December 11, 2013

Modifications to the AICPA’s Trust Principles Framework and the Impact to Service Organization Control Reporting
Trust Principles Framework?

• What:
  – The Trust Principles Framework is for use by practitioners when evaluating controls relevant to the security, availability, and processing integrity of a system, and the confidentiality and privacy of the information processed by the system.
  
  – The Framework is used for SOC 2 and 3 attestation engagements, as well as other consulting engagements.
SOC 2 & 3 Audits and the Trust Principles Framework

• SOC 2 and 3 audits cover a specific scope of services and is performed against one or several of the Principles outlined in the Trust Principles Framework

  – **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.
  – **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 generally accepted privacy principles issued by the AICPA and CICA.
Why is it changing and when?

• Why:
  – Address concerns over the length and complexity of certain trust services reports,
  – Increase the clarity of the criteria,
  – Eliminate redundancy amongst the criteria,
  – Update the criteria based on the changing technology and business environment
  – Example:
    Security 1.1: “The entity’s security policies are established and periodically reviewed and approved by a designated individual or group”
    Availability 1.1: “The entity’s system availability and related security policies are established and periodically reviewed and approved by a designated individual or group.”

• When:
  – The trust services principles and criteria are effective for periods ending on or after March 15, 2014
Why should I care?

• Do you know the difference between SSAE 16, SOC 1, SOC 2 and SOC 3
• Do you know what you get from your service organizations and is it correct?

• You should care if:
  1. Your organization has an SOC 2 or SOC 3 audit performed by a practitioner.
  2. You have a vendor management program and review the SOC 2 and 3 reports of third-party vendors that provide services to your company
Summary of changes?

• **Restructuring of the trust services principles and criteria**
  
  – Criteria for security, availability, processing integrity, and confidentiality are consolidated to account for commonalities applicable to all four principles (common criteria), with criteria applicable only to a single principle separately identified
  
  – **Result:** More concise SOC 2 reports that avoid the repetition from the current framework

• **Risk assessment**
  
  – The AICPA documented risks that they’ve identified as illustrative examples that may prevent the criteria from being met as well as examples of controls that would address those risks
  
  – **Result:** Increased clarity as to the true intent / spirit of a criteria

• **Practitioner guidance**
  
  – Practitioner guidance on scoping and reporting issues – TBD
  
  – **Result:** TBD – more consistent application by practitioners?

• **Common Criteria Categories**
  
  – The new common criteria are aligned following the components of the COSO framework – 7 categories. Current framework only has 4 categories
The New Trust Criteria

• Existing framework included almost 120 controls covering Security, Availability, Processing Integrity and Confidentiality
• Roughly 26 controls within each Principle had some overlap with another Principle
  – Result:
    • Practitioners issuing SOC 2 reports that were hundreds of pages with redundant information.
    • Exceptions noted for one Criteria could be reported 4 different times in the same report.

• Revised framework consolidates the commonalities into:
  – 28 distinct, common criteria (excluding Privacy)
  – 3 criteria specific to Availability
  – 6 criteria specific to Processing Integrity
  – 6 criteria specific to Confidentiality
Common Criteria

• New categorization for Common Criteria:
  
  – *Organization and management*. The criteria relevant to how the organization is structured and the processes the organization has implemented to manage and support people within its operating units. This includes criteria addressing accountability, integrity, ethical values and qualifications of personnel, and the environment in which they function.
  
  – *Communications*. The criteria relevant to how the organization communicates its policies, processes, procedures, commitments, and requirements to authorized users and other parties of the system and the obligations of those parties and users to the effective operation of the system.
  
  – *Risk management and design and implementation of controls*. The criteria relevant to how the entity (i) identifies potential risks that would affect the entity’s ability to achieve its objectives, (ii) analyzes those risks, (iii) develops responses to those risks including the design and implementation of controls and other risk mitigating actions, and (iv) conducts ongoing monitoring of risks and the risk management process.
Common Criteria

- **Monitoring of controls.** The criteria relevant to how the entity monitors the system, including the suitability, and design and operating effectiveness of the controls, and takes action to address deficiencies identified.

- **Logical and physical access controls.** The criteria relevant to how the organization restricts logical and physical access to the system, provides and removes that access, and prevents unauthorized access to meet the criteria for the principle(s) addressed in the engagement.

- **System operations.** The criteria relevant to how the organization manages the execution of system procedures and detects and mitigates processing deviations, including logical and physical security deviations, to meet the objective(s) of the principle(s) addressed in the engagement.

- **Change management.** The criteria relevant to how the organization identifies the need for changes to the system, makes the changes following a controlled change management process, and prevents unauthorized changes from being made to meet the criteria for the principle(s) addressed in the engagement.
Common Criteria

Most of the Common Criteria closely relate to the existing Trust Principle criteria and were modified for clarity:

<table>
<thead>
<tr>
<th>New CC #</th>
<th>Common Criteria</th>
<th>Old #</th>
<th>Current Trust Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>CC1.2</td>
<td>Responsibility and accountability for designing, developing, implementing, operating, monitoring, maintaining, and approving the entity’s system controls are assigned to individuals within the entity with authority to ensure policies and other system requirements are effectively promulgated.</td>
<td>S 1.1</td>
<td>Responsibility and accountability for developing and maintaining the entity’s system [security, availability, processing integrity, confidentiality] policies, and changes and updates to those policies, are assigned.</td>
</tr>
<tr>
<td></td>
<td>The entity communicates the responsibilities of internal and external users and others whose roles affect system operation.</td>
<td>A 1.1</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>C 1.1</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>PI 1.1</td>
<td></td>
</tr>
<tr>
<td>CC2.3</td>
<td>Responsibility and accountability for the entity’s system [security, availability, confidentiality, and processing integrity] policies and changes and updates to those policies are communicated to entity personnel responsible for implementing them.</td>
<td>S 2.2</td>
<td>Responsibility and accountability for developing and maintaining the entity’s system [security, availability, processing integrity] obligations of users and the entity’s security commitments to users are communicated to authorized users.</td>
</tr>
<tr>
<td></td>
<td>The [security, availability, and processing integrity] obligations of users and the entity’s security commitments to users are communicated to authorized users.</td>
<td>A 2.2</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>PI 2.2</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>S 2.3</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>A 2.3</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>C 2.3</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>PI 2.3</td>
<td></td>
</tr>
</tbody>
</table>

However, the new framework appears to include 7 criteria that don’t closely relate to any existing framework requirements.
New Criteria

• CC 1.1 - The entity has defined organizational structures, reporting lines, authorities, and responsibilities for the design, development, implementation, operation, monitoring, and maintenance of the system enabling it to meet its commitments and requirements as they relate to [insert the principle(s) being reported on; for example, security, availability, processing integrity, and confidentiality].
  — Added attention on the organizational structure as a result of the large effect of governance in operations

• CC 2.4 - Internal and external personnel with responsibility for designing, developing, implementing, operating, monitoring, and maintaining controls, relevant to the [insert the principle(s) being reported on; for example, security, availability, processing integrity, and confidentiality] of the system, have the information necessary to carry out those responsibilities.
  — Focus on information availability to those with responsibility for controls over the system
New Criteria

• CC 6.1 - Vulnerabilities of system components to [insert the principle(s) being reported on; for example, security, availability, processing integrity, and confidentiality] breaches and incidents due to malicious acts, natural disasters, or errors are monitored and evaluated and countermeasures are implemented to compensate for known and new vulnerabilities.
  — Requirement for active monitoring of existing and new vulnerabilities that may disrupt system security, availability, etc.

• CC 7.3 - Change management processes are initiated when deficiencies in the design or operating effectiveness of controls are identified during system operation and monitoring.
  — Appropriate administration of issues related to the design and operation of controls
New Criteria

• PI 1.1 - Procedures exist to prevent, detect, and correct processing errors to meet processing integrity commitments and requirements.
  – Emphasis on systemic checks for error prevention, detection and correction during processing routines

• PI 1.4 - Data is stored and maintained completely and accurately for its specified life span in accordance with processing integrity commitments and requirements.
  – Data retention specifically was not a focus within PI and was more or less subjective to any described controls within the criteria related to data backup

• PI 1.6 - Modification of data is authorized, using authorized procedures in accordance with processing integrity commitments and requirements.
  – No prior criteria focused on the modification of data outside of normal system processing routines / operations
## AICPA Provided Illustrative Risks and Controls

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Risks</th>
<th>Illustrative Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>CC6.1</td>
<td>Vulnerabilities of system components to [insert the principle(s) being reported on; for example, security, availability, processing integrity, and confidentiality] breaches and incidents due to malicious acts, natural disasters, or errors are monitored and evaluated and countermeasures are implemented to compensate for known and new vulnerabilities.</td>
<td>Logging and monitoring software is used to collect data from system infrastructure components and endpoint systems and used to monitor system performance, potential security threats and vulnerabilities, resource utilization, and to detect unusual system activity or service requests. This software sends a message to the operations center and security organization and automatically opens a priority incident or problem ticket and change management system record item.</td>
</tr>
<tr>
<td></td>
<td>Vulnerabilities that could lead to a breach or incident are not detected in a timely manner.</td>
<td>Call center personnel receive telephone and e-mail requests for support, which may include requests to reset user passwords or notify entity personnel of potential breaches and incidents. Call center personnel follow defined protocols for recording, resolving, and escalating received requests.</td>
</tr>
</tbody>
</table>
What about Privacy?

- The privacy principle addresses the system’s collection, use, retention, disclosure, and disposal of personal information.

- Privacy does not follow the Trust Principles – instead uses GAPP (Generally Accepted Privacy Principles).

- 10 Principles

<table>
<thead>
<tr>
<th>PRIVACY PRACTICE</th>
<th>IF</th>
<th>THEN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management</td>
<td>If you don’t effectively manage your privacy program,</td>
<td>… your customers will take their business elsewhere.</td>
</tr>
<tr>
<td>Notice</td>
<td>If you do not provide your customer with your privacy notice,</td>
<td>… you may be in violation of GLBA.</td>
</tr>
<tr>
<td>Choice and Consent</td>
<td>If you do not provide your customer with the ability to control when you collect, use and disclose their personal information,</td>
<td>… you may damage customer relations.</td>
</tr>
<tr>
<td>Collections</td>
<td>If you collect more personal information than necessary,</td>
<td>… you may create a greater exposure for abuse of that information.</td>
</tr>
<tr>
<td>Use, Retention and Disposal</td>
<td>If you use the personal information for purposes other than specified,</td>
<td>… you may lose customer trust.</td>
</tr>
<tr>
<td>Access</td>
<td>If you don’t give your customers access to their personal information,</td>
<td>… you run the risk of not having accurate customer data.</td>
</tr>
<tr>
<td>Disclosure to Third Parties</td>
<td>If your third-party processor uses the personal information of your customers for purposes other than specified in your contract,</td>
<td>… your customer will still hold you accountable for improper use of that information.</td>
</tr>
<tr>
<td>Security for Privacy</td>
<td>If you don’t protect your customer’s personal information,</td>
<td>… you run the risk of a significant security breach.</td>
</tr>
<tr>
<td>Quality</td>
<td>If you don’t maintain accurate customer data,</td>
<td>… your targeted marketing and sales may suffer.</td>
</tr>
<tr>
<td>Monitoring and Enforcement</td>
<td>If you don’t effectively monitor your privacy practices,</td>
<td>… you may be subject to fines and penalties.</td>
</tr>
</tbody>
</table>
Where can I find more information on this stuff?

• AICPA Exposure Draft:

• Generally Accepted Privacy Principles
  – [http://www.aicpa.org/INTERESTAREAS/INFORMATIONTECHNOLOGY/RESOURCES/PRIVACY/GENERALLYACCEPTEDPRIVACYPRINCIPLES/Pages/default.aspx](http://www.aicpa.org/INTERESTAREAS/INFORMATIONTECHNOLOGY/RESOURCES/PRIVACY/GENERALLYACCEPTEDPRIVACYPRINCIPLES/Pages/default.aspx)