ISO 27001 Certification
Establish the ISMS
Information Security Management System
The organization **shall** do the following:
- Define the scope and boundaries of the ISMS
- Define an ISMS policy
- Define the risk assessment approach
- Identify the risks
- Analyze and evaluate the risks
- Identify and evaluate the options for the treatment of risks
The organization shall do the following:

- Select control objectives and controls for the treatment of risks
- Obtain management approval of the proposed residual risks
- Prepare a Statement of Applicability

So what are the control objectives and controls for the treatment of risks are?
They are the 1,033 “shoulds” contained within the ISO/IEC 27002 (formerly ISO 17799) standard.
Those 1,033 “shoulds” are contained within eleven (11) security clauses which comprise 39 main control objectives and 142 controls. There is also one (1) introductory clause which deals with risk assessment and treatment.

That being said how many control objectives and controls should be on your Statement of Applicability?
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Security Policy</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.1</td>
<td>Information Security Policy</td>
<td>Information security policy document</td>
<td>Y</td>
<td>IT web</td>
<td>Y</td>
<td>ISO</td>
<td>BOV</td>
<td>Jul-06</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Review of the information security policy</td>
<td>Y</td>
<td>NA</td>
<td>Y</td>
<td>ISO</td>
<td>CIO</td>
<td>May-08</td>
</tr>
<tr>
<td>6</td>
<td>Organization of Information Security</td>
<td>Internal organization</td>
<td>Y</td>
<td>Letter or statement from president</td>
<td>Y</td>
<td>President</td>
<td>NA</td>
<td>Jul-08</td>
</tr>
<tr>
<td>6.1</td>
<td></td>
<td>Management commitment to information security</td>
<td>Y</td>
<td>Organization of IS</td>
<td>Y</td>
<td>ISO</td>
<td>CIO</td>
<td>Jul-08</td>
</tr>
<tr>
<td>6.1.1</td>
<td></td>
<td>Information security coordination</td>
<td>Y</td>
<td>Organization of IS</td>
<td>Y</td>
<td>ISO</td>
<td>CIO</td>
<td>Jul-08</td>
</tr>
<tr>
<td>6.1.2</td>
<td></td>
<td>Allocation of information security responsibilities</td>
<td>Y</td>
<td>Organization of IS</td>
<td>Y</td>
<td>ISO</td>
<td>CIO</td>
<td>Jul-08</td>
</tr>
<tr>
<td>6.1.3</td>
<td></td>
<td>Authorization process for information processing facilities</td>
<td>Y</td>
<td>PM Methodology</td>
<td>Y</td>
<td>ISO</td>
<td>CIO</td>
<td>Jul-08</td>
</tr>
<tr>
<td>6.1.4</td>
<td></td>
<td>Confidentiality agreements</td>
<td>N</td>
<td>Membership certificates</td>
<td>Y</td>
<td>ISO</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>6.1.5</td>
<td>Contact with authorities</td>
<td>Contact with special interest groups</td>
<td>Y</td>
<td>APA Report</td>
<td>Y</td>
<td>APA</td>
<td>NA</td>
<td>Sep-07</td>
</tr>
<tr>
<td>6.1.6</td>
<td></td>
<td>Independent review of IS</td>
<td>Y</td>
<td>Membership certificates</td>
<td>Y</td>
<td>ISO</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>6.1.7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.1.8</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
At this point you have reached the end of what is referred to as Stage 1 and are ready for a Stage 1 or Phase 1 audit. Which basically is just a review of documentation.
Establish the Information Security Management System

- Information Security Policy
- Scope
- Risk Management
- Statement of Applicability
Standards to Assist in the Plan Phase

- ISO/IEC 27001
- ISO/IEC 27002
- FIPS PUB 199
- NIST SP800-60
- NIST SP800-30
- ISO TR 13335-3 and TR 13335-4:2000
- NIST SP800-18
- NIST SP800-53A
- ISO/IEC 27005
Implement and Operate the ISMS
Information Security Management System
The organization **shall** do the following:
- Formulate a risk treatment plan
- Implement the risk treatment plan
- Implement the controls selected in the Plan Phase
- Define effectiveness metrics
Implement and Operate the ISMS

- Implement security awareness training program
- Manage operation of the ISMS
- Manage resources for the ISMS
- Implement security incident detection and response
Implement and Operate the Information Security Management System

- Risk Treatment Plan
- Controls
- Effectiveness metrics
- Security Awareness Training
- Managed ISMS operations and resources
- Incident response
Standards to Assist in the Do Phase

- ISO/IEC 27001
- ISO/IEC 27002
- FIPS PUB 200
- NIST SP800-5
- NIST SP800-53
- ISO TR 13335-4:2000
Monitor and Review the ISMS
Information Security Management System
The organization shall do the following:
- Execute monitoring and reviewing procedures
- Undertake regular reviews of the effectiveness of the ISMS
- Measure the effectiveness of controls
- Review the risk assessments at planned intervals
- Conduct internal ISMS audits
- Undertake a management review of the ISMS on a regular basis
- Update security plans
- Record actions and events
Monitor and Review the Information Security Management System

- Risk Assessment Reviews
- Controls Reviews
- Effectiveness Reviews
- Documented Internal Audits
- Documented Management Reviews
- Documented Actions and Events
- Updated security plan
Standards to Assist in the Check Phase

- NIST SP800-61
- NIST SP800-37
- NIST SP800-53
- NIST SP800-26
Maintain and Improve the ISMS
Information Security Management System
The organization **shall** do the following:

- Implement the identified improvements in the ISMS
- Take appropriate corrective and preventive actions
- Communicate the actions and improvement to all interested parties
- Ensure that the improvements achieve their intended objectives
Maintain and Improve the Information Security Management System

- Improvement implementation plan
- Corrective Action Plan
- Preventive Action Plan
- Communication Plan
- Implemented improvements review plan
Standards to Assist in the Act Phase

- ISO/IEC 27001
- ISO/IEC 27002
- NIST SP800-37
- ISO 19011:2000
How many documented procedures are actually required by the ISO 27001 standard?
1. A documented procedure shall be established to define the management actions needed to provide for control of documents.

2. The responsibilities and requirements for planning and conducting audits, and for reporting results and maintaining records shall be defined in a documented procedure.

3. The documented procedure for corrective action shall define requirements for:

4. The documented procedure for preventive action shall define requirements for:
ISO 27001 Certification
Step 1 – Agency/Institution makes the decision to obtain ISO 27001 certification

Step 2 – Management makes commitment, assigns responsibilities and allocates resources (I’ll go over this in more detail in a couple of slides)

Step 3 – Define Information Security Policy

Step 4 – Define the scope of the Information Security Management System
Step 5 – Perform Risk Assessment for the scope of the ISMS
Step 6 – Decide how to manage identified risks
Step 7 – Select control objectives and controls to be implemented
Step 8 – Prepare Statement of Applicability
Step 9 – Implement the controls (more on this later)

Step 10 – Identify a Certifier

- An organization accredited by UKAS (United Kingdom Accreditation Service) and ANAB (ANSI-ASQ National Accreditation Board)
  - [http://www.anab.org/](http://www.anab.org/)
  - ANAB has only certified one company in the US and that is BSI-America.
  - [http://www.bsiamerica.com/](http://www.bsiamerica.com/)
Step 11 – Apply to certifier
  - Organization statement (who am I)
  - ISMS Scope Statement
  - Statement of Applicability

Step 12 – Phase I audit (Desktop review of documentation)

Step 13 – Resolution of any identified findings – normally a 6 to 8 week gap
Step 14 – Phase II audit – full on-site to determine:
- ISMS implemented and operated
- ISMS monitored and reviewed
- ISMS maintained and improved

Step 15 – Recommendation for certification or conditional recommendation or rejection
Let’s go back and look at Step 2 in a little more detail.

**Step 2 – Management makes commitment, assigns responsibilities and allocates resources**

Management shall provide evidence of its commitment to the establishment, implementation, operation, monitoring, review, maintenance and improvement of the ISMS by:
Step 2 – Management makes commitment, assigns responsibilities and allocates resources

- Establishing an ISMS policy;
- Ensuring that ISMS objectives and plans are established;
- Establishing roles and responsibilities for information security;
- Communicating to the organization the importance of meeting information security objectives and conforming to the information security policy, its responsibilities under the law and the need for continual improvement;
Step 2 – Management makes commitment, assigns responsibilities and allocates resources

- Providing sufficient resources to establish, implement, operate, monitor, review, maintain and improve the ISMS;
- Deciding the criteria for accepting risks and the acceptable levels of risk;
- Ensuring that internal ISMS audits are conducted; and
- Conducting management reviews of the ISMS.
Of the 39 control objectives and the 142 controls, the agency/institution has to provide evidence that each control has been implemented, reviewed (think audited), measured for effectiveness, reviewed by management, and all these reviews have to be documented.
The key is management commitment
This is a long-term project, even if you think you have an ISMS already in place
This is a resource intensive project with a lot of documentation, meetings, and staff commitment
Say What You Do
Do it
Prove That You Did It
- J. Kenneth Magee
- Phone: (804) 225-3350 Ext 663
- Fax: (804) 225-3357
- kenneth.magee@apa.virginia.gov
QUESTIONS