Agenda

- Types of Reports
- SOC 1 - 2 - 3 Comparison
- Further information on SOC 2 and SOC 3 Reports
- SOC 2 / SOC 3 Trust Principles defined by AICPA
- SOC 2 / SOC 3 reporting benefits
- Example Report
Types of Reports

- **SOC 1 Report (ISAE 3402)**
  Controls at a service organization relevant to user entities internal control over financial reporting

- **SOC 2 Report**
  Controls at a service organization which cover the criteria of the AICPA Trust Principles Security, Availability, Processing Integrity, Confidentiality or Privacy

- **SOC 3 Report**
  “Summary” of a SOC 2 report, but report can be published in the web
# SOC 1 - 2 - 3 Comparison

<table>
<thead>
<tr>
<th>Report type</th>
<th>Intended users</th>
<th>Format</th>
<th>Distribution limitations</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>SOC 1</td>
<td>Customers financial statement auditors</td>
<td>Long -form report&lt;br&gt;Description of controls and systems&lt;br&gt;Tests performed and results of testing</td>
<td>Restricted to current customers</td>
<td>Payroll processing&lt;br&gt;Credit card transaction processing</td>
</tr>
<tr>
<td>SOC 2</td>
<td>Users seeking assurance over information handling</td>
<td>“SOC1 look-alike report”:&lt;br&gt;- Long -form report&lt;br&gt;- Description of controls /systems&lt;br&gt;- Tests performed &amp; results&lt;br&gt;- Scope relates to “information handling objectives “ (security, availability, processing integrity, confidentiality and/or privacy )&lt;br&gt;- Organization reports controls in place to meet prescribed principles/criteria</td>
<td>Restricted to users with “sufficient knowledge”&lt;br&gt;e.g., current and prospective customers, business partners, regulators, employees</td>
<td>Supply chain information handler reporting on processing integrity&lt;br&gt;Data center outsourcer reporting on security and availability&lt;br&gt;Organization’s alignment with ISO 27001 or Cloud Security Alliance framework</td>
</tr>
<tr>
<td>SOC 3</td>
<td>Same as SOC 2</td>
<td>Short-form report&lt;br&gt;Limited description of controls/systems</td>
<td>No restrictions&lt;br&gt;e.g., mass distribution, web-site, current &amp; prospective customers</td>
<td>Bank reporting on privacy over e-banking application</td>
</tr>
</tbody>
</table>
Further information on SOC 2 and SOC 3 Reports

**SOC 2 Report**
- Subject matter: Controls at a service organization which cover the criteria of the AICPA Trust Principles:
  - Security
  - Availability
  - Processing Integrity
  - Confidentiality
  - Privacy
  - One or more Trust principles can be chosen for a SOC 2 Report
- Purpose of the report: To provide management of a service organization, user entities and other specified parties with information and an auditor’s opinion about controls at the service organization that may affect user entities’ security, availability, processing integrity, confidentiality or privacy.
- Type 1 (point in time: Controls placed in operation) and Type 2 Report (for a period of min. 6 months: Controls placed in operation and tests of operating effectiveness)

**SOC 3 Report**
- “Summary” of a SOC 2 report, but report can be published in the web
- Purpose of the report: To provide interested parties with an auditor’s opinion about controls at the service organization that may affect user entities’ security, availability, processing integrity, confidentiality, or privacy.
- Only Type 2 Reports available
### SOC 2 / SOC 3 Trust Principles defined by AICPA

<table>
<thead>
<tr>
<th>Trust Principle</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Security</strong></td>
<td>The system is protected against unauthorized access (both physical and logical).</td>
</tr>
<tr>
<td></td>
<td>- refers to the protection of the system resources through logical and physical access controls</td>
</tr>
<tr>
<td><strong>Availability</strong></td>
<td>The system is available for operation and use as committed or agreed.</td>
</tr>
<tr>
<td></td>
<td>- refers to the accessibility of the system, products, or services as committed by contract, service-level agreement, or other agreements</td>
</tr>
<tr>
<td><strong>Processing Integrity</strong></td>
<td>System processing is complete, accurate, timely, and authorized.</td>
</tr>
<tr>
<td></td>
<td>- refers to the completeness, validity, accuracy, timeliness, and authorization of system processing</td>
</tr>
<tr>
<td><strong>Confidentiality</strong></td>
<td>Information designated as confidential is protected as committed or agreed.</td>
</tr>
<tr>
<td></td>
<td>- addresses the system’s ability to protect information designated as confidential in accordance with the organization’s commitments and requirements through its final disposition and removal from the system</td>
</tr>
<tr>
<td><strong>Privacy</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>
SOC 2 / SOC 3 reporting benefits

► **Build competitive advantage** - An early adopter can use the SOC 2 and SOC 3 reports as a market differentiator.

► **Assist clients with vendor oversight activities** - New and emerging regulations establish vendor management requirements; a SOC 2 and SOC 3 report will assist client management with monitoring the services provided by outsourced third-parties.

► **Enhance client communications** - A well described system in a SOC 2 and SOC 3 report can increase transparency to clients and enhance their understanding of outsourced internal controls.

► **Manage client support costs** - A SOC 2 and SOC 3 report can be used to reduce client audits, due diligence/ vendor risk questionnaires and on-site visits, while providing an added level of assurance.

► **Satisfy contractual agreements** - New clients may request a SOC 2 and SOC 3 report as part of their contract; existing clients may amend their contracts.

► **Improve/lean your processes** - SOC 2 and SOC 3 assessment activities generate process improvement ideas and opportunities to further centralize and standardize processes and controls.
Common Criteria of Trust Principles

► CC 1.0 related to Organization and Management
► CC 2.0 related to Communications
► CC 3.0 related to Risk Management and Design and Implementation of Controls
► CC 4.0 related to Monitoring of Controls
► CC 5.0 related to Logical and Physical Access Controls
► CC 6.0 related to System Operations
► CC 7.0 related to Change Management

► additional Criteria for Availability
► additional Criteria for Processing Integrity
► additional Criteria for Confidentiality
Example Report

- Illustrative **Type 2 SOC 2 Report** with the Criteria in the Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM)

- Cloud Control Matrix Domains:

  - AIS  Application & Interface Security
  - AAC  Audit Assurance & Compliance
  - BCR  Business Continuity Mgmt & Op Resilience
  - CCC  Change Control & Configuration Management
  - DSI  Data Security & Information Lifecycle Mgmt
  - DSC  Datacenter Security
  - EKM  Encryption & Key Management
  - GRM  Governance & Risk Management
  - HRS  Human Resources Security
  - IAM  Identity & Access Management
  - IVS  Infrastructure & Virtualization
  - IPY  Interoperability & Portability
  - MOS  Mobile Security
  - SEF  Sec. Incident Mgmt, E-Disc & Cloud Forensics
  - STA  Supply Chain Mgmt, Transparency & Accountability
  - TVM  Threat & Vulnerability Management
Questions?