FORVIS

WEBINAR

How Technology Service Providers Can Help Increase Their Client Base

March 28, 2023

SOC & HITRUST

TO RECEIVE CPE CREDIT

WEBINAR

- You must respond to at least 3 of the 4 polling questions per CPE hour
- You must be logged in for a minimum of 50 minutes per every CPE hour in order to receive CPE credit

FORVIS

Speaker Introductions

Jennifer Jones
National Managing Principal
919.610.4658
jennifer.jones@forvis.com

Ryan Boggs
Principal
828.989.3176
ryan.boggs@forvis.com

FORVIS

Learning Objectives

WEBINAR

- Define third parties, third-party risk, and third-party risk management
- Recognize the current risk landscape faced by clients of third-party service providers
- Identify options for third-party service providers to build trust with their customers and prospects in order to increase their client base

FORVIS

Service Providers

- A Third-Party Service Provider (TSP) is generally defined as an external person or company who provides a service or technology
- In today's technology-driven business environment, it is virtually impossible to efficiently and effectively conduct business without entering into a business relationship in which another business may be accessing, sharing, or leveraging an organization's data assets
- A fourth-party provider is a service provider with whom you do not have direct contract; however, your vendor does have a business relationship with them for their services or products

FORVIS

Third-Party Risk and TPRM

- Third-party risks are the potential risks that arise from companies relying on outside parties to perform business services or activities
- Third-party risk management (TPRM) is a form of risk management that focuses on identifying and reducing risks relating to the use of third parties (sometimes referred to as vendors, suppliers, partners, contractors, or service providers)

FORVIS

Take a Step Back and Put Yourself in Your Clients' Shoes

- Why do clients use our third-party services? What is the value proposition that we offer?
- If they can receive this service somewhere else, what value on top of the primary service can I provide?

If you want to be successful in business (in life, actually), you have to create more than you consume. Your goal should be to create value for everyone you interact with. Any business that doesn't create value for those it touches, even if it appears successful on the surface, isn't long for this world. – Jeff Bezos

FORVIS

Adding Value Beyond the Primary Solution

The Basics

- Solicit customer feedback
- Create a positive user experience
- Provide unrivaled customer support
- Educate customers on your product or service through free training, webinars, or other outreach mediums

FORVIS

Already Doing All That?

What else can TSPs do to add value?

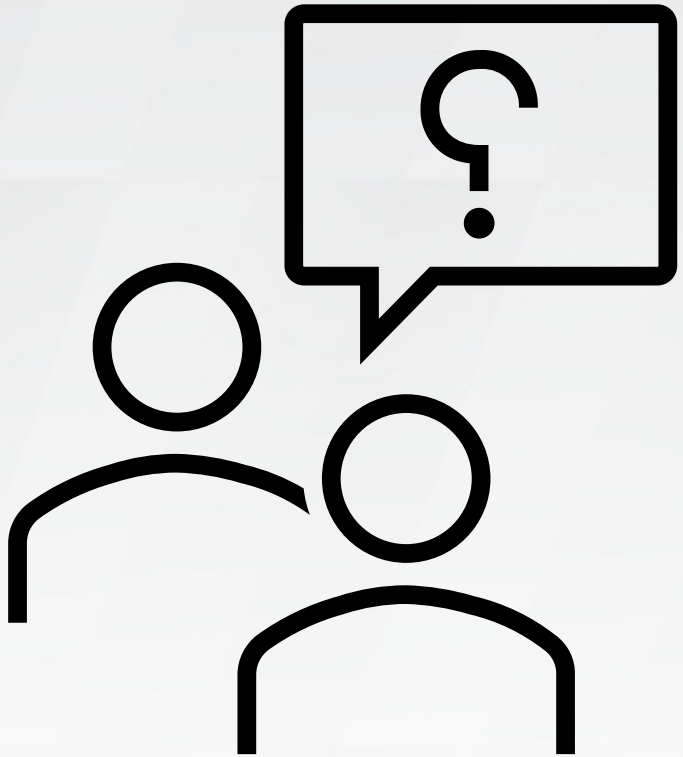
FORVIS

Build and Maintain Trust

FORVIS

Importance of Trust

- Solicit feedback from your operations and sales team
  - What are their pain points?
  - What questions do prospects ask the most?
  - Are there any recurring or common concerns received from current clients?



FORVIS

Dollars to Donuts, It's Trust

- Trust that their data will be kept secure
- Trust that association with your business will not negatively impact their own reputation
- Trust that any information stored will be available whenever they need it
- Trust that you will keep your promises

Trust is the firm belief in the reliability, truth, ability, or strength of someone or something and is variable, intangible, and often hard to communicate or quantify, but it doesn't make it any less important; your reputation depends on it.

FORVIS

What's Driving These Requests?

- At the most fundamental level, such customer and prospect requests are driven by perceived risks
- Risks are commonly perceived and evaluated as part of a company's Vendor Management Program
- A Vendor Management Program is something that all businesses, TSPs, and non-TSPs alike should have to help control risk from interacting with other businesses

FORVIS

Vendor Management Program

- TSPs inherently expose customers to an array of risks including strategic, reputational, operational, transactional, and cybersecurity risks
- The purpose of a Vendor Management Program is to identify, measure, monitor, and control the risks associated with TSPs
- This program establishes the authority, basis, and platform for the development, communication, implementation, interpretation, and enforcement of appropriate and applicable operating standards and procedures to manage vendors

FORVIS

Vendor Management Program

So, who is responsible for a Vendor Management Program?

- Board of Directors?
- Chief Executive Officer?
- Compliance Officer?
- General Counsel?
- Chief Information Officer?

FORVIS

Vendor Management Program

- Each member of the organization plays a vital role in helping to ensure controls at vendors are properly implemented, managed, and monitored
- This matrix responsibility stems from senior leadership of a company, providing direction and oversight, all the way down to individual users of the vendor's services that interact with the vendor on a day-to-day basis

FORVIS

Considerations for an Effective Vendor Management Program

- Enforcement of a mandatory due diligence process
- Compliance with laws and regulations
- Review of contracts
- Engagement of Subject Matter Experts within the company (For example, for a TSP with which you will be sharing information assets, the Chief Information Officer and/or the CIO's team members should be engaged)
- Continuous and ongoing evaluation and monitoring through audits, surveys, questionnaires, and dedicated third-party risk management software solutions

FORVIS

Vendor Management Program and Trust

- The purpose of a Vendor Management Program is to evaluate and objectively quantify risk and trust of each vendor within the company's ecosystem
- It all circles back to trust—trust in the services TSPs provide

FORVIS

Building Trust

- As a result of an increased focus on Vendor Management across all industries, TSPs are now faced with addressing vendor security questionnaires that sometimes contain more than 165+ questions and reporting on multiple regulatory and compliance frameworks (HIPAA, ISO, HITRUST, GDPR, NIST, PCI, etc.)
- Establishing a systematic approach to identifying reporting requirements can reduce internal team members having to constantly draft responses to vendor management questionnaires

With so many clients and prospects and with the focus on due diligence continuously increasing, how are TSPs going to do this exactly?

FORVIS

Building Trust

- Before TSPs can communicate trust to clients and prospects, they need to be able to trust themselves, something that is attained via the virtue of a strong control environment
- Preparing for reporting on compliance begins with senior leadership
- By identifying reporting on controls as a strategic initiative to help build customer and prospective customer trust, TSPs are afforded the ability to prepare, assess, and report on controls in a timely and efficient manner

FORVIS

Building Trust

- **Preparation** and engaging the right experts is key, as there are a multitude of vehicles for communicating and demonstrating trust in a TSP's services, and each vehicle has various complexities associated when it comes to compliance requirements
- The first step in building a program to demonstrate trust is to perform a **readiness assessment** – identify what reporting framework or frameworks you want to use, who the intended users are, what they care about, what existing controls you have, what controls you need, and where you can improve
- By performing a readiness assessment, the TSP gains the confidence to pursue the appropriate level of reporting without unwanted surprises

FORVIS

Building Trust

- Readiness assessments can take many forms but often consider internal controls, compliance with regulatory requirements, data retention and disposal, access rights, and insurance
- To obtain the most from a readiness assessment exercise, SMEs in all departments within an organization should be engaged
- Timelines for readiness assessments can vary from two weeks to years depending on the compliance requirements and gaps identified during the readiness assessment

FORVIS

Reporting Vehicles

- There are various types of compliance reporting vehicles for TSPs
- Some of the most common are:
  - AICPA's SOC 1, SOC 2, SOC 3 Reports
  - HITRUST Alliance's bC Verified Self-Assessment, i1 Validated Assessment, r2 Validated Assessment
  - ISO 27001 Compliance Report

FORVIS

AICPA's SOC 1, SOC 2, and SOC 3

- SOC 1 Reports: Reporting on an examination of controls at a service organization relevant to user entities' internal controls over financial reporting
- SOC 2 Reports: Reporting on an examination of controls at a service organization relevant to Security, Availability, Processing Integrity, Confidentiality, and/or Privacy
- SOC 3 Reports: Short-form version of a SOC 2 report intended for general use (no distribution restrictions)

FORVIS

SOC Report Comparison

	Intended Users	Why	What
SOC 1	Users of the system and their financial statement auditors	Audits of financial statements	Controls relevant to users' financial reporting
SOC 2	Management, Regulators, and Others	GRC programs oversight due diligence	Concerns regarding security, availability, processing integrity, confidentiality, and/or privacy
SOC 3	Any users with need for confidence in a service organization's controls	Marketing purposes, detail not needed	Easy-to-read report on controls

FORVIS

Two Types of SOC 1 and SOC 2 Reports

- Type 1 – report on the fairness of the presentation of management's description of the service organization's system and the suitability of the design of the controls to achieve the related control objectives included within the description as of a specified date
- Type 2 – report on the fairness of the presentation of management's description of the service organization's system and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives included within the description throughout a specified period

FORVIS

HITRUST Alliance's HITRUST Assessments

HITRUST Readiness Assessment

- A Readiness Assessment helps organizations prepare for HITRUST compliance.
- Results of Readiness Assessments are intended for management only.
- Readiness Assessments can be performed for e1, i1, and r2.

HITRUST Essentials, 1-Year (e1) Assessment *Essentials*

- The e1 is an "entry-level" assessment.
- The e1 has only 44 requirement statements and is not tailorable.
- The e1 is designed to provide entry-level assurance focused on the most critical cybersecurity controls and demonstrates that essential cybersecurity hygiene is in place.
- Results can be shared externally.

HITRUST Implemented, 1-Year (i1) Validated Assessment

- The i1 is a "best practices" assessment recommended for situations that present moderate risk.
- The i1 has 182 requirement statements and is not tailorable.
- The i1 is designed to provide higher levels of transparency, integrity, and reliability over existing moderate assurance reports, with comparable levels of time, effort, and cost.
- Results can be shared externally.

HITRUST Risk-Based, 2-Year (r2) Validated Assessment

- Formerly named the HITRUST CSF Validated Assessment, the r2 remains the industry gold standard as a risk-based and tailorable assessment that continues to provide the highest level of assurance for situations with greater risk exposure due to data volumes, regulatory compliance, and/or other risk factors.
- This assessment averages 375 requirement statements but is tailorable.
- HITRUST r2 Interim and Bridge Assessments are also available.
- Results can be shared externally.

FORVIS

HITRUST Alliance's HITRUST Assessments

- HITRUST CSF is the common security framework developed by the HITRUST Alliance that has been adopted by the healthcare industry as the compliance standard for demonstrating HIPAA compliance
- The HITRUST CSF rationalizes relevant regulations and standards, such as ISO 27001, NIST 800-53, 800-171, HIPAA, and GDPR, into a single overarching security and privacy framework

FORV/S

ISO 27001 Certification

- Organizations operating at an international scale are faced with a unique challenge associated with information security and privacy assurance
- ISO/IEC 27001 and ISO/IEC 27002 are the main ISO standards that provide organizations with the opportunity to enhance their information security
- ISO/IEC 27001 is primarily a framework to assist organizations in managing information security, while ISO/IEC 27002 specifies implementation guidance for information security controls specified within ISO/IEC 27001

FORVIS

Stages of ISO 27001 Audits

- Stage 1 Audit – “documentation” review: auditor will review your processes and policies to establish whether they are in line with the requirements of ISO 27001, and these reviews are intended for internal/management’s use only and help an organization assess readiness
- Stage 2 Audit – “certification” audit: auditor will conduct a thorough assessment of an organization’s ISMS and whether or not it complies with ISO 27001 requirements and then, following approval from a Certification Body, an ISO 27001 report intended for external user consumption is issued

FORVIS

Post-Readiness Assessment

- After the readiness assessment is complete and gaps in compliance are remediated, the company is now prepared to undergo certification, validation, and/or examination by a third-party assessor
- Third-party certification, validation, and/or examination provides customers with a window into the interworking of TSPs, including operations and compliance, and is one of the best vehicles for establishing and maintaining trust

FORVIS

Post-Readiness Assessment

- These assessments are performed by an independent party instead of management's own Internal Audit Department to help provide a more objective view of internal controls and protections in place to mitigate risks
- Certification and recertification cycles can be determined between the company and assessor based on customer and prospective customer requirements

FORVIS

Value of Third-Party Assessments

- Delivers service providers' users with information on the internal control environment, including the operating effectiveness of controls affecting the users' internal controls over financial reporting
- Addresses a service provider's users' need to understand the internal controls at the service provider related to security, availability, processing integrity, confidentiality, and/or privacy
- Aids the service provider's users' financial statement auditors in determining reliance on controls in place at the service provider
- Eliminates the need for multiple customers to perform onsite audits

FORVIS

Value of Third-Party Assessments (Continued)

- Satisfies a requirement by many companies that an audit of internal controls be in place at their service provider
- Indicates to potential customers a service provider's commitment to internal controls and transaction processing integrity
- Identifies improvement opportunities in operational areas at the service provider
- Provides an additional marketing opportunity and competitive advantage over other service providers

FORVIS

Conclusion

- By obtaining reports such as the AICPA's SOC 1 or SOC 2 report, a HITRUST report, and/or an ISO 27001 compliance report, TSPs can report on controls in an efficient and effective manner
- Select RFIs and RFPs require TSPs to outline how they plan to secure data they may obtain, transmit, and/or store on behalf of their customers; third-party assessments reduce that barrier to entry and provide for upstream and strategic growth
- The value proposition associated with reporting on controls is clear: by reducing internal team members' time responding to customer and prospect requests and concerns, TSPs can focus on internal operations and growth

FORVIS

FORVIS Can Help!

WEBINAR

- FORVIS has a dedicated team that focuses solely on helping third-party providers build trust with their clients and prospects through compliance reporting vehicles such as SOC, HITRUST, ISO 27001, and NIST day in, day out
- Transparent, proven methodologies
- Innovative technology and tools that drive more efficient and effective engagements
- Quality and creditability you can trust
- Future-focused approach

FORVIS

WEBINAR

Questions?

forvis.com

FORVIS

Assurance / Tax / Advisory

CONTINUING PROFESSIONAL EDUCATION (CPE) CREDIT

WEBINAR

FORVIS, LLP is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors. State boards of accountancy have final authority on the acceptance of individual courses for CPE credit. Complaints regarding registered sponsors may be submitted to the National Registry of CPE Sponsors through its website: www.nasbaregistry.org

FORVIS

CPE CREDIT

WEBINAR

- CPE credit may be awarded upon verification of participant attendance
- For questions, concerns, or comments regarding CPE credit, please email FORVIS at cpecompliance@forvis.com

FORVIS

WEBINAR

Thank you!

forvis.com

FORVIS

Assurance / Tax / Advisory