Service Organization Control (SOC 2)

Changes to Criteria for the Trust Services Principles (TSP)
SOC 2: Revised TSP

- Background on TSP
- Why the Change
- What Changed
- Restructured TSP
- Risk Assessment
- Impact of Changes
- Next Steps
- Questions
Background on TSP

Five attributes of a system known as principles:

- **Security** - The system is protected against unauthorized access (both physical and logical)
- **Availability** - The system is available for operation and use as committed or agreed
- **Processing integrity** - System processing is complete, accurate, timely, and authorized
Background on TSP

- Confidentiality - Information designated as confidential is protected as committed or agreed.
- Privacy - Personal information is collected, used, retained, disclosed, and destroyed in conformity with the commitments in the entity’s privacy notice and with criteria set forth in GAPP.
Why the Change

• Redundancy of criteria in each principle
  – Repeat list of controls tested based on criteria applicable for each principle

• Appearance of a lack of clarity for the reader and users of report

• Streamline Reporting of Controls
What Changed

Restructuring of TSP

• Defined New Control Categories
• Established set of Common Criteria applicable to all TSP’s (evaluated within Security TSP)
• Generally Accepted Privacy Principles (GAPP) revised separately

Risk Assessment

• Documented risk assessments
• Additional guidance to link criteria, specific risks to criteria, and the corresponding control
## Restructured TSP

### Prior Control Categories for Each Principle
- Policies
- Communication
- Procedures
- Monitoring

### New Control Categories within Common Criteria
- Organization & Management
- Communication
- Risk Management & Design & Implementation of Controls
- Logical & Physical Access
- System Operations
- Change Management
- Monitoring of Controls

## Restructured TSP

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Security</th>
<th>Availability</th>
<th>Processing Integrity</th>
<th>Confidentiality</th>
<th>Privacy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common Criteria</td>
<td>28 Common Criteria within seven new categories</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.</td>
<td>Organization and management</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td>Communications</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td>Risk Management &amp; Design &amp; Implementation of Controls</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.</td>
<td>Monitoring of Controls</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.</td>
<td>Logical and Physical Access Controls</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.</td>
<td>System Operations</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7.</td>
<td>Change management</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Previously there were four categories:
- Policies
- Communication
- Procedure
- Monitoring

### Additional Criteria

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Security</th>
<th>Availability</th>
<th>Processing Integrity</th>
<th>Confidentiality</th>
<th>Privacy</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>3</td>
<td>6</td>
<td>6</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>
New Risk Management Category

- Requires a more formalized Risk Assessment
- Evaluation of controls mitigating the risks

Risk Assessment

- Risk assessment should include:
  - Risks/Threats
  - Controls that mitigate risks (mapping)
  - Ownership of controls
  - Management’s evaluation of controls

*Waiting on AICPA Guidance for more details
Impact of Changes

Restructuring of TSP

- Eliminates redundancy of the controls
- Provides clarity for the users and readers of report

Risk Assessment

- Requires formal identification of risks and threats
- Management’s ownership and evaluation of controls mitigating the risks
Impact of Changes

Reporting of revised SOC 2 TSP’s

- Effective for periods ending on or after December 15, 2014
- Early adoption permitted. A-lign to officially start issuing after July 1, 2014, depending on client circumstances.
Next Steps

- Auditors to assist service organizations transition to the new criteria
  - Help clients to understand differences in reporting
  - Provide guidance on nature and effort of risk assessment
- Mapping the control activities between the old and new criteria
- Revised TSP to be adopted for the those service organization implementing SOC 2 reporting for first time
A-align – Contact Information

Neil Gonsalves
Director
www.a-lign.com
neil.gonsalves@a-lign.com
Tel. 1-888-702-5446 ext. 104
Questions