Understanding the Relationship Between SOC 2® and HITRUST®

Moderator: Ken Vander Wal, Chief Compliance Officer – HITRUST
Panelists: Paul Johnson, Partner - Wipfli
          Brenda Magri, Sr. Director Security Strategy - Fiserv
          Heather Kain, Advisory Manager– Deloitte & Touche LLP
Agenda

I. Introductions
II. Company Overviews
III. SOC 2 and SOC 2 +
IV. Benefits of SOC 2 + HITRUST CSF
V. Engagement Considerations
VI. Panel Q&A
VII. Audience Q&A
<table>
<thead>
<tr>
<th>Category</th>
<th>Statistic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deposit accounts</td>
<td>140 million</td>
</tr>
<tr>
<td>Use Fiserv for account processing</td>
<td>more than 1 in 3</td>
</tr>
<tr>
<td>Mobile banking end users</td>
<td>approximately 28 million</td>
</tr>
<tr>
<td>Mobile banking end users</td>
<td>32 consecutive years</td>
</tr>
<tr>
<td>Mobile banking end users</td>
<td>of double-digit EPS growth</td>
</tr>
<tr>
<td>Nearly associates worldwide</td>
<td>24,000</td>
</tr>
<tr>
<td>Proprietary consumer research</td>
<td>every 90 days</td>
</tr>
<tr>
<td>In more than 80 countries</td>
<td>12,000 clients</td>
</tr>
<tr>
<td>Financial services professionals attend Forum</td>
<td>nearly 4,000</td>
</tr>
<tr>
<td>Patents issued and pending</td>
<td>140 patents+</td>
</tr>
<tr>
<td>Boardroom Series online</td>
<td>12,000</td>
</tr>
<tr>
<td>Community participants</td>
<td>24/7/365</td>
</tr>
</tbody>
</table>
Fiserv Billing & Payments Group

Prepare
- Consumer Data
  - Design Composition
  - Print
  - Archive

Pay
- Consumer Data
  - Paper
  - FIs
  - Alternate Channels
  - Biller Site

Present
- Consumer Data
  - Paper
  - Walk-In
  - Biller Direct Registered
  - BD Direct Deposit
  - Biller Direct - Convenience Fee
  - Banks / FIs
  - Alternate Channels

Protect
- Consumer Data
  - Reconcile
  - Settle
  - Protect
Deloitte Touche Tohmatsu Limited (DTTL) Global Network

Deloitte globally

DTTL

Americas

EMEA

Asia-Pacific
**Wipfli Facts at a Glance**

- Employs over 2,000 associates
- Approximately 250+ partners
- Ranked in the top 20 among America’s 100 largest public accounting firms
- Market-driven organization focused on a commitment to go to market through industry specialization
- Specializes in serving small, medium, and large closely held, privately owned businesses as well as public companies
- Serves more than 60,000 clients
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 (SSAE18)</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 criteria)</td>
</tr>
<tr>
<td>Application of SOC 2</td>
<td>SOC 2 can be applied for regulatory or non-regulatory purposes, and may cover business areas outside of financial reporting. Report may be distributed to customers and other. SOC 2 can be applied to virtually every industry and business sector.</td>
</tr>
</tbody>
</table>

**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

**Intended Audience/Users**

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

The controls pertain to the criteria covered in the AICPA trust services criteria 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, including HITRUST.

SOC 2+ report are flexible enough that they can be tailored to meet the specific needs of organizations.
AICPA Trust Services Criteria

The five attributes of a system within a SOC 2 report are known as Criteria:

- **Security**
- **Availability**
- **Processing Integrity**
- **Confidentiality**
- **Privacy**
Overview of the SOC 2+ and HITRUST Certification Process

**Getting Ready**
- Purchase HITRUST licensing requirements
- Attend trainings

**Scope**
- Establish SOC2 and HITRUST scope

**Readiness**
- Purchase HITRUST licensing requirements
- Attend trainings

**Self-Assessment - Optional**
- Complete in tool
- Understand CAP requirements

**Gap Remediation**
- Implement changes for unmet requirement statements

**Testing**
- SOC 2 Interim
  - Perform testing with combined frameworks
- SOC 2 Rollforward
  - Perform testing with combined frameworks
- Validated HITRUST Assessment
  - Complete in tool
  - Agree upon scoring

**QA Evidence**
- Coordinate response to HITRUST with certified assessor

**Draft HITRUST Report**
- QA Request
- CAPs
- Submit plans to address low scores

**Final Steps**
- HITRUST Certification
Why SOC 2 + HITRUST + Certification?

- Applies to all industry sectors
- Allows year-over-year assessment

Hitrust is a maturity assessment

Fiserv provides print, billing and financial services for:

- Providers
- Healthcare Insurance Providers
- Third Parties to Providers
SOC 2 + HITRUST CSF Table of Contents Example

Report Sections

I. Management Assertion
II. Independent Service Auditor’s Report
III. Entity’s Description of its System
IV. Trust Services Criteria/HITRUST CSF Criteria* Controls Tested and Results
V. Mapping of Applicable Trust Services Criteria to the HITRUST CSF, and HITRUST CSF certification report (when included)

* HITRUST CSF criteria can be security controls required for certification (75 in version 9) or all security controls (135)
Suitability of HITRUST CSF for SOC 2 Reporting

AICPA Requirements for Suitable Criteria

✓ Objectivity—Criteria should be free from bias
✓ Measurability—Criteria should permit reasonably consistent measurements, qualitative or quantitative, of subject matter
✓ Completeness—Criteria should be sufficiently complete so that those relevant factors that would alter a conclusion about subject matter are not omitted
✓ Relevance—Criteria should be relevant to the subject matter.

The HITRUST CSF has been developed following due process procedures. The criteria are made available to users of the report.
HITRUST Certification, SOC 2 or Both?

• Scope
• Timing
• Audience
• Prioritization/Focus
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/
- 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

Paul Johnson
Wipfli - Partner
pjohnson@wipfli.com
651.766.2895

Heather Kain
Advisory Manager
Deloitte & Touche LLP
hkain@Deloitte.com
203.856.1141

Brenda Magri
FISERV – Senior Director, Security Strategy Division Information Security Officer
Brenda.Magri@Fiserv.com
214.750.2804
This presentation contains general information only and Deloitte, Wipfli, and FISERV are not, by means of this presentation, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This presentation is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this presentation.
Visit www.HITRUSTAlliance.net for more information

To view our latest documents, visit the Content Spotlight