Assessing Security of Protected Health Information for Information Systems

**Purpose:**
to reveal unaccounted for vulnerabilities in information systems and assure the protection of protected health information

**Data Breaches:**
- University of North Carolina at Chapel Hill
  - 100,000 women affected
- Presbyterian Anesthesiology Associates
  - 10,000 patients affected

---

**NIST 800-30:**

**Input:**
- Hardware
- Software
- System interfaces
- Data and information
- People
- System mission
- History of system attack
- Data from intelligence agencies, NIPC, OIG, FedCIV, mass media
- Reports from prior risk assessments
- Any audit comments
- Security requirements
- Security test results
- Current controls
- Planned controls
- Threat-source motivation
- Threat capacity
- Nature of vulnerability
- Current controls
- Mission impact analysis
- Asset critically assessment
- Data critically
- Data sensitivity
- Likelihood of threat exploitation
- Magnitude of impact
- Adequacy of planned or current controls

**Output:**
- System Boundary
- System Functions
- System and Data Criticality
- System and Data Sensitivity
- Threat Statement
- List of Potential Vulnerabilities
- List of Current and Planned Controls
- Likelihood Rating
- Impact Rating
- Risks and Associated Risk Levels
- Recommended Controls
- Risk Assessment Report

**Risk Assessment Methodology Flowchart**

---

**Results:**

<table>
<thead>
<tr>
<th>Categories</th>
<th>Critical Elements</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Risk Management</td>
<td>0.2</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Review of Security Controls</td>
<td>0.2</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Life Cycle</td>
<td>0.512</td>
<td>0.615</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. Authorize Processing</td>
<td>0.375</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. System Security Plan</td>
<td>1</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TOTAL</td>
<td>0.431</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6. Personnel Security</td>
<td>0.857</td>
<td>0.957</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8. Production, Input/Output Controls</td>
<td>1</td>
<td>0.957</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9. Contingency Planning</td>
<td>1</td>
<td>0.6</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>10. Hardware and System Software Maintenance</td>
<td>1</td>
<td>0.846</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>11. Data Integrity</td>
<td>0</td>
<td>0.375</td>
<td></td>
<td></td>
</tr>
<tr>
<td>12. Documentation</td>
<td>0.625</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>13. Security Awareness, Training, and Education</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14. Incident Response Capability</td>
<td>1</td>
<td>0.333</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TOTAL</td>
<td>0.664</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15. Identification and Authentication</td>
<td>0.769</td>
<td>0.769</td>
<td>0.769</td>
<td></td>
</tr>
<tr>
<td>16. Logical Access Controls</td>
<td>0.7</td>
<td>0.7</td>
<td>0.7</td>
<td></td>
</tr>
<tr>
<td>17. Audit Trails</td>
<td>0.667</td>
<td>0.667</td>
<td>0.667</td>
<td></td>
</tr>
<tr>
<td>TOTAL</td>
<td>0.856</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Overall Total</td>
<td>0.600</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

This material is based upon work supported by the National Science Foundation under grant #1062970. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.