Less is More: Mastering the Art of SOC 2® +

Moderator: Chad Phillips, Managing Director, National SOC2 Leader

Panelists:
- Mike Seifert, VP, Division Risk Officer – Fiserv
- Scott Crowell, IT Risk and Compliance Director – Fiserv
- Jay Williams, Sr. IT Risk and Compliance Consultant – Fiserv
- Biju Thomas, Advisory Senior Manager – Deloitte
- Heather Kain, Advisory Senior Consultant – Deloitte
Agenda

I. Introductions
II. Fiserv Overview
III. Fiserv Output Solutions Overview
IV. Deloitte Overview
V. What are SOC2 Reports
VI. SOC2 +
VII. Panel Q&A
VIII. Audience Q&A
Fiserv Overview & Background

Fiserv by the Numbers (excerpt from May 2016 Annual Shareholder Meeting materials)
Output Solutions
Business Overview
Fiserv Output Solutions: Why We’re in Business

Our Vision is to be the leading provider of business critical communications by providing our clients products and services of superior value and reach.

Our Purpose is to help make our customers successful.

Our Operating Model is based on customer centricity, results orientation and market driven strategies.
SOC 2 Emergence

SOC 2 is emerging as a leading standard across industries that can be applied for regulatory or non-regulatory purposes to cover business areas outside of financial reporting.

<table>
<thead>
<tr>
<th>Topic</th>
<th>SOC 2 Guidance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Professional Guidance</td>
<td>AICPA Statement on Standards for Attestation Engagements no. 18 encompassing AT-C Section 105, Concepts Common to All Attestation Engagements, AT-C Section 205, Examination engagements and TSP section 100, Trust Services Principles and Criteria Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy</td>
</tr>
<tr>
<td>Scope</td>
<td>Controls at a service organization intended to mitigate risks related to security, availability, processing integrity, confidentiality, or privacy (trust services principles)</td>
</tr>
<tr>
<td>Application of SOC 2</td>
<td>SOC 2 can be applied for regulatory or non-regulatory purposes to cover business areas outside of financial reporting. The report can be distributed to customers and other stakeholders to demonstrate a focus on system and processing controls to meet their requirements. SOC 2 can be applied to virtually every industry and business sector. SOC 2 will allow service organizations to provide assurance to customers and other stakeholders that effective internal controls are in place.</td>
</tr>
</tbody>
</table>

**Intended Audience/Users**
- Third-party management/risk management
- Internal/external auditors
- Useful to a third party’s customers, regulators, business partners

**SOC 2—How it improves System Security**
- Adoption of leading information security practices/controls during the attestation process
- Year on year service auditor assessments improve the security posture of the organization
## Trust Principle Definitions\(^1\)

### 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 (GAPP) issued by the AICPA and CICA.

---

\(^1\) As defined in paragraph .10 of TSP section 100 © 2017 HITRUST Alliance.
Panel Q&A
Strategy Drivers

Market and contractual obligations to address healthcare industry trends (i.e. HITRUST)

Inefficient use of third party assurance spend

Overwhelming audit, questionnaire and vendor management requests from clients and third parties

Necessity to optimize compliance program requirements for efficiency, effectiveness and manageability (integrated framework)
Less is More: SOC 2+

SOC 2+ reports create substantial efficiencies for organizations. Organizations are able to spend less time and fewer resources conducting performance reviews at their OSPs. Both OSPs and customers are also less likely to be exposed to compliance violations that can result in various forms of liability, including fines.

For OSPs, the benefits are even more significant. SOC 2+ reports allow OSPs to demonstrate to their stakeholders that effective internal controls are in place. These controls pertain to the criteria covered in the TSPs of security, availability, processing integrity, confidentiality, and privacy, as well as many of the most detailed requirements covered in other regulatory and industry-specific frameworks. They offer a standardized format for meeting a broad range of regulatory and non-regulatory control requirements, eliminating the need for redundant activities and one-off responses. They're also flexible enough that they can be tailored to meet the specific needs of organizations.
Overview of the Certification Process

**Getting Ready**
- **Scope**
  - Establish SOC2 and HITRUST scope
- **Readiness**
  - Purchase licensing requirements
  - Attend trainings

**Organization**
- **Self-Assessment**
  - Complete in tool
  - Understand CAP requirements
- **Gap Remediation**
  - Implement changes for unmet requirement statements

**Assessor firm**
- **SOC 2 Interim**
  - Perform testing with combined frameworks
- **SOC 2 Rollforward**
  - Perform testing with combined frameworks

**HITRUST**
- **Validated Assessment**
  - Complete in tool
  - Agree upon scoring

**Testing**
- **QA Request**
- **Draft Report**
- **Final Steps**
- **HITRUST Certification**
- **CAPs**
  - Submit plans to address low scores

**QA Evidence**
- Coordinate response to HITRUST with certified assessor
Audience Q&A
SOC 2+ HITRUST Resources

Information and Downloadable Guides from HITRUST
- HITRUST CSF current version
  - https://hitrustalliance.net/hitrust-csf/
- Which Assessment is Right for Me?
  - https://hitrustalliance.net/assessment-right/
- HITRUST CSF and SOC 2 FAQs
- Risk Analysis Guide

Information and Downloadable Guides from AICPA
- HITRUST FAQ
- SOC 2 + HITRUST CSF Illustrative Report
- Trust Services Map to HITRUST CSF
  - https://www.aicpa.org/InterestAreas/FRC/AssuranceAdvisoryServices/DownloadableDocuments/SOC_II_to_HITRUST_Mapping.xlsx

Information and Downloadable Guides from Deloitte & Touche LLP
- Third Party Assurance Optimization
- Achieving Third-Parting Reporting Proficiency with SOC 2+
Contacts

Chad Phillips  
Deloitte - Advisory Managing Director  
chadphillips@Deloitte.com  
313.396.5938

Mike Seifert  
FOS - Vice President Division Risk Officer  
Mike.Seifert@Fiserv.com  
262.879.5824

Biju Thomas  
Deloitte - Advisory Senior Manager  
bjithomas@Deloitte.com  
404.220.1412

Scott Crowell  
FOS - Director IT Risk & Compliance  
Scott.Crowell@Fiserv.com  
281.275.1976

Heather Kain  
Deloitte - Advisory Manager  
hkain@Deloitte.com  
214.840.1423

Jay Williams  
FOS - Senior IT Risk & Compliance Consultant  
Clarence.Williams@Fiserv.com  
281.274.6351
Visit www.HITRUSTAlliance.net for more information

To view our latest documents, visit the Content Spotlight