records.

Approval and Distribution Policy

We complete these parts

Version control

Internal ISMS Audit Report and Checklist

Department: 

Completed by:
Template ISMS

Welcome

Welcome to [Template ISMS].

The scope of our ISMS is:

- Put the organization (ISMS) in the box.
- The scope of the ISMS is to define the security objectives and controls that must be in place to ensure the confidentiality, integrity, and availability of information assets.

The ISMS was first approved on [date].

Layout

Use the navigation bar on the left of the page.

Information Security Management

This part of the ISMS deals with continual improvement. It explains how corrective and preventive action is taken and how improvements are managed. The need for such actions can arise at any time. This page explains what to do.

The overall process is illustrated in the following diagram:

©Gamma Secure Systems Limited, 2007
The Plan in Action
Phase A (Constructing the ISMS)

- Meetings as necessary to obtain info to construct the ISMS
- Inaugural ISF meeting
- Review meetings
- Initiate certification arrangements
Create the ISMS

A.5 Create Documented ISMS

A.5.1 Scope and Information Security Context
- A.5.1.1 Introduction
- A.5.1.2 Scope
- A.5.1.3 Context
- A.5.1.4 Assets
- A.5.1.5 Threat agents
- A.5.1.6 Vulnerabilities
- A.5.1.7 Adverse impacts
- A.5.1.8 "Other procedures"
- A.5.1.9 "Check&Act"
- A.5.1.10 "Continual improvement"
- A.5.1.11 "Control of records"

A.5.2 ISMS Policy

A.5.3 Develop RTPs

A.5.4 Statement of Applicability

A.5.5 Incident Handling and Effectiveness Measurement

A.5.6 Training & Awareness

A.5.7 Internal ISMS Audit Procedure and Schedule

A.5.8 Management System Review Procedure and Schedule

A.5.9 ISMS Document Control Procedure

A.5.10 To-Do-List

A.5.11 Compliance
Create the ISMS

A.5 Create Documented ISMS
  A.5.1 Scope and Information Security Context
    A.5.1.1 Introduction
    A.5.1.2 Scope
    A.5.1.3 Context
    A.5.1.4 Assets
    A.5.1.5 Threat agents
    A.5.1.6 Vulnerabilities
    A.5.1.7 Adverse impacts
    A.5.1.8 "Other procedures"
    A.5.1.9 "Check&Act"
    A.5.1.10 "Continual improvement"
    A.5.1.11 "Control of records"
  A.5.2 ISMS Policy
  A.5.3 Develop RTPs
  A.5.4 Statement of Applicability
  A.5.5 Incident Handling and Effectiveness Measuremements
  A.5.6 Training & Awareness
  A.5.7 Internal ISMS Audit Procedure and Schedule
  A.5.8 Management System Review Procedure and Schedule
  A.5.9 ISMS Document Control Procedure
  A.5.10 To-Do-List
  A.5.11 Compliance
Create the ISMS

A.5 Create Documented ISMS
   A.5.1 Scope and Information Security Context
      A.5.1.1 Introduction
      A.5.1.2 Scope
      A.5.1.3 Context
      A.5.1.4 Assets
      A.5.1.5 Threat agents
      A.5.1.6 Vulnerabilities
      A.5.1.7 Adverse impacts
      A.5.1.8 "Other procedures"
      A.5.1.9 "Check&Act"
      A.5.1.10 "Continual improvement"
      A.5.1.11 "Control of records"
   A.5.2 ISMS Policy
   A.5.3 Develop RTPs
   A.5.4 Statement of Applicability
   A.5.5 Incident Handling and Effectiveness Measurements
   A.5.6 Training & Awareness
   A.5.7 Internal ISMS Audit Procedure and Schedule
   A.5.8 Management System Review Procedure and Schedule
   A.5.9 ISMS Document Control Procedure
   A.5.10 To-Do-List
   A.5.11 Compliance
Phase B (Preparation for certification)

<table>
<thead>
<tr>
<th>Milestone Code</th>
<th>Milestone Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>B.1</td>
<td>Phase Initiation Meeting</td>
</tr>
<tr>
<td>B.2</td>
<td>Training</td>
</tr>
<tr>
<td>B.2.1</td>
<td>Classroom training</td>
</tr>
<tr>
<td>B.2.2</td>
<td>On-the-job audit training (desktop)</td>
</tr>
<tr>
<td>B.2.3</td>
<td>On-the-job audit training (implementation audits)</td>
</tr>
<tr>
<td>B.2.4</td>
<td>ISF training</td>
</tr>
<tr>
<td>B.3</td>
<td>Initiate Internal ISMS Audit Programme</td>
</tr>
<tr>
<td>B.4</td>
<td>Initiate Awareness Training Programme</td>
</tr>
<tr>
<td>B.4.1</td>
<td>Give Awareness Seminar</td>
</tr>
<tr>
<td>B.5</td>
<td>Conduct Management System Review</td>
</tr>
<tr>
<td>B.5.1</td>
<td>Conduct Management System Review</td>
</tr>
</tbody>
</table>

- **Training**: auditors and administrators
- **ISF Meeting**: (system review and agree readiness for certification)
- **Security awareness seminar**: (whole department)
Phase C (Certification)

<table>
<thead>
<tr>
<th>Milestone</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>81</td>
<td>Phase C - Certification</td>
</tr>
<tr>
<td>82</td>
<td>C.1 Initial Audit</td>
</tr>
<tr>
<td>83</td>
<td>C.1.1 Stage 1 audit</td>
</tr>
<tr>
<td>84</td>
<td>C.1.2 Stage 1 audit support</td>
</tr>
<tr>
<td>85</td>
<td>C.1.3 Stage 2 audit</td>
</tr>
<tr>
<td>86</td>
<td>C.1.4 Stage 2 audit support</td>
</tr>
<tr>
<td>87</td>
<td>C.2 Certification</td>
</tr>
<tr>
<td>88</td>
<td>C.2.1 Delcare recommended for certification</td>
</tr>
<tr>
<td>89</td>
<td>C.2.2 Certificate awarded</td>
</tr>
</tbody>
</table>

©Gamma Secure Systems Limited, 2007
RESULTS
Certification

ISD Achieves ISO/IEC 27001:2005 Certification

Information Services Department proudly announces that ISD has officially been certified for ISO/IEC 27001:2005 - Information Security Management as of April 3 2007 for all ISD related services. The certification audit was conducted by DNV Certification authority based in Norway after an extensive audit which was carried out in two phases. The objective of the Information Security Management System ISMS is to empower [redacted] to manage its information security risks.

[redacted] is the first [redacted] to acquire this prestigious ISO 27001 Certification.
Commendation

Based on Dr. David Brewer’s request, I wish to confirm that the Information Services Department of [Redacted] have recently received ISO 27001 Certification through the certification body of DNV (Det Norske Veritas) for all IT related services we provide to our company (5,500+ employees). The preparation for certification was handled jointly by Gamma Secure Systems Limited and Secure Matrix.

Thanks to Dr. David Brewer and his team, he had us prepared and ready in no time. His cheerful personality, confidence, great knowledge and professionalism will convince anyone that he is the best man for this type of job. It is worth mentioning that we had received more than 7 proposals for the same job but after meeting with him personally, we were immediately convinced to go with his team.

The scope of work included setting up and implementing the Information Security Management System (ISMS), assessing our current IT Security Status, recommending an action plan, setting up the Information Security Forum (ISF), training our staff to utilize and update the ISMS, train security officers to audit, and ultimately to prepare us technically and psychologically for the certification audit. This entire process took only 2 months which is incredibly quick and efficient compared with the other offers we received ranging from 4 months to 2 years! This also means cost savings.

[Redacted] Company is now considered the 1st [Redacted] in [Redacted] to achieve such certification and we are grateful for this achievement (Our certification number is [Redacted] UKAS).

[Redacted]
Conclusions

- Fundamental management system is quick to build
- It’s a management issue
- The concepts work in practice
- Together they meet the challenges of Basel II
- But not only that, they are a driver for success
ISO/IEC 27001: Case Study – Data Centre Implementation

Any Questions?

Dr. David Brewer, FBCS, MIOD

dbrewer@gammassl.co.uk

www.gammassl.co.uk