MS ISO/IEC 27001:2007
INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS) IMPLEMENTATION

By: Noor Aida Idris  CISSP, ISMS Lead Auditor
CyberSecurity Malaysia
AGENDA

• Introduction to Information Security Management System (ISMS)

• ISMS Implementation

• Benefit of ISMS Certification for CyberSecurity Malaysia

• Critical Success Factors
WHAT IS INFORMATION SECURITY?

Preservation of **confidentiality**, **integrity** and **availability** of information; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved


- **Confidentiality** - the property that information is **not disclosed** to unauthorized individuals, entities, or processes

- **Integrity** - the property of safeguarding the **accuracy** and **completeness** of information

- **Availability** - the property of being **accessible** and **usable upon demand** by an authorized individuals, entities, or processes
CYBER SECURITY INCIDENTS (1997-2009)

- A total of 13,314 security incidents referred since 1997 (excluding spams)
- For year 2009, total no. of spams detected was a whooping 184,407

Source: MyCERT
CONSEQUENCES OF SECURITY INCIDENTS

What is the level of significance for the following consequences if your organization’s information is lost, compromised or unavailable?

- Damage to reputation and brand: 85%
- Loss of stakeholder confidence: 77%
- Loss of revenues: 72%
- Loss of customers: 71%
- Regulatory action/sanction: 68%
- Litigation/legal action: 65%
- Damage to employee relationships: 49%

Source: Ernst & Young, 2008
HOW DO WE RESPOND?

- Understand the threats
- Mitigate the risks
- Security strategy – people, process, technology
- Establish security requirements:
  - Risk assessment
  - Legal, statutory, regulatory and contractual requirements
  - Set of principles, objectives and business requirements for information processing that an organization has developed to support its operations
WHAT IS ISMS?

• ISMS is that part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security.

• The management system includes organizational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources.

WHY ISMS?

Objective of information security as defined in ISO/IEC 27002

“To minimize the risks and impacts to business whilst maximising business opportunities and investments and to ensure business continuity”
AGENDA

- Introduction to Information Security Management System (ISMS)
- **ISMS Implementation**
- Benefit of ISMS Certification for CyberSecurity Malaysia
- Critical Success Factors

- Information technology – Security techniques – Information security management systems - Requirements
- **Certification and auditable standard**
- Mandatory risk based approach
- Clause 4 to Clause 8 – conformity clauses
SUMMARY OF MS ISO/IEC 27001:2007

- 4: Information Security Management System
  - 4.1 General Requirements
  - 4.2 Establishing & managing information security
    - 4.2.1 Establish the ISMS
    - 4.2.2 Implement & operate ISMS
    - 4.2.3 Monitor & review ISMS
    - 4.2.4 Maintain & improve ISMS
  - 4.3 Documentation requirements
    - 4.3.1 General
    - 4.3.2 Control of documents
    - 4.3.3 Control of records

- 5: Management responsibility
  - 5.1 Management commitment
  - 5.2 Resource management
    - 5.2.1 Provision of resources
    - 5.2.2 Training, awareness & competence

- 6: Internal ISMS Audit

- 7: Management Review of ISMS
  - 7.1 General
  - 7.2 Review input
  - 7.3 Review output

- 8: ISMS Improvement
  - 8.1: Continual improvement
  - 8.2: Corrective action
  - 8.3: Preventive action
MS ISO/IEC 17799:2006 or ISO/IEC 27002:2005

- Establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization
- It contains best practices of control objectives and controls (with some implementation guidelines) in many areas of information security management
- The controls listed are also included in MS ISO/IEC 27001 Annex A
- It is NOT a certification and auditable standard
OVERVIEW OF ISMS IMPLEMENTATION

Information Security Management Requirement
(based on MS ISO/IEC 27001:2007)

Information Security Controls
(based on ISO/IEC 27002:2005)
[11 areas, 133 controls]
The organization shall establish, implement, operate, monitor, review, maintain and improve a documented ISMS within the context of the organization’s overall business activities and the risks they face.

Clause 4.1 General Requirements
ISMS Implementation - CyberSecurity Malaysia’s experience

2006
- Preliminary study on NISER ISMS implementation
- Kickoff of the ISMS Implementation – PLAN Phase

2007
- Implement and resume the DO, CHECK and ACT Phase
- Risk Assessment
- Awareness & training programme
- Internal audit

2008
- 1st stage audit
- 2nd stage audit
- We are certified!

2009
- Surveillance audit

2010
- Surveillance audit

Continuous Improvement

Copyright © 2010 CyberSecurity Malaysia
SMBP-S-PSL-14-ISMS-v1
ESTABLISH THE ISMS

- Define the scope and boundaries of the ISMS
- Define an ISMS policy
- Define the risk assessment approach of the organization
- Identify the risks
- Analyse and evaluate the risks
- Identify and evaluate options for the treatment of risks
- Select control objectives and controls for the treatment of risks
- Obtain management approval of the proposed residual risks
- Obtain management authorization to implement and operate the ISMS.
- Prepare a Statement of Applicability (SOA)
DEFINE THE SCOPE AND BOUNDARIES OF ISMS

- Define the scope and boundaries of the ISMS in terms of the characteristics of the business, the organization, its location, assets, technology, and including details of and justification for any exclusions from the scope.

- Limited part of organization or the whole organization.
DEFINE AN ISMS POLICY

- Define an ISMS policy in terms of the characteristics of the business, the organization, its location, assets and technology and taking account any legal and regulatory requirements.

- Takes into account business and legal or regulatory requirements, and contractual security obligations.

- Should be approved by management.
RISK ASSESSMENT APPROACH

• Risk Assessment - the overall process of risk analysis (systematic use of information to identify sources and to estimate risk) and risk evaluation (process of comparing the estimated risk against given risk criteria to determine the significance of risk)

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

• Conduct risk assessment
PREPARE SOA

• Statement of Applicability (SOA)

• SOA is a document describing:
  – the control objectives and controls selected and the reasons for selections
  – the control objectives and controls currently implemented
  – the reasons for the exclusions
IMPLEMENT AND OPERATE THE ISMS

- Formulate and implement risk treatment plan
- Implement and operate controls
- Measure effectiveness of selected controls
- Implement training and awareness programmes
- Manage operation of the ISMS
- Manage resources
- Implement procedures and other controls
IMPLEMENT CONTROLS

• Implement controls that has been selected in risk assessments and treatments:

• Controls objectives and controls from Annex A MS ISO/IEC 27001 shall be selected; additional control objectives and controls may also be selected.
MEASURE EFFECTIVENESS

• Achieving effective information security by balancing business requirements with security requirements

• Metrics of measurement should be:
  – Accurate and reliable information
  – Repeatable, verifiable and scalable
IMPLEMENT TRAINING AND AWARENESS PROGRAMME

• The aim of training and awareness program is to generate a well-founded risk management and security culture.

• Specific security training should be applied wherever necessary to support the awareness program, and to enable all parties to fulfill their security tasks.
# AWARENESS & TRAINING

<table>
<thead>
<tr>
<th>AWARENESS/ TRAINING</th>
<th>ISMS TRAINING PROGRAM</th>
<th>MODULE/TOOL TARGET</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISMS competency training</td>
<td>• ISMS Implementation</td>
<td>• ISMS implementers</td>
</tr>
<tr>
<td></td>
<td>• Certified Lead Auditor</td>
<td>• ISMS internal auditors</td>
</tr>
<tr>
<td></td>
<td>• Risk assessment training</td>
<td>• Senior management</td>
</tr>
<tr>
<td>ISMS introduction training employees</td>
<td>• Standards requirements &amp; code of practice</td>
<td>All employees</td>
</tr>
<tr>
<td></td>
<td>• Risk assessment workshop</td>
<td></td>
</tr>
<tr>
<td>General ISMS awareness</td>
<td>• Awareness talks</td>
<td>All employees</td>
</tr>
<tr>
<td></td>
<td>• Posters</td>
<td>3rd party (vendor, consultant, etc)</td>
</tr>
<tr>
<td></td>
<td>• Email messages</td>
<td></td>
</tr>
<tr>
<td>ISMS assessment</td>
<td>• Ad-hoc quizzes</td>
<td>All employees</td>
</tr>
<tr>
<td></td>
<td>• Online test</td>
<td></td>
</tr>
</tbody>
</table>
AWARENESS MATERIALS – POSTERS SAMPLE

BE SMART!
SECURE YOUR NOTEBOOK

- Always lock using anti-theft device or security alarm
- Never leave unsecured notebook unattended
- Protect notebook with unique password
- Enable screen saver with password
- Encrypt sensitive data

HAVE YOUR PEACE OF MIND
TO HOUSE YOUR BUSINESS
CRITICAL DATA BUT
IS YOUR SERVER SECURE?

- Install the most recent service pack
- Get all available critical updates and OS security patches
- Assign a strong password
- Delete or secure old setup files
- Audit and check logs regularly
MONITOR AND REVIEW THE ISMS

- Monitor and review performance
- Review the risks and carry out risk reassessments
- Review incident handling results
- Management reviews
- Review the effectiveness of the controls
- Audits
REVIEW OF THE ISMS

- Regular Review of ISMS Effectiveness
  - Taking into account results of security audits, incidents, suggestions and feedback from all interested parties

- Review Level of Residual and Acceptable Risk
  - Taking into account the changes to the organization, technology, business objectives and processes, identified threats, and external events

- Regular Management Review of ISMS
  - Management shall review the ISMS at planned intervals to ensure its continuing suitability, adequacy and effectiveness
CONDUCT INTERNAL ISMS AUDITS

• Internal audit shall be conducted at planned intervals to determine whether the controls objectives, controls, processes and procedures:
  – Conform to the identified security requirements
  – Are effectively implemented and maintained
  – Perform as expected
MAINTAIN AND IMPROVE THE ISMS

- Implement identified improvements
- Take corrective and preventive actions
- Communicate actions and improvements
- Ensure improvements achieve intended objective
IMPLEMENT IDENTIFIED IMPROVEMENTS

• Organization shall continually improve the effectiveness of the ISMS through the use of the information security policy, security objectives, audit results, analysis of monitored events, corrective and preventive actions and management review.
DETECT NONCONFORMITY

- Nonconformity:
  - the absence of, or failure to implement and maintain one or more ISMS requirements; or
  - a situation which would, on the basis of available objective evidence, raise significant doubt as to the capability of the ISMS to fulfill the information security policy and security objectives of the organization
TAKE CORRECTIVE/PREVENTIVE ACTIONS

• Corrective action
  – to eliminate the cause of a nonconformity or other undesirable situation to prevent recurrence

• Preventive action
  – to eliminate the cause of a potential noncompliance or other undesirable potential situation
AGENDA

• Introduction to Information Security Management System (ISMS)

• ISMS Implementation

• **Benefit of ISMS Certification for CyberSecurity Malaysia**

• Critical Success Factors
BENEFITS OF ISMS FOR CYBERSECURITY MALAYSIA

• Increase information security awareness amongst the staff
• Reduced number of security incident by improving management of information security incident and from lesson learnt
• Risks are well managed especially when staff become more risk aware
• Systematic approach to manage information security for our organization
AGENDA

• Introduction to Information Security Management System (ISMS)

• ISMS Implementation

• Benefit of ISMS Certification for CyberSecurity Malaysia

• **Critical Success Factors**
CRITICAL SUCCESS FACTORS

• Management commitment and support
• Good understanding of security requirements, risk assessment and risk management
• Effective awareness programs, training and education in inculcating security as a culture
• Willingness “to change”
• Distribution of guidance on information security policy and standards to all managers, employees and other parties
• Make it a fun thing, NOT a serious subject
CyberSAFE Program

Cyber Security Awareness For Everyone

Let’s Make The Internet A Safer Place

www.cyberSAFE.my

Who am I?

Parents

Kids

Adults

Youths

Organizations

Securing Our Cyberspace
CyberSAFE, short for Cyber Security Awareness For Everyone, is CyberSecurity Malaysia’s initiative to educate and enhance the awareness of the general public on the technological and social issues facing internet users, particularly on the dangers of getting online.

CyberSAFE aims to provide the necessary information and resources to all targeted groups for them to be able to make informed choices and manage the abovementioned issues easier.

Welcome to CyberSAFE website

Be Smart Be Safe

Please select your category on how to protect yourself and your computer.

Who am I?

Parents

Kids

Adults

Youths

Organizations

CyberSAFE Digest

- Web Zine Archive
- e-Security Bulletin
- CyberSAFE Newsletter
- Guidelines

CyberSAFE Multimedia Content

- Video
- Poster
- Games & Quizzes
- Cyber Tools

CyberSAFE Community

- CyberSAFE Ambassador
- Learning Zone
- ActiveZone
- News Highlights

CyberSAFE Help

- Cyber999
- CyberSAFE First Aid
- Speaker Request
- Contact Us

Cybersafe Malaysia is on Facebook

Join CyberSAFE Malaysia for

SAFER INTERNET DAY 2010
on 9 February and WIN
GREAT PRIZES!

www.cybersafe.my
CyberSAFE Activities

CyberSAFE Awareness Talk

CyberSAFE Forum

CyberSAFE Multimedia References

CyberSAFE Digital Content Competition

<table>
<thead>
<tr>
<th>VIDEO COMPETITION</th>
<th>VALUE</th>
<th>POSTER COMPETITION</th>
<th>VALUE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. JVC HD Video Camera GC-FM1</td>
<td>1,500</td>
<td>1. Netbook</td>
<td>1,500</td>
</tr>
<tr>
<td>2. iPod Touch 8GB</td>
<td>850</td>
<td>iPod Touch 8GB</td>
<td>850</td>
</tr>
<tr>
<td>3. Panasonic Lumix DMC-FS12</td>
<td>750</td>
<td>Panasonic Lumix DMC-FS12</td>
<td>750</td>
</tr>
<tr>
<td>4. iPod Nano</td>
<td>650</td>
<td>iPod Nano</td>
<td>650</td>
</tr>
<tr>
<td>5. Samsung 3.5&quot; 1TB Drive</td>
<td>400</td>
<td>Samsung 3.5&quot; 1TB Drive</td>
<td>400</td>
</tr>
<tr>
<td>6. FlashDrive 32Gb</td>
<td>300</td>
<td>FlashDrive 32Gb</td>
<td>300</td>
</tr>
<tr>
<td>7. FlashDrive 32Gb</td>
<td>300</td>
<td>FlashDrive 32Gb</td>
<td>300</td>
</tr>
<tr>
<td>8. FlashDrive 16GB</td>
<td>180</td>
<td>FlashDrive 16GB</td>
<td>180</td>
</tr>
<tr>
<td>9. FlashDrive 16GB</td>
<td>180</td>
<td>FlashDrive 16GB</td>
<td>180</td>
</tr>
<tr>
<td>10. FlashDrive 16GB</td>
<td>180</td>
<td>FlashDrive 16GB</td>
<td>180</td>
</tr>
</tbody>
</table>

TOTAL VALUE | 5,290 | 5,290

Copyright © 2010 CyberSecurity Malaysia

CyberSAFE Community Partners
CONCLUSION

Security is EVERYONE’s responsibility!

“Information security is a major priority at this company. We’ve done a lot of stupid things we’d like to keep secret.”
Corporate Office:
CyberSecurity Malaysia,
Level 8, Block A,
Mines Waterfront Business Park,
No 3 Jalan Tasik, The Mines Resort City,
43300 Seri Kembangan,
Selangor Darul Ehsan, Malaysia.

T +603 8946 0999
F +603 8946 0888

www.cybersecurity.my

CyberSecurity Malaysia is
ISO/IEC 27001 Certified!