FORVIS

# Protecting Your Data: Cybersecurity, Third-Party Risk Management, and SOC Reports

November 8, 2022

# TO RECEIVE CPE CREDIT

- **Individuals**
  - Participate in entire webinar
  - Answer polls when they are provided
- **Groups**
  - Group leader is the person who registered and logged on to the webinar
  - Answer polls when they are provided
  - Complete group attendance form
  - Group leader sign bottom of form
  - Submit group attendance form to cpecompliance@forvis.com within 24 hours of webinar
- If all eligibility requirements are met, each participant will be emailed their CPE certificate within 15 business days of webinar

FORVIS

# Meet the Presenters

**Jennifer Jones**
National Practice Leader, SOC and HITRUST

919.610.4658
Jennifer.Jones@forvis.com

**Ryan Boggs**
Principal, SOC and HITRUST

828.989.3176
Ryan.Boggs@forvis.com

FORVIS

# Agenda

- Introductions
- Cybersecurity Update
- Third-Party Risk and Internal Controls
- SOC Suite of Services
- How to Read and Evaluate a SOC Report
- Closing

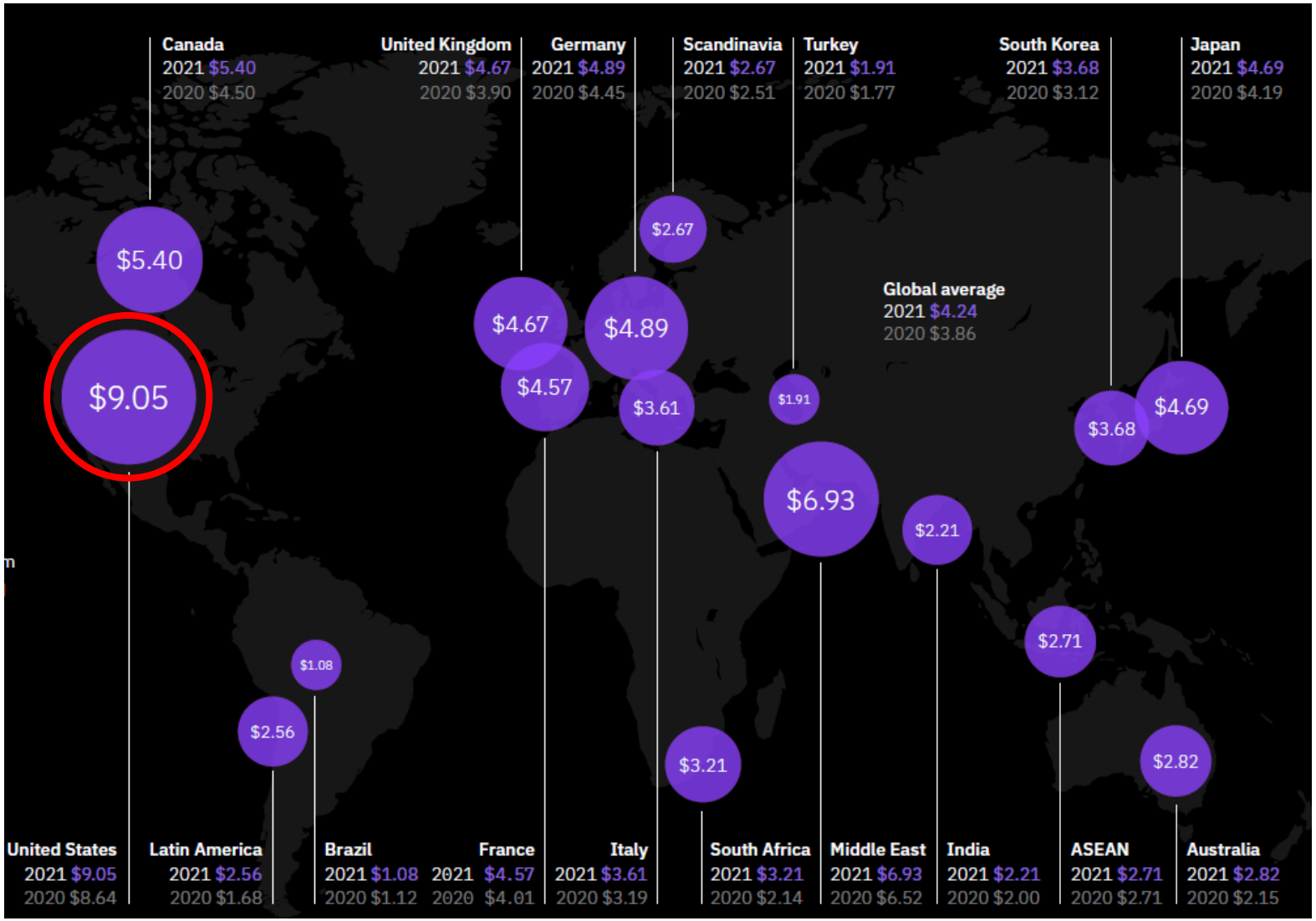
# 2022 Updates

- Revisions to NAIC Models 670 (2022) and 672 (2023)
- State Adoptions of Model 668 – Safe Harbors
- Comprehensive Privacy Laws (CA, CO, VA, CT, UT)
- Strengthening American Cybersecurity Act of 2022
- Cyber Incident Reporting for Critical Infrastructure Act of 2022 – 2024
- SEC Proposed Rule of Cybersecurity Risk Management
- HIPAA Privacy Rule Amendments
- The America Data Privacy and Protection Act (ADPPA)

FORVIS

# Breach Costs are up:

The U.S. leads the total cost of data breaches for the 11th year in a row.

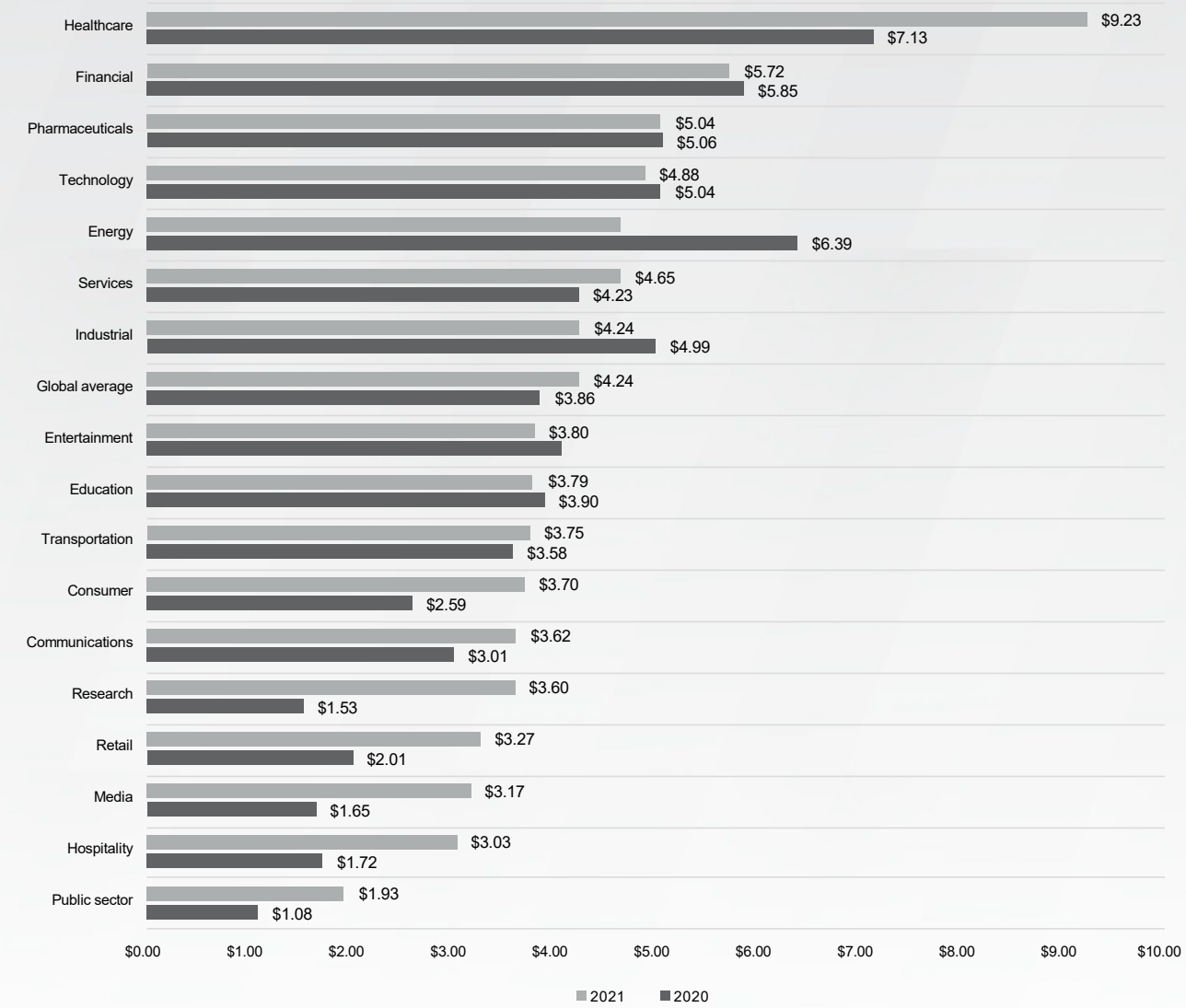



2021 Cost of a Data Breach Report – Ponemon Institute, IBM Security

Figure 4

# Average Total Cost of a Data Breach by Industry

Measured in US$ millions




## Healthcare $9.23m

UP from $7.13m

A 29.5% increase

## 11

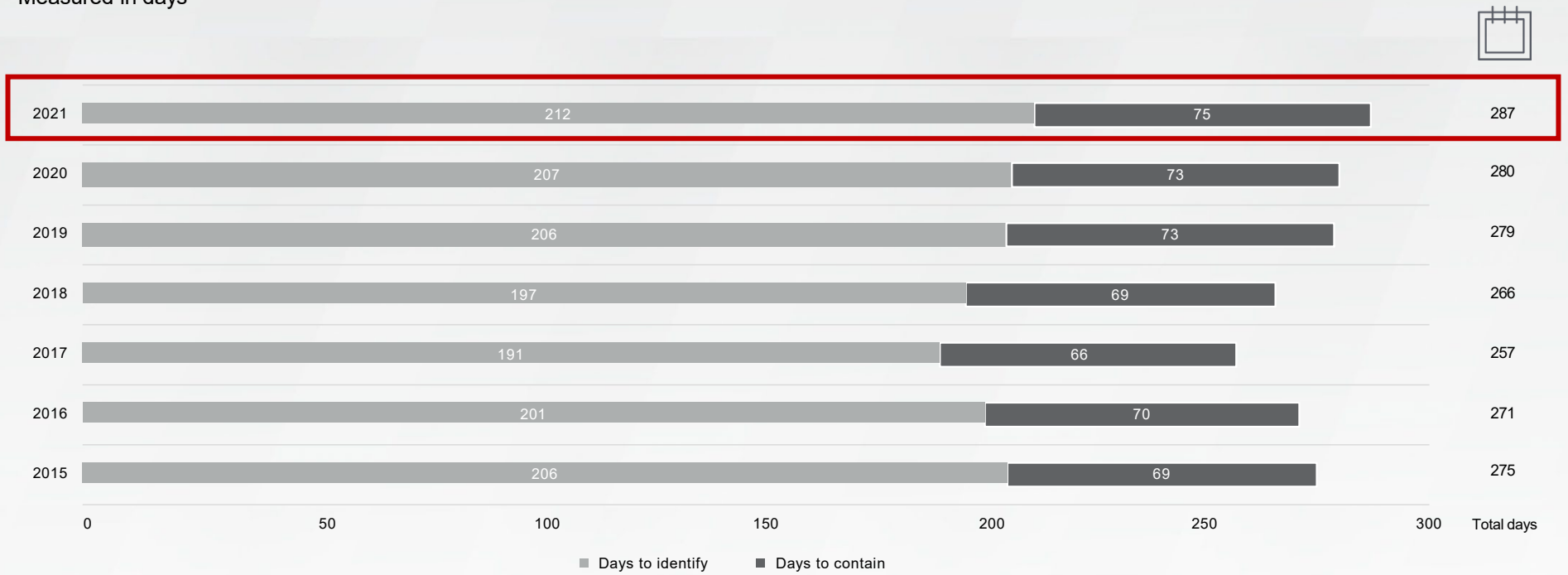
Consecutive years Healthcare had the highest industry cost of a breach

FORVIS

# Average Time to Detect a Breach in the U.S.

## Average Time to Identify and Contain a Data Breach

Measured in days




FORVIS

# Single Biggest Risk? Users

## Importance of Awareness Training

**Users** – Your own employees:  an estimated 65% of breaches are caused by an organization's users.

C-level executives are 12 times more likely to be the target of social engineering attacks.

Are ALL employees/contractors required to complete information security training?

FORVIS

# Ransomware Attack

**Your personal files are encrypted**

You have 5 days to submit the payment!!!

To retrieve the private key, you need to pay

Your files will be lost

FORVIS

# Risk Assessments
# The Value of Your Data to You

- Daily business operations rely on data that may not be deemed critical.
- Part of evaluating risk is maintaining data classification assessments.
- **You ARE a target!**
- NOTE: Global meat processor paid ransom of $11m.

$4.62m

Average total cost of a ransomware breach

FORVIS

# What are the 10 Best Practices?

1. Email Protection Systems
2. Endpoint Protection Systems
3. Access Management
4. Data Protection and Loss Prevention
5. Asset Management
6. Network Management
7. Vulnerability Management
8. Incident Response
9. Device Security
10. Cybersecurity Policies

Source: https://www.phe.gov/Preparedness/planning/405d/Documents/HICP-Main-508.pdf

FORV/S

# Cybersecurity Insurance

- Policy applications are more detailed than before
  - Incorrect statements on the application can lead to denied or reduced claim payouts
- Multifactor authentication requirements
  - Applications are being denied or will have higher deductibles if MFA is not in place
- Expect a forensics visit
  - Vital as they help close the gaps that permitted the breach, but they also reveal weak controls
- One of the top 5 reasons for nonpayment
  - Failing to require or complete information security training

**Poor control environments may reduce claim payouts**

FORVIS

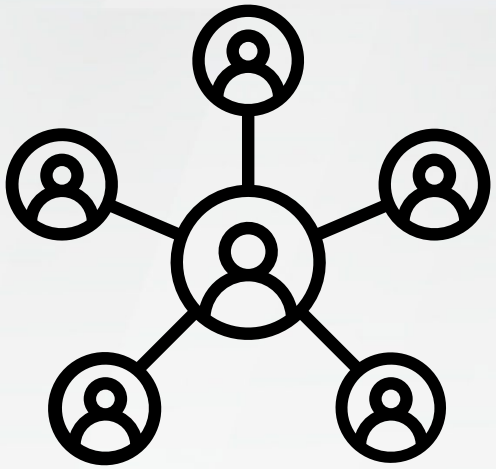
# Third-Party Risk and Internal Controls

- 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.
- Some examples in your own control environment may include claims processing software, Data Center hosting providers, hosted General Ledger applications, and/or other software-as-a-service solutions.

FORVIS

# Third-Party Risk and Internal Controls

- **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 related to the use of third parties (sometimes referred to as vendors, suppliers, partners, contractors, or service providers).



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 (Continued)

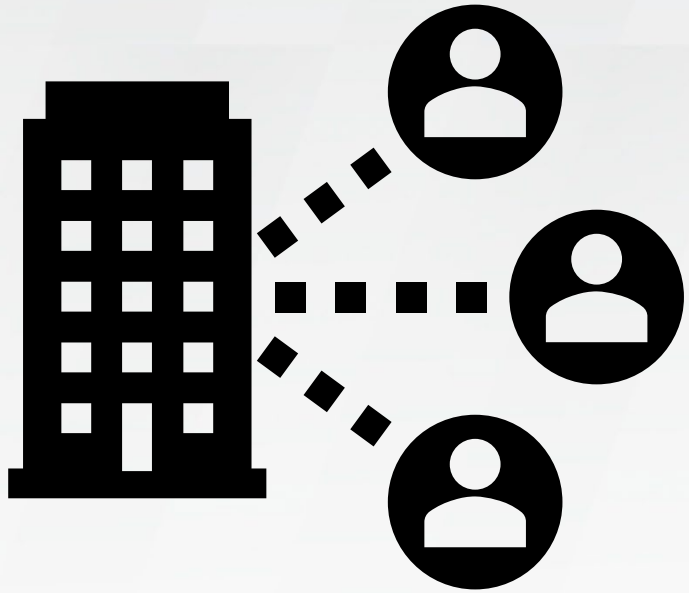
So, who is responsible for a Vendor Management Program?

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

FORVIS

# Vendor Management Program (Continued)

- 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

# Vendor Management Program – Key Risk Summary

- This table summarizes the key third-party risks for which companies should plan to protect the interests of their clients, employees, and the overall health of their operations.
- These risks may contribute to operational and reputational harm, with a potential for Significant Revenue Impact, if not handled properly.

| Third Party Risks | |
|---|---|
| Information Security/Data Privacy | Third party has insufficient experience and controls to protect the company's customers' information from unauthorized access, disclosure, modification, or destruction |
| Business Continuity | Third party cannot continuously maintain its services due to business disruption (e.g. ineffective redundancy procedures) |
| Financial Viability | Third party is not financially secure to continue to provide services at acceptable levels |
| Country/Credit | Ineffective oversight of vendors or civil unrest |
| Contract Compliance | Third-party's policies and procedures for products not consistent with users' policies |
| Legal/Regulatory | Third party does not possess necessary licenses to operate and remain compliant with domestic and international laws, if applicable |

FORVIS

# How to Manage Risk

- Evaluate vendors based on risk to the company
  - What data is held?
  - How critical is the application to operations (availability)?
  - Number of users?
- Based on evaluation, perform monitoring procedures
  - Continuous monitoring
  - Annual vendor surveys and questionnaires
  - Evaluate compliance reports, such as **SOC reports**

FORVIS

# How to Manage Vendor Risk

- Pre-contract due diligence
  - Identify clear requirements during the Request For Proposal stage
  - Require vendor security questionnaire and/or compliance attestations that clearly identify how each vendor will store and manage data to be completed
  - Evaluate information provided
- Evaluate all vendors based on risk to the company at least annually
  - What data is held?
  - How critical is the application to operations (availability)?
  - Number of users?
- Based on evaluation, perform monitoring procedures
  - Continuous monitoring
  - Annual vendor surveys and questionnaires
  - Evaluate compliance reports, such as **SOC reports**

FORVIS

# What are SOC Reports?

- System and Organization Controls (SOC) for Service Organizations
  - SOC for Service Organizations Reports are internal control reports on the services provided by a service organization providing valuable information that users need to assess and address risks associated with an outsourced service.
- Why SOC Reporting?
  - As more and more companies use third-party service providers, there is more demand for a detailed understanding of the processes and controls of these third-party service providers (referred to as service organizations).
  - Service organizations need to show their customers (referred to as user organizations) or prospective customers what processes and controls they have in place around internal controls over financial reporting and/or information security controls around the systems or services they provide.

### For CPAs

Provides information to user auditors and service auditors on understanding and performing SOC for Service Organizations Reports

### For Users & User Entities

Provides information to user entities on how to mitigate the risks associated with outsourcing services

### For Service Organizations

Provides information to service organizations that they can use to build trust and confidence in their systems

FORVIS

# SOC Suite of Services

## SOC 1

These attestation reports are specifically intended to meet the needs of entities that use service organizations (user entities) as their financial statement auditors (user auditors) use these reports to help evaluate the effect of the controls at the service organization on the user entities' financial statements.

## SOC 2

These attestation reports are intended to meet the needs of a broad range of users that need assurance about a service organization's controls as they relate to the security, availability, and processing integrity of the systems the service organization uses to process its users' data and the confidentiality and privacy of the information processed by those systems.

## General Examination

These attestation reports are reports on which the Service Auditor issues an opinion about whether a subject matter is in accordance with (or based on) the criteria or the assertion is fairly stated, in all material respects. This type of report is highly customizable to whatever a service organization's needs may be and is intended to provide a service organization's user entities with reasonable assurance over a subject matter.

## SOC 3

SOC 3 reports are designed to meet the needs of users who need assurance about the controls at a service organization relevant to security, availability, processing integrity, confidentiality, and/or privacy but do not have the need for or the knowledge necessary to make effective use of a SOC 2® Report. Since they are general use reports, SOC 3® reports can be freely distributed.

## SOC for Cybersecurity

The AICPA's cybersecurity risk management reporting framework helps organizations communicate about the effectiveness of their cybersecurity risk management programs.

FORVIS

# SOC Reporting Basics

| | SOC 1 | SOC 2 |
|---|---|---|
| **What is Covered by the Report?** | Controls related to financial reporting for user organizations | Controls relevant to security, availability, confidentiality, processing integrity, and/or privacy |
| **Intended Audience** | Auditors and management of user organizations (“auditor to auditor communication”) | Auditors, stakeholders (e.g., management, business partners, customers), regulators |
| **Report Format** | Long form which includes a detailed description of the system and controls | Long form which includes a detailed description of the system and controls |

- SOC 1 and SOC 2 reports are the most common and most useful for vendor risk management purposes.

FORVIS

# SOC Reporting Basics – Key Terms

- **Service Organization or Service Provider**
  - Organization providing the outsourced service
- **Subservice Organization**
  - Organization used by the service organization to provide third-party services to the service organization
- **User Organization or User Entity**
  - Organization receiving the outsourced service
- **Service Auditor**
  - Auditor performing SOC examination of the service organization's controls
- **User Auditors**
  - External auditors of the user organization/entity

FORVIS

# SOC Reporting Basics – Key Terms (Continued)

- **Type 1**
  - Not to be confused with a SOC 1, a Type 1 report signifies that the report is only as of a specific point in time
  - This type of report includes design and implementation but does not include operating effectiveness of controls
  - Example: SOC 1 Type 1 or SOC 2 Type 1
- **Type 2**
  - Not to be confused with a SOC 2, a Type 2 report signifies that the report covers the operations of controls over a specified period of time
  - This type of report includes design, implementation, and operating effectiveness of controls
  - Example: SOC 1 Type 2 or SOC 2 Type 2

FORVIS

# How to Evaluate a SOC Report – Initial Questions

- **User to Service Provider(s)**
  - What does the User (the company) outsource and to whom?
  - How does that compare to the scope of the SOC 1 report(s) received from those Service Providers?
    - Nature/type of services
    - Applications covered/not covered
    - Geographies/processing centers covered/not covered
- **Subservice Organization to Service Provider**
  - Is there anything that the Service Provider outsources to a third party?
  - If so, how is this handled in the opinion?

FORVIS

# How to Evaluate a SOC Report – Anatomy

- **Section 1: Report of Independent Service Auditors**
  - The "opinion"
- **Section 2: Management's Written Assertion**
  - May also include a subservice organization's assertion
- **Section 3: Management's Description of the System**
  - Provided by the service organization to describe the overall control environment and the control objectives and control activities related to the system being examined
- **Section 4: Control Objectives and Control Activities**
  - Independent Service Auditor's tests of controls and results of those tests included in a Type II
- **Section 5 (optional): Supplemental Material Provided by the Service Organization**

FORVIS

# How to Evaluate a SOC Report - What to Look For

- **Section 1: Report of Independent Service Auditors**
  - Was the auditor's opinion qualified or not? If qualified, why was it qualified?
- **Section 2: Management's Written Assertion**
  - This section generally contains the same information as the opinion
- **Section 3: Management's Description of the System**
  - Review the scope of description to identify systems and applications covered
  - Evaluate subservice organizations and potentially obtain SOC reports for any significant subservice organizations relevant to financial reporting
  - Evaluate complementary user entity controls and verify these controls are within your environment
- **Section 4: Control Objectives and Control Activities**
  - This section includes tests and results, important to identify any issues noted by the Service Auditor and how they might impact your own control environment
  - Important to evaluate whether or not tests are sufficient for your needs – Inquiry alone is never sufficient
- **Section 5: Optional Section (May include management's responses to testing exceptions)**
  - Management can provide responses to testing exceptions here, which can be useful in determining impact to your own control environment

FORVIS

# FORVIS SOC and HITRUST

- **FORVIS can help with SOC Reporting needs!**
  - FORVIS has a **dedicated team** that focuses only 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 credibility** you can trust
  - **Future-focused** approach

As a user, if you come across third parties from which you have asked for a SOC report and they don't have one, feel free to refer us!

FORVIS

# CONTINUING PROFESSIONAL EDUCATION (CPE) CREDIT

**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

- 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

# Thank you!

forvis.com



FORVIS

Assurance / Tax / Advisory