ISO/IEC 27001: The Standard

Dr. David Brewer, FBCS, MIOD

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

- Overview
- Information security
- ISO/IEC 27001
- ISO/IEC 27002
- Summary
OVERVIEW
History

Charged with establishing international IT Security 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

Ensure information security is always appropriate to your business
ISO/IEC 27002

- Security Policy
- Organising Security
- Asset Management
- Human Resources
- Physical and Environmental Security
- Communications and Operational Management
- Access Control
- Information Security
- 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
Accredited certification

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

The Audit
- Hold the Opening Meeting
- Perform the Audit
  - [Check previous actions]
  - Check documentation (e.g. SOA, risk analysis)
  - Check implementation (various interviews)
- Produce the Audit Report
- Hold the Closing Meeting
Other 27000 series standards

- 27000 – Overview and vocabulary
- 27003 – Implementation advice
- 27004 – Measurements
- 27005 – Risk management
- 27011 – Guidelines for telecommunications
International take-up

ISMS Registrations by Continent

3 September 2007
## International take-up

### 305

<table>
<thead>
<tr>
<th>Name</th>
<th>Location</th>
<th>Certification</th>
<th>Standard</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bank Of India</td>
<td>India</td>
<td>TW07/00002/SMS</td>
<td>SGS United Kingdom Limited ISO/IEC 27001:2005</td>
</tr>
<tr>
<td>ICICI BANK LIMITED - CTD, Mumbai</td>
<td>India</td>
<td>208788</td>
<td>Bureau Veritas Certification ISO/IEC 27001:2005</td>
</tr>
<tr>
<td>ICICI BANK LIMITED - DATA CENTER, Mumbai, Hyderabad</td>
<td>India</td>
<td>213817</td>
<td>Bureau Veritas Certification ISO/IEC 27001:2005</td>
</tr>
<tr>
<td>ICICI Bank Limited, C-SERV Phone Banking, Mumbai, Hyderabad</td>
<td>India</td>
<td>192679</td>
<td>Bureau Veritas Certification BS 7799-2:2002</td>
</tr>
<tr>
<td>ICICI Bank Limited, C-SERV Phone Banking, Mumbai, Hyderabad, Thane</td>
<td>India</td>
<td>192679</td>
<td>Bureau Veritas Certification ISO/IEC 27001:2005</td>
</tr>
<tr>
<td>ICICI Bank Limited-Global Trade Services Unit(GTSU)</td>
<td>India</td>
<td>IS 89521</td>
<td>BSI BS 7799-2:2002</td>
</tr>
<tr>
<td>ICICI Bank Ltd. - Global Trade Services</td>
<td>India</td>
<td>IS 89521</td>
<td>BSI ISO/IEC 27001:2005</td>
</tr>
<tr>
<td>Punjab National Bank Information Technology Division</td>
<td>India</td>
<td>IS 518289</td>
<td>BSI ISO/IEC 27001:2005</td>
</tr>
<tr>
<td>Reserve Bank of India</td>
<td>India</td>
<td>200</td>
<td>CIS ISO/IEC 27001:2005</td>
</tr>
<tr>
<td>Reserve Bank of India</td>
<td>India</td>
<td>18/0</td>
<td>CIS ISO/IEC 27001:2005</td>
</tr>
<tr>
<td>State Bank of India Information Security Department</td>
<td>India</td>
<td>IS 503689</td>
<td>BSI ISO/IEC 27001:2005</td>
</tr>
</tbody>
</table>

©Gamma Secure Systems Limited, 2007
What’s so special

20 years ago everyone thought information security was a technical issue
  - *Computers are highly technical devices*
  - *Software “easily” changed*

Actually it is a **management issue**, albeit with rapidly changing highly technical overtones due to the dominance of IT
Viruses

- Contagious often of pandemic proportion

- Impact depends on payload:
  - Denial of service
  - Disclosure
  - Back doors
  - Botnets
  - Time bombs...

- New ones discovered every day

For example, experts estimate that the Mydoom worm infected approximately a quarter-million computers in a single day in January 2004. (Times Online). Back in March 1999, the Melissa virus was so powerful that it forced Microsoft and a number of other very large companies to completely turn off their e-mail systems until the virus could be contained. The ILOVEYOU virus in 2000 had a similarly devastating effect. That's pretty impressive when you consider that the Melissa and ILOVEYOU viruses are incredibly simple.
Hacking

- Action at a distance or inside?
- Web site defacement
- Changing data
- Stealing data
- How do you know that it has happened?

Ehud Tenenbaum (Solar Sunrise)

Vladimir Levin (Citibank break ins)
Denial of service

- Viruses are not the only means
- Here an old fashioned SYN Flood

Other network attacks
- Ping floods (keep asking “are you there?”)
- Smurf (ping flood to an IP broadcast address)
- Ping of death (fragmented ping packet > 65535 bytes)
- Teardrop (fragmented packets and overlaps)
- LAND (forged SYN packets force target to talk to itself)
Password attacks

- **Password theft**
  - Sniffing passwords (e.g. L0PHT2.0), Shoulder surfing, dumpster-diving, sticky notes

- **Password guessing/cracking**
  - Dozens available free on the Internet (e.g. L0PHTCrack)

- **Social engineering**
  - Help desk, IT staff ruses, phishing

- **Could be more than just passwords**
  - Personal information
  - Credit card security codes

Source: http://www.antiphishing.org/
Eavesdropping

- TEMPEST (computers radiate)
- Wireless networks
- Wireless telephones
- Stand next to a person using a mobile
Application level attacks

- Over enthusiastic customers (*computers can’t cope with the load*)

- Amarillo (*Multi MB video, recipients sent it to their friends…*)

- Changing software to steal airtime (*e.g. “free” international mobile calls*)

- Exploiting ineffective financial controls in business systems to commit fraud (*Enron, Barings, …*)

- Errors (*e.g. In December 2005, a clerk sold 6500 shares at 1 yen instead of 1 share at 6500 yen, with a loss estimated at 225M US$*)
Fire, flood, monsoons

- Don’t mix well with IT
- Disaster recovery will work, but it detracts from meeting prime objectives
- Other causes:
  - Building work (cables cut)
  - Power outage
Conclusions

- Multi dimensional problem:
  - *Highly technical*
  - *Human*
  - *Physical*
  - *Environmental*
  - *Organisational*
  - *Legal*

- Potential extremely high event frequency

- Focus on prevention

- Can’t always tell you have been attacked

- Can’t forget detection and need for containment and recovery

- Ever changing threat

- Vastly differing risk postures

- Risk based “management system” (PDCA)

- Solid set of countermeasures
ISO/IEC 27001
Information Security Management Systems - Requirements

©Gamma Secure Systems Limited, 2007
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"
Risk Treatment Plans

- Risk Assessment (RA)
- Risk Treatment Plan (RTP)
- Statement of Applicability (SOA)
- Operate Controls
- Awareness Training
- Manage Resources
- Prompt Detection and Response to Incidents

PLAN

Scope • Policy •

DO

CHECK

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

©Gamma Secure Systems Limited, 2007
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

What shall we do?

- Avoid the risk
- Accept the risk
- Transfer the risk
- Mitigate the risk

Select the controls

Choose the appropriate controls
Statement of Applicability

- 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

MS Improvements
- Preventive Action
- Corrective Action

DO

ACT

CHECK

- Management Review
- Internal Audit

Secure Matrix

©Gamma Secure Systems Limited, 2007
Statement of applicability

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 (Annex A ~ IS 27002) is about
- Go through all 133 controls, say whether applicable or not
- Justify by giving the reason for its selection or exclusion

SOA ↔ “Alternative Ideas” List (AIL)

It is a “safety net”

NOTE: The Statement of Applicability provides a summary of decisions concerning risk treatment. Justifying exclusions provides a cross-check that no controls have been inadvertently omitted.
Awareness Training

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

ACT

CHECK

©Gamma Secure Systems Limited, 2007
Awareness training

- Awareness, training and competence
- Security principles
- Attacks
- Policies/procedures
- Incidents
- Key points

Eavesdropping

- TEMPEST (computers radiate)
- Wireless networks
- Wireless telephones (no encryption)

Stand next to a person using a mobile
Prompt detection ...

- Incident Identification and Reporting
- Incident Handling and Escalation
- Communicating Results and Tidying Up

<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>

©Gamma Secure Systems Limited, 2007
Internal ISMS Audit

- 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

- MS Improvements
- Preventive Action
- Corrective Action

DO

- Management Review
- Internal Audit

CHECK

©Gamma Secure Systems Limited, 2007
Internal ISMS audit

- An internal ISMS audit schedule
- Regularly check that controls as implemented meet policy objectives, e.g. reduce risks to the accepted level
Management Reviews

- Secure Matrix

PLAN
- Policy
- Scope
- Risk Assessment (RA)
- Risk Treatment Plan (RTP)
- Statement of Applicability (SOA)
- Operate Controls
- Awareness Training
- Manage Resources
- Prompt Detection and Response to Incidents

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

CHECK
Management reviews

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?
Metrics - Effectiveness

- 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

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

DO

CHECK

©Gamma Secure Systems Limited, 2007
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

Detect event in sufficient time to prevent or mitigate impact

1 - %CFES = (TCFES / TC) x 100
where TCFES = Σ co-workers who have received training in security, and TC = Total no. of co-workers

F – PFS = (IPF / TIS) x 100
where IPF = Σ Security incidents caused by lack of training, and TIS = Total no. of security incidents

1 - %SPSM = (TSP / TSA) x 100
where TSP = Σ Information systems protected from malware, and TSA = Total number of systems threatened by malicious software

Extracts from New ISO Work Item on ISMS metrics

©Gamma Secure Systems Limited, 2007
ISMS effectiveness

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

If not there will be an impact (or near miss)

May need to take action

PLAN

DO

CHECK

Statement of Applicability
Operate
Awareness
Manage
Board Review

Prompt Detection and Response to Incidents
Manage Resources
Internal ISMS Audit

Corrective Action
Preventive Action
Improvements

Need other checks as well

©Gamma Secure Systems Limited, 2007
ISO/IEC 27002
Code of Practice for Information Security Management
ISO/IEC 27002

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  
Business Continuity Management  
Compliance  

But this is more than just IT, as we learnt earlier.
Recast in the form of a story

- **Deployment**: reduce the likelihood of our staff/contractors from causing a security breach
- **A secure environment**: restricting physical access to information in the workplace
- **Outside work**: Taking care when sending or using (non-IT) information outside the workplace
- **Open (computer) access**: Controlling access to computers that an attacker can physically access in the workplace
- **Action at a distance**: Protecting our computers from cyber attack
- **Applications**: Making sure that our applications are secure
- **Operating conditions**: Making sure our computer hardware works
- **Does it work?**: Asking how we can check that our security controls are working before we are attacked
- **When things go wrong**: What do we do when there is an incident
For example: deployment...

- Internal control is about marshalling our objectives to achieve our mission

- Wish to deploy people to do that
  - Our staff (employees, officers, ...)
  - Contractors

- We want them to follow our rules

- So what are they?

<table>
<thead>
<tr>
<th>A.5</th>
<th>Security policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>A.5.1</td>
<td>Information security policy</td>
</tr>
<tr>
<td>Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>A.5.1.1</th>
<th>Information security policy document</th>
<th>Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>An information security policy document shall be approved by management, and published and communicated to all employees and relevant external parties.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Deployment...

- But what are these laws and regulations? We need to ensure that our policy is legal...

- And there is a whole host of these ... but you need to see which ones apply first
Disposition of controls

- Carry on like this and we will use up all 133 controls

<table>
<thead>
<tr>
<th></th>
<th>Policy</th>
<th>Organisation</th>
<th>Asset Management</th>
<th>HR</th>
<th>Physical</th>
<th>Operations</th>
<th>Access control</th>
<th>Development</th>
<th>Incident Handling</th>
<th>BCP</th>
<th>Compliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deployment</td>
<td>2</td>
<td>6</td>
<td>6</td>
<td></td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A secure environment</td>
<td></td>
<td></td>
<td></td>
<td>5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2</td>
</tr>
<tr>
<td>Outside work</td>
<td>1</td>
<td>4</td>
<td>2</td>
<td></td>
<td>3</td>
<td>6</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Open (computer) access</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>11</td>
</tr>
<tr>
<td>Action at a distance</td>
<td>1</td>
<td>1</td>
<td>4</td>
<td>11</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Applications</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>13</td>
<td>1</td>
<td>12</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operating conditions</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>3.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Does it work?</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2</td>
</tr>
<tr>
<td>When things go wrong</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>7</td>
<td>4</td>
<td>5</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>
Excellent IT focus

- Covers physical, environmental and personal security, compliance with the law etc, but ...
- ... IT component focuses on IT platforms
- Generic foundations for business applications
- Indeed scope of ISO/IEC 27001 is everything concerning information security, including the business applications
- You may supplement with other AILs
SUMMARY
Summary

- Comprehensive standard for information security
- Management standard (Plan-Do-Check-Act)
- Allows controls to adapt to changing circumstances (policy getting in the way of the business? – change the policy)
- Comprehensive IT-platform focussed AIL
- Increases awareness – better security – better business
ISO/IEC 27001: The Standard

Any Questions?

Dr. David Brewer, FBCS, MIOD

dbrewer@gammassl.co.uk

www.gammassl.co.uk