چالش های پیاده سازی و اخذ گواهینامه ی نظام مدیریت امنیت اطلاعات

ISMS Implementation and Certification CHALLENGES
Presenter

• Hossein Teimoori

• ISMS Lead Auditor
• ISMS Lead Tutor (IRCA Approved)
• +200 Audits
Content

- ISMS Definitions
- ISMS Standards
- ISMS History
- ISO 27001 Structure
- ISMS Implementation process
- Certification
- Implementation Process
- Certification cycle
- ISMS Implementation & Certification Challenges + Tips
Definitions
Information is an asset that, like other important business assets, is essential to an organization’s business and consequently needs to be suitably protected.

یک دارایی سازمانی است که مانند سایر دارایی‌های مهم سازمان برای کسب و کار (ماموریت) آن ضروری بوده و در نتیجه می‌بایستی به نحو مناسبی محافظت شود.
**Information Formats**

- Printed or written on paper
  - روی کاغذ
- Stored electronically
  - ذخیره شده بصورت الکترونیکی
- Transmitted by post or electronic means
  - قابل انتقال بوسیله ی پست یا ابزارهای الکترونیکی
- Shown on corporate videos
  - قابل پخش بصورت فیلم ها ویدئویی
- Verbal - spoken in conversations
  - قابل صحبت شدن
- ‘… Whatever form the information takes, or means by which it is shared or stored, it should always be appropriately protected.’

Source: ISO 27002:2007
Information Lifecycle

-Creation
-Use
-Destruction
1. **Information**: databases and data files, contracts and agreements, system documentation, research information, user manuals, training material, operational or support procedures, business continuity plans, fallback arrangements, audit trails, and archived information;

2. **Software assets**: application software, system software, development tools, and utilities;

3. **Physical assets**: computer equipment, communications equipment, removable media and other equipment;

---

1. Source (ISO 27002 page 19)
4) **Services**: computing and communications services, general utilities, e.g. heating, lighting, power, and air-conditioning;

4) **داراییهای خدماتی**: سرویس‌های ارتباطی و محاسباتی، تجهیزات عمومی مانند سیستم گرمایش، نور، تهویه هوا و ... 

5) **People**, and their qualifications, skills, and experience;

5) **داراییهای انسانی**: و شایستگی‌ها، مهارت‌ها و تجربیات آنها 

6) **Intangibles**, such as reputation and image of the organization.

6) **داراییهای نا ملموس**: مانند شهرت و وجهه سازمان 

1. Source (ISO 27002 page 19)
• **Confidentiality**: the property that information is not made available or disclosed to unauthorized individuals, entities, or processes

محرمانگی: ویژگی عدم دسترسی افراد غیرمجاز به اطلاعات

• **Integrity**: the property of safeguarding the accuracy and completeness of assets

یکپارچگی: ویژگی صحت و تمامیت اطلاعات

• **Availability**: the property of being accessible and usable upon demand by an authorized entity

دسترس پذیری: ویژگی امکان دسترسی و استفاده از اطلاعات در صورت درخواست یک موجودیت مجاز
PDCA Cycle

Plan
- What to do?
- How to do it?

Do
- Do what was planned

Act
- How to improve next time?

Check
- Did things happen according to plan?

INPUTS

OUTPUTS
Continual improvement of the management system

بهبود مداوم سیستم مدیریت

Interested Parties
ذینفعان

I.S. requirements & expectations
الزامات و انتظارات

Managed information Security
امنیت اطلاعات مدیریت شده

Plan
برنامه‌ریزی

Establish
استقرار

Implement & operate
پیاده‌سازی و اجرا

Monitor & review
پایش و بازنگری

Check
چک

Do
اجرا

Act
اقدام

Maintain & improve
نگهداری و بهبود
PDCA Cycle’s ROLE

**Plan**
Improving Process through PDCA Cycle

- **Improvement Objective**: Measure and monitor results against objectives.
- **Baseline Performance**: Improve process and change ISMS as needed to achieve and sustain desired results.

**Do**

**Act**

**Check**

Results
ISMS Standards

استانداردها
<table>
<thead>
<tr>
<th>Title</th>
<th>Title</th>
<th>Title</th>
<th>Title</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO27000</td>
<td>Vocabulary &amp; Fundamentals</td>
<td>مفاهیم و واژگان</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISO27001</td>
<td>Requirements</td>
<td>الزامات</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISO27002</td>
<td>Code of Practice (Already known as ISO17799)</td>
<td>راهنمای عملکرد (قبل با عنوان ISO17799 شناخته می‌شود)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISO27003</td>
<td>Implementation guidance</td>
<td>راهنمای پیاده‌سازی</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISO27004</td>
<td>Metrics &amp; measurement</td>
<td>شاخص‌ها و انداده گیری کنترل‌ها</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISO27005</td>
<td>Guidelines for Risk Management</td>
<td>راهنمای مدیریت ریسک</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISO27006</td>
<td>Assessment and certification</td>
<td>الزامات ارزیابی و صدور گواهینامه</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISO27007</td>
<td>Guidelines for auditing ISMS</td>
<td>ISMS راهنمای مميزی</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISO27008</td>
<td>Guidance on auditing information security controls</td>
<td>راهنمای مميزی کنترل‌های اطلاعاتی</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### ISMS-related Standards

<table>
<thead>
<tr>
<th>Title</th>
<th>عنوان</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO/IEC TR 13335 Guideline for management of IT security</td>
<td>راهنماي مديريت امنيت IT</td>
</tr>
<tr>
<td>ISO19011 Guideline for auditing Mng Systems</td>
<td>راهنماي مميزي سيستم هاي مديریتی</td>
</tr>
<tr>
<td>ISO17021 Requirements for assessment and certification bodies</td>
<td>الزامات نهادهای ارزیابی و صدور گواهینامه</td>
</tr>
</tbody>
</table>
ISO 27001 History
<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>1993</td>
<td>Industry working group was initiated and code of practice issued</td>
</tr>
<tr>
<td>1995</td>
<td>BS7799-1 was formalized</td>
</tr>
<tr>
<td>1998</td>
<td>BS7799-2 was formalized</td>
</tr>
<tr>
<td>1999</td>
<td>BS7799-1 &amp; BS7799-2 were published</td>
</tr>
<tr>
<td>2007</td>
<td>ISO27006:2007 is formalized</td>
</tr>
<tr>
<td></td>
<td>ISO17799:2005 was renamed ISO27002</td>
</tr>
<tr>
<td>2008</td>
<td>ISO27005:2008 is formalized</td>
</tr>
</tbody>
</table>
ISO 27001
STRUCTURE
ISO 27001:2005

- ISMS: System Management of Information Security
- Management Responsibility
- Internal Audit
- Management Review of ISMS
- ISMS Improvement

Sections:
- Intro
- Scope
- Norm. Refer.
- Terms & Defin.

Annexes:
- Annex A: Control Objectives & Controls
- Annex B: OECD Principles
- Annex C: Correspondence to 9k & 14k
<table>
<thead>
<tr>
<th>خط مشی امنیت 5</th>
<th>ساختار امنیت اطلاعات 6</th>
<th>مادیت دارایی‌های امنیت</th>
<th>مدیریت رویدادهای امنیت اطلاعاتی 13</th>
<th>مدیریت تداوم حیات سازمانی 14</th>
<th>انطباق 15</th>
</tr>
</thead>
<tbody>
<tr>
<td>A.8 امنیت منابع</td>
<td>A.9 محیط فنی</td>
<td>A.10 عملکرد امنیت</td>
<td>A.11 دسترسی</td>
<td>A.12 اطلاعات نیکه‌داری</td>
<td></td>
</tr>
</tbody>
</table>
ISO27001- 
Annex A /// ISO27002
ISO 27001
Objectives
Risk Management

- Risks
- Residual Risks
- Safeguards

ریسک ها
ریسکهای باقی مانده
اقدامات کنترلی
Continual Improvement

Continuous Improvement

Act  | Plan
Check | Do

Consolidation through Standardization

Standard

Time

Improvement

25/49  H.Teimoori  ISMS Implementation & Certification Challenges
ISMS IMPLEMENTATION Process

Exercise: Identifying relevant controls
Implementation Process

Plan
- Measure Current Security Control
- Updating Assets Database
- Risk Assessment

Do
- Security Awareness programs
- Develop sets of procedure

Check
- Measure and Analyze Controls Effectiveness
- Perform Compliance Audit
- Management Review

Act
- Improve its Capabilities and Maturity in Information Security

Implement ISMS within scope
- Security clauses
  - Security policy
  - Asset management
  - Human resources security
  - Organizing information security
  - Access control
  - Communications and operations management
  - Physical and environmental security
  - Information security incident management
  - Business continuity management
  - Information systems, acquisition, development and maintenance
  - Compliance
Implementation Process

TMMI V 3.1 Consultancy, Implementation and Audit Services Framework

Abbreviations:

KPL = Kualitatem Private Limited, PEG = Process Engineering Group, TMMI® = Test Maturity Model Integration
ISMS CERTIFICATION
The value of certification is
THE DEGREE OF PUBLIC CONFIDENCE AND TRUST
that is established by an impartial and competent assessment by a third-party.

(Clause 4.1.2)
ISO 17021 Certification Process

- Contract
- Pre Audit
- Stage 1 Audit
- Stage 2 Audit
- Surveillance Audit 1
- Surveillance Audit 2
- Certification/Registration

Flowchart showing the stages:
1. Initial Audit
2. Stage 1 Audit
3. Stage 2 Audit
4. Surveillance Audit 1
5. Surveillance Audit 2
6. Certification/Registration
7. Pre Audit
8. Contract
Overview of ISO/IEC 17021

Stage 1

Stage 2

Certification

Surveillance 1

Sanctions

Re-Certification

NC Closing Process

Rest of Certification Cycle
Common Implementation Challenges

- Wrong scoping
- Wrong estimation of time and costs
- Change Fear/resistance
- Intra-Organizational Competitions
- Problematic steering

Common CERTIFICATION Challenges (NC Root-Causes)

- Lack of Management commitment
- Ignorance of external parties issues
- Inappropriate Risk Assessment
- Lack of proactive approach
Wrong SCOPING

Tips:
- Use Gap Analysis
- Prioritize
- Initial Scope can be extended later
2 Wrong Time & Cost Estimation

Tips:
- Benchmark
- Initial Study / Gap Analysis
- Prepare for worst scenario

Project progress and reason for delays

- You can replace this sample text with your own text
- You can replace this sample text with your own text

©2012 Presentation-Process.com
### Fear/resistance to Change

#### Reasons

1. Misunderstanding about the need for change
2. Fear of the unknown
3. Lack of competence
4. Connected to the old way
5. Low trust
6. Temporary fad
7. Not being consulted
8. Poor communication

...
Fear/resistance to CHANGE

Reactions to Change

Self-esteem

Denial

Anger

Confusion

Depression

Crisis

Acceptance

New confidence

Time
Fear/resistance to CHANGE

Key barriers to successful change

IBM Survey

- Changing mindsets and attitudes: 58%
- Corporate culture: 49%
- Lack of commitment of higher...: 32%
- Shortage of resources: 33%
- Complexity is underestimated: 35%
- Lack of transparency because of...: 18%
- Lack of change know how: 20%
- Lack of motivation of involved employees: 16%
- Change of IT systems: 12%
- Change of process: 15%
- Technology barriers: 8%
3 Fear/resistance to CHANGE

Key ingredients for successful change

- Monetary and non-monetary incentives: 19%
- Efficient organization structure: 33%
- Adjustment of performance measures: 36%
- Efficient training programs: 38%
- Change supported by culture: 48%
- Change agents (pioneers of change): 55%
- Corporate culture that motivates and...: 65%
- Honest and timely communication: 70%
- Employee involvement: 72%
- Top management sponsorship: 92%
ISMS Implementation & Certification Challenges

Fear/resistance to CHANGE

Change Management Steps

1. Create urgency
2. Create a coalition
3. Develop a vision and strategy
4. Communicate the vision
5. Empower action
6. Get quick wins
7. Leverage wins to drive change
8. Embed in culture

Creating a climate for change

Engaging and enabling the whole organization

Implementing and sustaining change

*The 8-Step Process for Leading Change – Dr. John Kotter*
Problematic

Intra-Org Competitions

Tips:
- Know about “Conflict Management”
- Identify in advance and Manage during the implementation phase
Inappropriate Steering

Tips:
- Use a experienced & qualified consultant
- Get enough trainings
Lack of Management commitment

Tips:
- Not to show off
- Long Term Look (Think of more than 1 contract)
7 Ignorance of External Parties Issues

Tips:
- Define and Follow SLAs/OLAs before RA
8 Inappropriate RISK ASSESSMENT

Tips:
- Solid Procedure
- Cross Functional Team
- Owner
Loss of Initial Driver

Tips:
- Act Flexibly and as needed
با تشکر

H.Teimoori@nis-cert.com