IT Risk
Week 11
ISACA’s Risk IT Framework
ISACA’s Risk IT Framework

1. What is IT Risk?
2. What are the three types of IT Risk?
3. What are the three risk processes that an enterprise ought to have?
4. What is risk appetite?
5. What is risk tolerance?
6. What are the three parts of a risk culture?
Risk Evaluation

• What are some ways you might express IT risk in business terms?
  – COBIT
  – COSO ERM

• What is a risk scenario?

• What is a risk factor?

• What are the four types of risk response and when would you use them?
ISACA’s Risk IT Framework

• Part of Enterprise Risk Management
• Look at the breadth of IT risk, not just cyber-security
• Should align to business strategy

• Risk IT Framework
  – Risk Governance
    How much risk can you stand?
  – Risk Evaluation
    What risks do you actually face?
  – Risk Response
    How can you make these risks acceptable?
How much risk can you stand?

<table>
<thead>
<tr>
<th>12. Has your board of directors considered IT risks?</th>
<th>Response Percent</th>
<th>Response Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>39.3%</td>
<td>11</td>
</tr>
<tr>
<td>No</td>
<td>60.7%</td>
<td>17</td>
</tr>
</tbody>
</table>
What risks do you actually face?

9. Have you had a cyber-security risk assessment performed?

<table>
<thead>
<tr>
<th>Response</th>
<th>Response Percent</th>
<th>Response Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>28.6%</td>
<td>8</td>
</tr>
<tr>
<td>No</td>
<td>71.4%</td>
<td>20</td>
</tr>
</tbody>
</table>

answered question: 28
skipped question: 0
How can you make these risks acceptable?

- Accept it
- Avoid it
- Share or Transfer it
- MiDgate it with controls

Make it less likely

Make it less impactful
Two views of cyber-security controls

<table>
<thead>
<tr>
<th>ISACA</th>
<th>SANS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preventive</td>
<td>Getting In</td>
</tr>
<tr>
<td>Detective</td>
<td>Staying In</td>
</tr>
<tr>
<td>Corrective</td>
<td>Acting</td>
</tr>
</tbody>
</table>

**Table of Contents**

- Twenty Critical Security Controls for Effective Cyber Defense: Common Audit Guidelines (CAG)  
  - Version 1.1 October 2, 2017  
  - Introduction  
    - Overview  
    - Potential Areas for Improvement  
- The 10 Critical Controls  
  - Identify and Manage Assets  
    - Identify and Manage Assets  
  - Protect Assets  
    - Protect Assets  
  - Detect Events that Compromise Assets  
    - Detect Events that Compromise Assets  
  - Respond to Incidents  
    - Respond to Incidents  
  - Recover from Incidents  
    - Recover from Incidents  

---

**Introduction**

Focusing attention on effective controls to meet the increasing complexity of threats to information assets is critical for organizations of all sizes. This guide provides a framework for organizations to assess and develop a comprehensive approach to security controls. The guide includes 10 critical controls, each with specific guidelines and examples to help organizations improve their cyber defense posture.
SANS Control # 3:
Secure Configurations of HW & SW

– Utah Department of Health – 701,000 records
  • Policy to delete information not followed
  • Old configuration gave hacker access

– St. Joseph’s Health System - 32,000 records
  • “…security settings incorrect.”

– SANs quick wins: Standard, hardened builds, preferably put on by vendors, no variations unless specifically approved
SANS Control # 3: Controlled Access Based on Need to Know

• Memorial Healthcare System – 10,000 records
  – Two employees “...improper access”
  – Intended to file fraudulent tax returns

• South Carolina Department of Health – 228,000 records
  – Employee moved 17 spreadsheets by email

• SANS quick wins: multi-level data classification with access allowed to minimally acceptable authorized users
## SANS Control # 17: Data Loss Prevention Data-at-rest

### 11. Do all desktops and laptops use data encryption by default?

<table>
<thead>
<tr>
<th>Response</th>
<th>Percent</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>28.6%</td>
<td>8</td>
</tr>
<tr>
<td>No</td>
<td>71.4%</td>
<td>20</td>
</tr>
</tbody>
</table>

- **answered question**: 28
- **skipped question**: 0

---

- **SANS quick win**: deploy hard drive encryption
SANS Control # 17: Data Loss Prevention Data-in-motion

- South Carolina Department of Health – 228,000 records
  - Employee moved 17 spreadsheets by email

- CA In-home support Services – 701,000 records
  - Unencrypted microfiche lost on way to insurance company

- SANS: Monitor outbound transactions for anomalies, move data using secure, authenticated, encrypted mechanisms
The All World Airlines Case

• Take 45 minutes
• Your team has been requested to compile a list of risks for each of five areas identified by the CFO for the risk assessment.
  – Group your thoughts by section, using the details that Don has provided, your understanding of the COBIT risk management issues and your understanding of IT issues.
  – How would you perform a risk assessment of the risks identified in question 1 to provide an objective and subjective assessment for management’s consideration?
  – Identify what role the retained organization should have in its interactions with the vendor for the outsourced IT function.