Securing your future

Mastering Third-Party Frameworks

WIPFLI

Agenda

Welcome and Introductions

Overview of third-party frameworks and the impact to you

Organizations perspective of vendor oversight

Third-party adoption of frameworks

Q&A

Jacqueline Cooper, CPA, MBA, CISA, CITP – SOC Practice

Jackie Cooper is a senior manager in the firm's risk advisory services practice. She has over ten years of experience working in public accounting and consulting. Jackie is responsible for managing projects related to compliance, security, confidentiality, availability, processing integrity and privacy in many industries including Health Care, Finance and Technology.   Additionally, she is responsible for performing walk-throughs of clients' internal environments, collaboratively identifying strengths or weaknesses of internal controls, preparing reports and providing other service offerings for clients.

Specializations

- SOC1, SOC2, and SOC3
- HITRUST Common Security Framework services
- Internal control assessments
- Internal audits
- IT audits
- IT governance
- Operational audits

We focus on emerging and mid-market organizations — the businesses that drive our economy forward.

We bring specialized knowledge in the following industries:

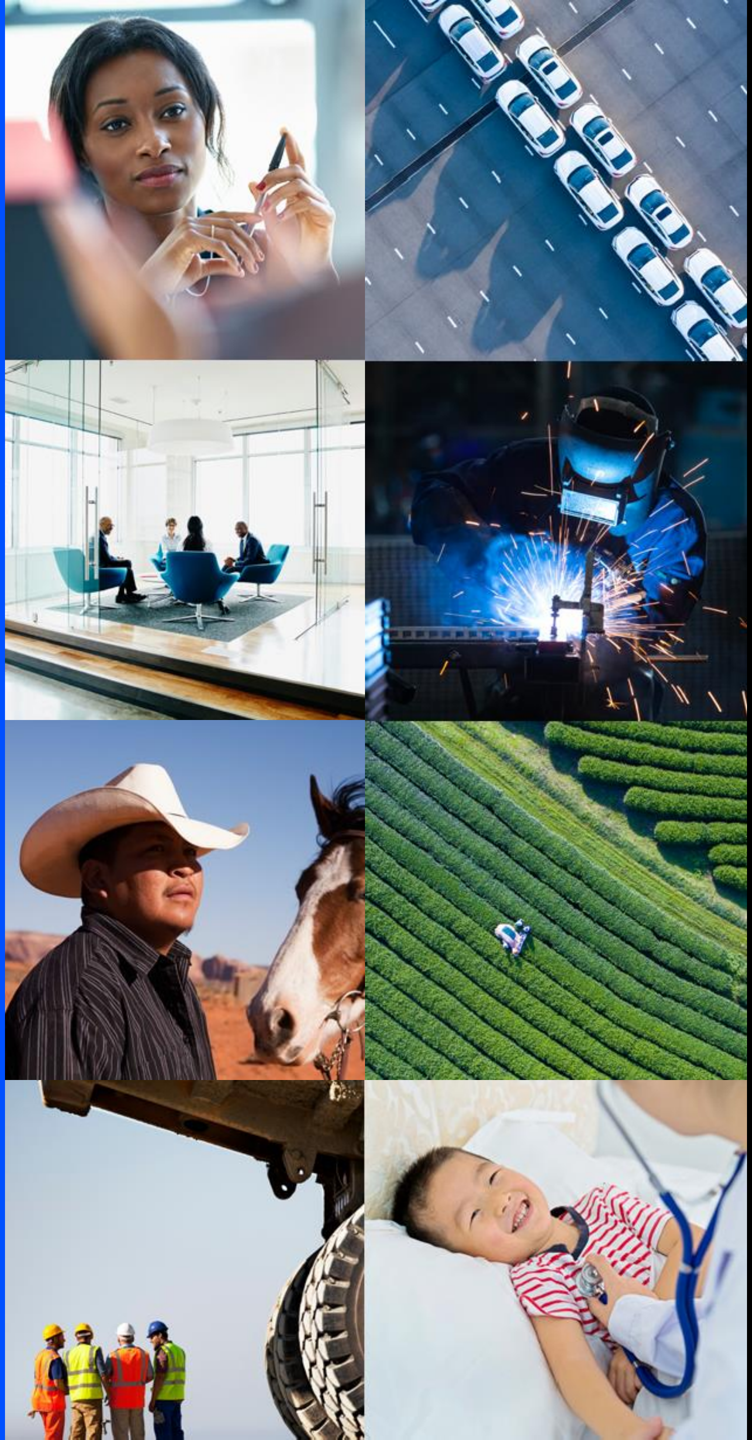
- Agribusiness
- Construction and real estate
- Dealerships
- Financial institutions and services
- Governments
- Healthcare
- Manufacturing and distribution
- Nonprofits
- Private equity
- Technology
- Tribal gaming and government

Global connections.

With more than 2,400 associates in 40+ offices in the U.S., two offices in India and one in the Philippines, we can meet you where you are and get you where you want to go.

Wipfli is a member of Allinial Global, an accounting firm association of legally independent accounting and consulting firms with offices in North America and throughout the world through international members and partnerships.

Member of Allinial GLOBAL™



Technology companies need to scale and become profitable quickly, without cutting corners or slowing down. And you need to mature operations and processes, without losing agility or your edge. We help with services that match your needs at each inflection point.

800+

More than 800 growing tech companies trust Wipfli to help them SCALE AT SPEED.

13

Partners / Principals

150+

Technology vertical specific associates

300+

Wipfli services

Tax and audit

We go beyond numbers to deliver strategy and tactics to mitigate liabilities and meet compliance regulations.

Compliance and risk

Our team proactively manages compliance and risk across your organization.

Outsourcing

Optimize your day-to-day operations when our team handles your accounting, controller, payroll, technology and cybersecurity needs.

Digital transformation

From strategy and custom software solutions to data, analytics, ERPs, CRMs, we help you connect, transform and grow.

ESG

Build a strategy and produce results that will increase revenue and draw investors and recruits.

Business transition

Be confident in your future with support in transition, succession planning, M&A and valuations.

Strategy & optimization

Build the organization you envision with a compelling vision, operational excellence and tech optimization.

People and talent

Navigate people-centered change and optimize talent with the right team, rewards and roles.

Organizational development

Build the team you need to lead today and tomorrow to scale your growth and increase your value.

Overview of Third-Party Frameworks and the Impact to You

WIPFLI

Third Party Frameworks

AICPA
SOC
aicpa.org/soc4so
SOC for Service Organizations | Service Organizations
™

HIPAA
COMPLIANT

HITRUST
CSF Certified

Why SOOOOO Many!

Where do all these frameworks come from?

- History of security issues
- Regulations/Laws
- Security Organizations
- Accreditation bodies
- Industry specific needs

Why do I have to do this?

- Business need
  - Competitive advantage
  - Client requirement
- Regulation requirement
  - Laws
  - Industry
- Risk Management
  - Vendor Due Diligence

Organizations perspective of third-party frameworks

WIPFLI

Organizations looking to work with third parties

What to look out for in a framework report

- Does it cover the scope of services you are looking for
- Is the opinion/reporting results/etc clean?
- Do the controls and tests (if applicable) make sense to you?
- Are they willing to answer any other questions?

Questions to consider for your third party

- Are there changes to the service that are up coming that you should be aware of?
- Are there major third parties that they are relying on that impact the services that is provided?
- Any public litigation that the company is going through?

Organizations looking to work with third parties

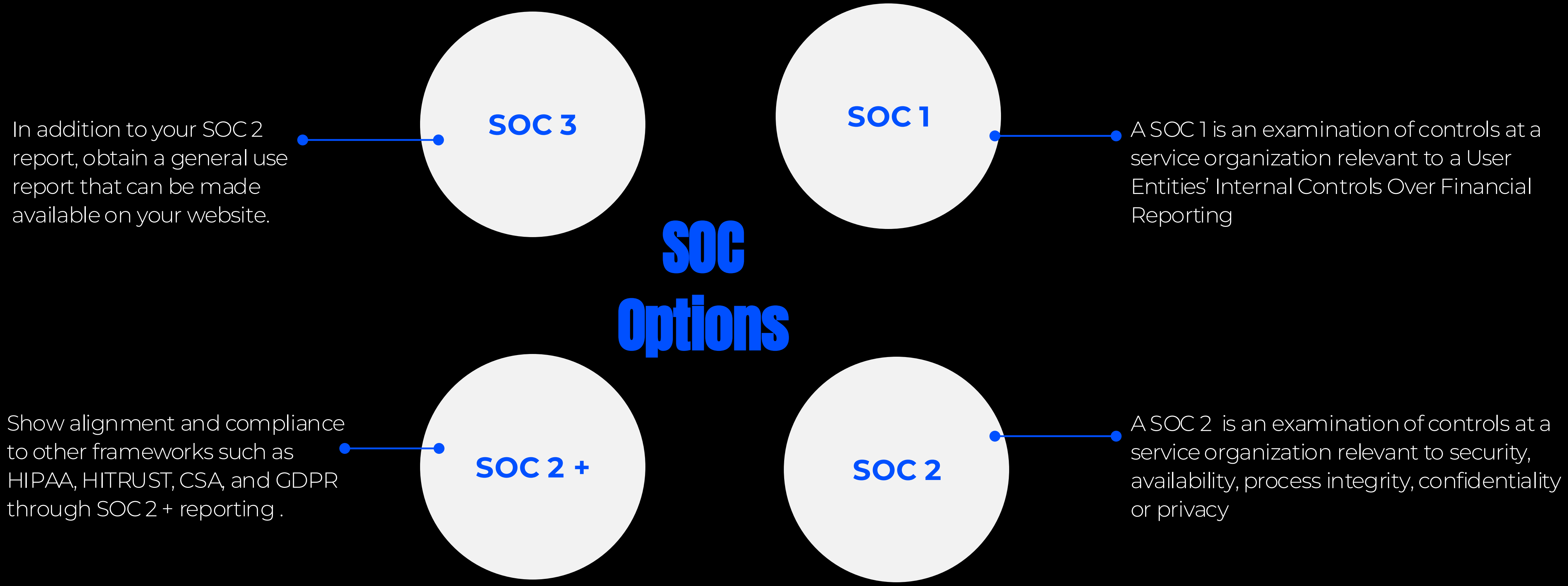
Risk assessment

- Vendor due diligence checks
- Perform risk assessment
  - Evaluate the service being provided
  - Evaluate the impact to your business
  - Evaluate any mitigation strategies
- Give the vendor a Ranking and document due diligence that needs to be performed annually

SOC and HITRUST Frameworks deep dive

WIPFLI

What Is SOC:



SOC Options

SOC 3

In addition to your SOC 2 report, obtain a general use report that can be made available on your website.

SOC 1

A SOC 1 is an examination of controls at a service organization relevant to a User Entities' Internal Controls Over Financial Reporting

SOC 2 +

Show alignment and compliance to other frameworks such as HIPAA, HITRUST, CSA, and GDPR through SOC 2 + reporting .

SOC 2

A SOC 2 is an examination of controls at a service organization relevant to security, availability, process integrity, confidentiality or privacy

SOC 2

Report Overview

- American Institute of Certified Public Accountants (AICPA) developed SOC 2 around five (5) Trust Services Criteria
  - Options include security (all), confidentiality, availability, processing integrity, privacy
- Audit Types
  - Type 1 – Design
  - Type 2 – Operating Effectiveness
- Report Components
  - Management Assertion
  - Independent Service Auditor’s Report
  - System Description
  - Applicable Trust Services Criteria and Related Controls, Tests of Controls, and Results of Tests
  - Other information provided by Management

SOC 2 Type 2 Report Coverage

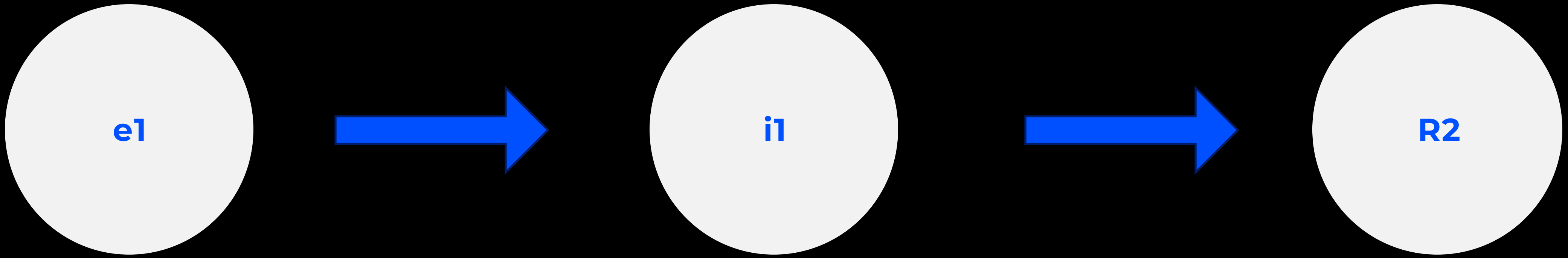
- Control Environment
- Communication and Information
- Risk Assessment
- Monitoring Activities
- Control Activities
- Logical and Physical Access Controls
- System Operations
- Change Management
- Risk Mitigation
- Other Optional Trust Services Criteria
  - Confidentiality
  - Availability
  - Processing Integrity
  - Privacy

What is HITRUST?

Work with our clients to meet their compliance needs

- HITRUST Alliance – Created the CSF framework
- Security and Privacy framework
- Companies often need both both HITRUST and SOC
- A lot need to consider cybersecurity requirements

HITRUST Options



e1

1-year certification

An entry-level validated assessment based on 44 foundational security controls. Organizations can build on these controls as a step toward attaining the more comprehensive i1 or r2 certifications.

i1

1-year certification

For mid-level organizations and offers a more comprehensive level of assurance than the e1, with more controls in scope. Work done to attain an active i1 certification can be applied toward attaining an r2.

R2

2-year certification
Requires an interim assessment

For organizations that need to demonstrate regulatory compliance with authoritative sources like HIPAA, the NIST Cybersecurity Framework. It is the most comprehensive and robust HITRUST certification.

Third-party adoption of frameworks

WIPFLI

I am the Vendor – what are my considerations

Which frameworks serve you

- What best suites my organization and my industry?
- What type of data am I collecting, or service am I providing?

Budget Considerations

- Do I need a compliance officer?
- Who are a we going to engage in the work?

Timing Consideration

- Who needs the report and by when?
- How much do I need to prepare?

Consider options for certification

- For my framework what are the reportion options?
- What are a stakeholders expectations?

Certification Stacking

What is it?

- Cert Stacking is when organizations want/need to demonstrate they meet multiple frameworks with their implemented security programs
- Focus for today is HITRUST Certification/SOC Examination Stacking
- External auditors assessing you against multiple frameworks
- Other common frameworks – ISO, HIPAA, CSA, state-based security programs

Why Cert Stack?

What are some reasons an organization would Cert Stack?

- Customers of organizations are requiring different frameworks ie. a SOC Examination and HITRUST Certified, etc
- Need to show SOC 2 compliance and would like a coordinated approach to HITRUST certification
- The ability to address both needs in an efficient way. Using a CPA firm that is also an approved HITRUST Authorized External Assessor firm (like Wipfli) will gain efficiencies in the engagement process (planning, testing, onboarding the audit teams)

Why are we seeing an increase market for cert stacking?

- HITRUST introduction of the e-1 and i-1
- Industries pushing for more security controls around information sharing
- States passing more privacy/security/third party laws
- Regulatory or Legal requirements in the organization's industry

Benefits of Cert Stacking

- Increased coverage for your diverse customer base
- Speed the sales cycle
- Differentiate your company from your competitors
- Increased efficiency over completing each audit separately
- Cost savings

Thank you for joining us!

- Key Takeaways: **Secure your organizations future**
  - Know your framework options and what is best for your industry, clients and organization
  - Can you rely on multiple frameworks or Cert stack to help meet third party requirements
  - Increase Trust and Creditability – Demonstrate a strong commitment to data protection and regulatory compliance

- Next Steps:
  - Determine what is best for your organization and security
  - Consider finding a partner/firm who is experienced and can help you execute to secure your organization

Stay Connected:

We'd love to hear from you!

https://www.wipfli.com/industries/tech/technology-assurance-services

Jackie Cooper – jcooper@wipfli.com

wipfli.com