Double the value: SOC 2+ reporting

April 13, 2021

Presented by:
Arshad Ahmed
Jaclyn Dettloff
Vikas Sharma
Your Presenters

Arshad Ahmed
Partner, IT Assurance Services
Partner-in-Charge, SOC Solutions
arshad.ahmed@crowe.com

Jaclyn Dettloff
Senior Manager, IT Assurance Services
jaclyn.dettloff@crowe.com

Vikas Sharma
Senior Manager, IT Assurance Services
vikas.sharma@crowe.com
Agenda

01 Third-party assurance landscape
02 Overview of SOC 2+ reporting option
03 Choosing a second framework
04 Agreed-upon procedures option
05 Questions and Closing
Third-party assurance

Current landscape
Building trust through assurance

Drivers for third-party assurance reporting

- Differentiate from their peers and expand market reach
- Meet due diligence and contractual requirements
- Demonstrate the maturity of information security program and technology practices
SOC reporting

<table>
<thead>
<tr>
<th>SOC 1 Report</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Primary users:</strong> user auditors, to support financial statement audits</td>
</tr>
<tr>
<td><strong>Focus:</strong> Internal controls over financial reporting (ICFR)</td>
</tr>
<tr>
<td><strong>Scope:</strong> Controls to meet organization-defined control objectives</td>
</tr>
</tbody>
</table>

Objective is to address customers’ risks related to ICFR – typical coverage areas:

- Account setup and maintenance
- Transaction processing
- System and data integrity (ITGCs)
- Report outputs
SOC reporting

SOC 2 Report

**Primary users:** customers’ vendor management function, to support program requirements

**Focus:** Internal controls over systems and data

**Scope:** Controls to meet one or more Trust Services criteria

Can address wider IT-related concerns, including:

- Security of systems and data
- System availability and data recoverability
- Processing integrity and accuracy (includes non-financial data)
- Safeguards to protect sensitive data
- Data privacy: collection, use and disclosure of PII
Current landscape

Challenges faced by **third parties**:
- Unique security requirements
- Inability to leverage questionnaire responses across customers
- Time-intensive customer audits

Challenges faced by **customers**:
- Effort to chase down questionnaire responses
- Complexity to evaluate responses
- Lower assurance (responses not validated)
SOC 2+ reporting
Overview and key differences

1. Current Landscape
2. SOC 2+ Overview
3. Second Frameworks
4. Agreed-Upon Procedures
5. Q&A
SOC 2+ overview

SOC 2+ at a Glance…

Scope and Effort
SOC 2 Trust Services Criteria and second industry framework

Key Features
- Leverages recognition of SOC 2
- Conducted according to AICPA SOC 2 examination procedures
- Provides more comprehensive view of internal controls

Deliverable
SOC 2 report, covering both frameworks, that includes:
- Opinion on control design and effectiveness over a period
- Description of controls
- Control test procedures and results
SOC 2+ report deliverable

Illustrative SOC 2 Opinion

To Company ABC

Scope
We have examined Company ABC’s accompanying description of its XYZ Solutions system... throughout the period January 1, 2021 to September 30, 2021... and the suitability of the design and operating effectiveness of controls stated in the description throughout the period January 1, 2021 to September 30, 2021, to provide reasonable assurance that Company ABC’s service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Confidentiality (applicable trust services criteria).

Opinion
In our opinion, in all material respects:

a. the description presents Company ABC’s XYZ Solutions system that was designed and implemented throughout the period January 1, 2021 to September 30, 2021, in accordance with the description criteria.

b. the controls stated in the description were suitably designed throughout the period January 1, 2021 to September 30, 2021, to provide reasonable assurance that Company ABC’s service commitments and system requirements would be achieved based on the applicable trust services criteria...

c. the controls stated in the description operated effectively throughout the period January 1, 2021 to September 30, 2021, to provide reasonable assurance that Company ABC’s service commitments and system requirements were achieved based on the applicable trust services criteria...

Illustrative SOC 2+ Opinion

To Company ABC

Scope
We have examined Company ABC’s accompanying description of its XYZ Solutions system... throughout the period January 1, 2021 to September 30, 2021... and the suitability of the design and operating effectiveness of controls stated in the description throughout the period January 1, 2021 to September 30, 2021, to provide reasonable assurance that Company ABC’s service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Confidentiality (applicable trust services criteria), and the requirements set forth in the HIPAA Security Rule (HIPAA criteria).

Opinion
In our opinion, in all material respects:

a. the description presents Company ABC’s XYZ Solutions system that was designed and implemented throughout the period January 1, 2021 to September 30, 2021, in accordance with the description criteria.

b. the controls stated in the description were suitably designed throughout the period January 1, 2021 to September 30, 2021, to provide reasonable assurance that Company ABC’s service commitments and system requirements would be achieved based on the applicable trust services criteria and the HIPAA Security Rule criteria...

c. the controls stated in the description operated effectively throughout the period January 1, 2021 to September 30, 2021, to provide reasonable assurance that Company ABC’s service commitments and system requirements were achieved based on the applicable trust services criteria and the HIPAA Security Rule criteria...
Benefits of SOC 2+

Report Users

• Look and feel of SOC 2
• More in-depth control information
• Greater coverage for vendor risk assessments and questionnaires
• Greater assurance from evaluation against two frameworks
• Supported by an independent auditor’s opinion

Service Organizations

• Single audit experience
• Highlights control maturity and depth
• Provides additional technical or industry-specific coverage
• Reduces time to manually respond to customer requests
• Single report deliverable to distribute
Typically, 20-50% additional controls needed to address second framework
Choosing your ‘+’
Second framework options

1. Current Landscape
2. SOC 2+ Overview
3. Second Frameworks
4. Agreed-Upon Procedures
5. Q&A
Commonly used frameworks

- Any existing control framework can be used
  - ✔ Part of SOC 2 report: opinion on control design and operating effectiveness
  - ✔ Most common SOC 2+ options noted at right

- Framework with IT / security focus recommended
  - ✔ Related subject matter: common relevance, common report users
  - ✔ Common areas of coverage between two frameworks

SOC 2+ Options

- HITRUST
  - Common Security Framework
- HIPAA
  - Security and/or Privacy Rules
- Cloud Security Alliance
  - Cloud Controls Matrix
- ISO
  - 27001
## SOC 2 + HIPAA Security Rule

<table>
<thead>
<tr>
<th>Control Areas</th>
<th>Illustrative Additional Requirements</th>
</tr>
</thead>
</table>
| Policies and Procedures| • Employee sanctions for non-compliance  
                          • Pervasive minimum retention of six years                                |
| Entity Level Controls  | • Awareness of password management practices  
                          • Business associate agreements (BAAs)                                   |
| IT Operations          | • Facility maintenance records  
                          • Continuity of operations                                               |
| Security Operations    | • Emergency access  
                          • Monitoring log-in attempts                                               |
| Technical Safeguards   | • Workstation security and portable media  
                          • Encryption of ePHI                                                      |
Control Areas

Policies and Procedures
- Clean desk, mobile devices, and teleworking
- Cryptography

Entity Level Controls
- Independent review of information security program
- Outsourced software development arrangements

IT Operations
- Inventories and asset management
- Business continuity program documentation

Security Operations
- Restriction of unauthorized software
- Audit log content and retention

Technical Safeguards
- Network segregation and sensitive system isolation
- Secure information exchange
**SOC 2 + | Cloud Security Alliance CCM**

<table>
<thead>
<tr>
<th>Control Areas</th>
<th>Illustrative Additional Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policies and Procedures</td>
<td>• Disciplinary actions, mobile devices and BYOD</td>
</tr>
<tr>
<td></td>
<td>• Cryptography, event logging and APIs</td>
</tr>
<tr>
<td>Entity Level Controls</td>
<td>• Employee non-disclosure and confidentiality agreements</td>
</tr>
<tr>
<td></td>
<td>• Documented, maintained control framework</td>
</tr>
<tr>
<td>IT Operations</td>
<td>• Supply chain management and accountability</td>
</tr>
<tr>
<td></td>
<td>• Data center environmental security and maintenance</td>
</tr>
<tr>
<td>Security Operations</td>
<td>• Application programming interfaces (APIs)</td>
</tr>
<tr>
<td></td>
<td>• Data input and output integrity routines</td>
</tr>
<tr>
<td>Technical Safeguards</td>
<td>• Infrastructure hardening (O/S, hypervisor)</td>
</tr>
<tr>
<td></td>
<td>• Information portability and data requests</td>
</tr>
</tbody>
</table>
## SOC 2 + | ISO 27001

### Control Areas

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Information Security Management System (ISMS)</td>
<td>• Compliance with international legal and regulatory standards</td>
<td>• Project management security considerations</td>
<td>• Secure coding practices</td>
<td>• Storage and access protections for logs</td>
</tr>
<tr>
<td>• Mobile devices, and teleworking</td>
<td>• Non-disclosure and confidentiality agreements</td>
<td>• Sensitive data identification and protections</td>
<td>• Configuration management</td>
<td>• Secure information exchange</td>
</tr>
</tbody>
</table>

---

© 2021 Crowe LLP
Framework Summary

HIPAA Security Rule
- Security standards to protect PHI
- Demonstrates HIPAA compliance – management, customers and regulators
Typically, 10-15% additional controls

HITRUST CSF**
- Comprehensive information protection framework
- Highlights more in-depth technical safeguards
- Resonates with healthcare customers
Typically, 25-35% additional controls

ISO 27001**
- Global information security standard
- Demonstrates ongoing management and improvement of information security program
- Resonates with international customers and within technology industry
Typically, 20-25% additional controls

CSA Cloud Controls Matrix**
- Security standards for cloud providers
- Tailored to cloud computing risks and practices
- Acknowledges and addresses specific security risks for cloud providers
Typically, 30-50% additional controls

**Does not provide certification
Agreed-upon procedures
A closer look

1. Current Landscape
2. SOC 2+ Overview
3. Second Frameworks
4. Agreed-Upon Procedures
5. Q&A
Agreed-Upon Procedures

AUPs at a Glance…

Scope and Effort
Custom scope of procedures, can be determined by organization and/or CPA firm

Deliverable
Attestation report that includes:
- Independent practitioner’s report
- Detailed procedures and results

Key Considerations
- Fully custom scope (no framework as basis)
- Very detailed procedures – best positioned to meet customer needs
- Market awareness: customer education may be needed
- Does not provide an opinion; only factually reports results of procedures
Agreed-Upon Procedures

- Existing type of AICPA attestation engagement
- Report deliverable includes:
  - Independent practitioner’s report
  - Detailed procedures and results

**THEN (SSAE 18)**
Single-use report
- Scope designed for a single report user
- Procedures must be formally accepted by the user

**NOW (SSAE 19)**
Can be for restricted or general use
- Able to be distributed to multiple report users
- Procedures now must only be acknowledged by management as appropriate
Q&A: Open Discussion