Developing Enterprise Security Framework

www.infogistic.com
Developing Enterprise Security Framework

- **READI**

  - **R**eadize Enterprise Security Needs
  - **E**valuate Existing Security Posture
  - **A**ssess Enterprise Risks
  - **D**efine Process to Regulate Technology
  - **I**mplement a Security Management System
Realize Enterprise Security Needs

- Establish enterprise security needs based on company’s
  - Objectives
  - Business functions
  - Operational environment
  - Governing laws and regulations
  - Future directions and initiatives
Evaluate Existing Security Posture

- Review existing security arrangements
- Identify Strengths
- Identify Weaknesses
Evaluate Existing Security Posture: Examples

- Gap Analysis against
  - ISO 27001 Information Security Management System
  - ISO 27002 Code of Practice for Information Security Management System
  - ISO 22301

- Security Assessments
  - Network Architecture Security Review
  - Security Configuration Review
    - Network Devices
    - Operating Systems
Assess Enterprise Risks

- Build Inventory of Assets
- Analyze Risks
- Evaluate Risks
Assess Enterprise Risks: Examples

NIST SP 800-39 Managing Information Security Risk
Assess Enterprise Risks: Examples

- **ISO 27005:2011**
  - Security Techniques – Information security risk management

- **ISO 31000:2009**
  - Risk Management – Principles and guidelines
Define Process to Regulate Technology

- Identify owner
- Assign responsibility
- Check for compliance
- Measure performance
- Identify Improvements
- Report Results
Define Process to Regulate Technology: Examples

Technology

- Acquire and implement SIEM Tool

Process

- Log management procedure
- Log review procedure
- Staffing structure
- Segregation of duties
- Incident management
- Compliance
Implement a Security Management System

- Establish Security Organization
- Document Policies and Procedures
- Develop & Implement Awareness Program
- Perform Compliance Checks
- Improve Security Management System
Implement a Security Management System: Examples

- ISO 27001:2013
  - Security techniques – Information security management systems – Requirements

- ISO 27002:2013
  - Security techniques – Code of practice for information security controls
Standard & Best Practices: ISO 27001

- ISO 27001:2013
  - Information Security Management System - Requirements

  - Specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization

  - Includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization
# Standard & Best Practices: ISO 27001

## ISO 27001: 2013 Information Security Management System

## Plan

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Understanding the organization and its context</td>
<td>Leadership &amp; commitment</td>
<td>Actions to address risks &amp; opportunities</td>
<td>Resources</td>
</tr>
<tr>
<td>Expectation of Interested parties</td>
<td>Policy</td>
<td>IS objectives and plans to achieve them</td>
<td>Competence</td>
</tr>
<tr>
<td>Scope of ISMS</td>
<td>Organization roles, responsibilities &amp; authorities</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISMS</td>
<td></td>
<td></td>
<td>Documented information</td>
</tr>
</tbody>
</table>

## Do

<table>
<thead>
<tr>
<th>8. Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operational Planning &amp; control</td>
</tr>
<tr>
<td>Information security risk assessment</td>
</tr>
<tr>
<td>Information security risk treatment</td>
</tr>
</tbody>
</table>

## Check

<table>
<thead>
<tr>
<th>9. Performance evaluation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitoring measurement, analysis &amp; evaluation</td>
</tr>
<tr>
<td>Internal audit</td>
</tr>
<tr>
<td>Management review</td>
</tr>
</tbody>
</table>

## Act

<table>
<thead>
<tr>
<th>10. Improvement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non conformity &amp; corrective action</td>
</tr>
<tr>
<td>Continual improvement</td>
</tr>
</tbody>
</table>
Standard & Best Practices: ISO 27002


0 Foreword
1 Introduction
2 Scope
3 Normative references
4 Terms & definitions
5 Structure of this standard
6 Bibliography
7 Information Security policies
8 Asset management
9 Access control
10 Cryptography
11 Physical & environmental security
12 Operations security
13 Communications security
14 System acquisition, development and maintenance
15 Supplier relationships
16 Information security incident management
17 Information security aspects of business continuity management
18 Compliance
Standards & Best Practices: ISO 27005

- ISO 27005:2011
  - Security techniques -- Information Security Risk Management
  - Provides guidelines for structured risk analysis
  - Support family of ISO 27000 for information security management
Standards & Best Practices: ISO 27005

- Context Establishment
- Risk Assessment
  - Risk Analysis
    - Risk Identification
    - Risk Estimation
    - Risk Evaluation
- Risk Treatment
- Risk Acceptance

Risk Decision Point 1
- Assessment Satisfactory
- NO
- YES

Risk Decision Point 2
- Treatment Satisfactory
- NO
- YES
Standards & Best Practices: ISO 22301

ISO 22301:2012

- Business Continuity Management Systems – Requirements

- Specifies requirements to plan, establish, implement, operate, monitor, review, maintain and continually improve a documented management system to prepare for, respond to and recover from disruptive events when they arise
Standards & Best Practices: ISO 22301

ISO 22301: 2012 Business Continuity Management Systems

### Plan

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Understanding the organization and its context</td>
<td>Leadership &amp; commitment</td>
<td>Actions to address risks &amp; opportunities</td>
<td>Resources</td>
</tr>
<tr>
<td>Expectation of Interested parties</td>
<td>Policy</td>
<td>BC objectives and plans to Achieve them</td>
<td>Competence</td>
</tr>
<tr>
<td>Scope of BCMS</td>
<td>Organization roles, responsibilities &amp; authorities</td>
<td></td>
<td></td>
</tr>
<tr>
<td>BCMS</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Do

<table>
<thead>
<tr>
<th>8. Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operational planning &amp; control</td>
</tr>
<tr>
<td>Business impact analysis &amp; risk assessment</td>
</tr>
<tr>
<td>Business continuity strategy</td>
</tr>
<tr>
<td>Establish &amp; implement BC procedures</td>
</tr>
<tr>
<td>Exercising &amp; testing</td>
</tr>
</tbody>
</table>

### Check

<table>
<thead>
<tr>
<th>9. Performance evaluation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitoring measurement, analysis &amp; evaluation</td>
</tr>
<tr>
<td>Internal audit</td>
</tr>
<tr>
<td>Management review</td>
</tr>
</tbody>
</table>

### Act

<table>
<thead>
<tr>
<th>10. Improvement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non conformity &amp; corrective action</td>
</tr>
<tr>
<td>Continual improvement</td>
</tr>
</tbody>
</table>
Standards & Best Practices: PCI SSC

- Payment Card Industry Security Standards Council
Standards & Best Practices

- ISO 20000-1:2011
  - Information technology – Service management – Part 1: Service management system requirements
- ISO 38500: 2008
  - Corporate governance of information technology
- COBIT
  - Road Map to Good IT Governance by ISACA
- Open Web Application Security Project (OWASP)
  - https://www.owasp.org
- NIST: National Institute of Standards & Technology
  - Special Publication (800 Series)
- CIS: Center for Internet Security
  - http://www.cisecurity.org/resources-publications/
## Developing Enterprise Security Framework

- Relationship with Standards & Best Practices

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Realize Enterprise Security Needs</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Evaluate Existing Security Posture</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assess Enterprise Risks</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Define Process to Regulate Technology</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Implement a Security Management System</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

© All rights reserved INFOGISTIC - 2013
Developing Enterprise Security Framework

- Enterprise Security Framework
  - Gap Analysis against ISO 27001 and ISO 27002
  - Risk Management using ISO 27005
  - Vulnerability Assessment & Penetration Test
  - Security Competence & Awareness Program
  - Training on Process Documentation
  - Internal Compliance Audit

- Integrating Technology & Process
  - Security Operations Centre
  - Governance Risk and Compliance
Integrating Process & Technology

<table>
<thead>
<tr>
<th>Security Analytics</th>
<th>ISO 27001</th>
<th>ISO 27002</th>
<th>ISO 38500</th>
<th>ISO 22301</th>
<th>ISO 20000</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policies &amp; Awareness</td>
<td>Physical</td>
<td>Perimeter</td>
<td>Internal Network</td>
<td>Host</td>
<td>Application</td>
</tr>
<tr>
<td>GRC</td>
<td>BMS</td>
<td>NGIPS</td>
<td>NGFW</td>
<td>Host Based Protection</td>
<td>X factor Authentication</td>
</tr>
</tbody>
</table>

- Security Analytics:
  - Smart ID
  - Email Security
  - IAM
  - Malware Analysis
  - Vulnerability Scanning
  - Encryption

- ISO Standards:
  - ISO 27001
  - ISO 27002
  - ISO 38500
  - ISO 22301
  - ISO 20000

© All rights reserved INFOGISTIC - 2013
Case Study

www.infogistic.com
Forrester: Top Technology Trends for 2014 And Beyond – 25th Nov 2013

− now that consumers and employees have continuous connectivity and an endless supply of apps, the CIO must drive the nimbleness that will be demanded by employees and customers, while he or she must also do so securely

− 7. “Trust” and “identity” get a rethink
  • It’s impossible to identify ‘trusted’ interfaces, many data breeches comes from trusted insiders.
  • The minimum cost of a data breech is $10 million, and in many cases it can be much larger”, and so it cannot be ignored.
Saudi Oil firm says 30,000 computers hit by virus
What Aramco Means

USD $790 billion revenue

55,000+ employees

State of the Art Infrastructure

Largest Oil Producer on Planet!

World’s Most Valuable Company; twice the size of Apple Inc.

Market Value: Apple, USD 619 Bn VS Saudi Aramco, 1.245 Trillion
Way Forward

- Aramco Engaged Consulting Companies Across the Globe
  - To conduct a fact finding exercise
  - To review their existing security posture
  - To formulate a plan to improve security
    - Technology Initiatives
    - Process Initiatives
Enterprise Data Protection Framework

INFOGISTIC was entrusted to develop and implement Enterprise Data Protection Framework

- Assessment of Existing Security Management System
- Development of Data Protection Framework
  - Mapping of existing documentation against cyber security best practices
  - Development of Data Protection Program
  - Recommendations on Technology Controls
- Pilot Implementation
- Lead Implementer Training
- e-Learning Portal
- Program Compliance Audit
As the world is increasingly interconnected, everyone shares the responsibility of securing cyberspace!!

Newton Lee

Thank You