Jump Start Your Security Program

Kathy Washenberger, CIO, FocusPoint Technologies
Purpose

1. Understand Your Business Risk Drivers

2. Use 3 L’s
   - Learn
   - Listen
   - Lead

3. Avoid Analysis Paralysis
Many Reasons
Involve the Business

Find Security Champions
$ Business Line Budgets
$ Project or Initiative Budgets
$ Legal/Compliance Drivers
$ Capital Budget
$ Technology Consolidation
<table>
<thead>
<tr>
<th>ISMS family of standards</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1 General information</td>
</tr>
<tr>
<td>5.2 Standard describing an overview and terminology: ISO/IEC 27000 (this document).</td>
</tr>
<tr>
<td>5.3 Standards specifying requirements</td>
</tr>
<tr>
<td>5.3.1 ISO/IEC 27001</td>
</tr>
<tr>
<td>5.3.2 ISO/IEC 27006</td>
</tr>
<tr>
<td>5.3.3 ISO/IEC 27009</td>
</tr>
<tr>
<td>5.4 Standards describing general guidelines</td>
</tr>
<tr>
<td>5.4.1 ISO/IEC 27002</td>
</tr>
<tr>
<td>5.4.2 ISO/IEC 27003</td>
</tr>
<tr>
<td>5.4.3 ISO/IEC 27004</td>
</tr>
<tr>
<td>5.4.4 ISO/IEC 27005</td>
</tr>
<tr>
<td>5.4.5 ISO/IEC 27007</td>
</tr>
<tr>
<td>5.4.6 ISO/IEC TR 27008</td>
</tr>
<tr>
<td>5.4.7 ISO/IEC 27013</td>
</tr>
<tr>
<td>5.4.8 ISO/IEC 27014</td>
</tr>
<tr>
<td>5.4.9 ISO/IEC TR 27016</td>
</tr>
<tr>
<td>5.4.10 ISO/IEC 27021</td>
</tr>
<tr>
<td>5.5 Standards describing sector-specific guidelines</td>
</tr>
<tr>
<td>5.5.1 ISO/IEC 27010</td>
</tr>
<tr>
<td>5.5.2 ISO/IEC 27011</td>
</tr>
<tr>
<td>5.5.3 ISO/IEC 27017</td>
</tr>
<tr>
<td>5.5.4 ISO/IEC 27018</td>
</tr>
<tr>
<td>5.5.5 ISO/IEC 27019</td>
</tr>
<tr>
<td>5.5.6 ISO 27799</td>
</tr>
</tbody>
</table>
Holistic Strategy/Process

Program Objectives

- Leadership
- Strategy/Charter/Policy
- Org Structure/Skills
- Awareness/Brand
- Risk Management
- Metrics

- Regulatory Compliance
  - Business Continuity
    - Vendor Management
  - Security Audit
    - Security Reviews
    - Privacy

- Identity/Access
  - Forensics
  - Event Management
  - Vulnerability Mgmt
  - Prevention/Detection
  - Incident Response/Testing

- Backup/Recovery
- Asset/Config Mgmt
- Network/Endpoint
- Application/Cloud
- Physical
- Mobile

Governance

Compliance

Technology/Environment

Operations
Maturity

Minimal

Foundational

Defined

Managed

Optimized
Understand and Involve the Business

Identify the “Crown Jewels”

Assess, Understand Gaps, Prioritize
Things to Avoid

1. Don’t Over-Commit
2. Don’t Use FUD
3. Don’t Focus Only on Tools
Remember...

Find and Use Business Champions

Start Small but Scale Fast

Build on Successes