



SCHNEIDER DOWNS

Big Thinking. Personal Focus.



# SOC Reporting “*Master Class*”

*April 11, 2024*



# Discussion Points

Big Thinking. Personal Focus

- Common SOC mistakes and misconceptions
- Best practices for audit evidence and documentation
- Secrets of how we design and test controls
- Steps to achieve and maintain compliance, and how to hold vendors accountable
- PRO tips for simplifying SOC and the security circus.





**Bill Deller CISA, CTPRP, CTPRA, CCSFP**  
Shareholder– IT Risk Advisory  
*Cybersecurity Governance, Risk and Compliance*  
412.697.5256  
wdeller@schneiderdowns.com

- Practice Leader - Schneider Downs Consulting practice for Cybersecurity GRC, with a focus on TPRM, SOC, HITRUST, and HIPAA
- Experience designing, managing, augmenting, and executing as part of Third Party Risk Management (TPRM) programs for Global-Systemically Important Banks (G-SIBs), Big Healthcare/Pharma, Higher Educational institutions, Power & Utility companies, and across other industries.
- Past President of the ISACA Pittsburgh Chapter, leading their mission of providing continuous education and promoting/elevating IT audit, control, and security careers.

# Introduction

Big Thinking. Personal Focus.

# How we help our clients



## Third Party Risk Management

- » is the process of identifying, assessing and controlling these and other **risks** presented throughout the lifecycle of your relationships with **third-parties**.
- » This often starts during procurement and extends all the way through the end of the offboarding process.

# SOC 101 - Report Differences and “Types”

**SOC 1 Report** – Assists customers’ financial statement auditors with evaluating how your services and controls affect their financial statements (Restricted Use Report)

Payroll providers

Mortgage services providers

**SOC 2 Report** – Provides customers with assurance about the controls implemented by an outsourced provider with regards to security, availability, confidentiality, processing integrity and/or privacy (Restricted Use Report)

Cloud computing providers (IaaS, PaaS, SaaS)

IT managed services providers

**SOC 3 Report** – Same purpose as SOC 2, however, can be freely distributed

Will not contain detailed information on controls and results of CPA’s control testing

**Type 1** - Report on the fairness of the presentation of management’s description of the system and the **suitability of the design of the controls**

**Type 2** - Report on the fairness of the presentation of management’s description of the system and the **suitability of the design and operating effectiveness of the controls**

# SOC 101 - Opinions

- Unqualified - All the subject matter meets the criteria;
- Qualified - There are material misstatements (not pervasive) in the system description and/or material deficiencies (not pervasive) in the design and/or operating effectiveness of controls, resulting in the failure of controls to meet a few of the applicable trust services criteria;
- Adverse - There are pervasive misstatements throughout the description and/or pervasive deficiencies in the design and/or operating effectiveness of controls, resulting in the failure of controls to meet most of the applicable trust services criteria.
- Disclaimer - When the service auditor is unable to obtain sufficient appropriate evidence on which to base the opinion and the service auditor concludes that the possible effects on the subject matters of undetected misstatements, if any, could be both material and pervasive.

Opinions and determining if deficiencies are material or pervasive are subject to the professional judgment of the CPA firm. You can have control deficiencies and still receive an unqualified opinion.

# SOC 101 – SOC vs other standards-based assessments

SOC 2 Attestation	ISO 27001/2 Certification	PCI-DSS Certification	HITRUST Certification	CMMC Certification
is a compliance standard for service organizations, developed by the American Institute of CPAs (AICPA), which specifies how organizations should manage customer data.	is an international standard on how to manage information security.	is a set of security standards designed to ensure that all companies that accept, process, store or transmit credit card information maintain a secure environment.	is a certifiable security framework that scales according to the type, size, and regulatory requirements of an organization and its systems.	is a unified standard for implementing cybersecurity across the defense industrial base (DIB).

# Standards-based assessment comparison – Definition

SOC 2 Attestation	ISO 27001/2 Certification	PCI-DSS Certification	HITRUST Certification	CMMC Certification
is a compliance standard for service organizations, developed by the American Institute of CPAs (AICPA), which specifies how organizations should manage customer data.	is an international standard on how to manage information security.	is a set of security standards designed to ensure that all companies that accept, process, store or transmit credit card information maintain a secure environment.	is a certifiable security framework that scales according to the type, size, and regulatory requirements of an organization and its systems.	is a unified standard for implementing cybersecurity across the defense industrial base (DIB).



# Standards-based assessment comparison – Geographical applicability

SOC 2 Attestation	ISO 27001/2 Certification	PCI-DSS Certification	HITRUST Certification	CMMC Certification
Most common the United States, but growing globally.	Less common in the United States, but still an international standard	International	United States	United States

# Standards-based assessment comparison – What’s audited

SOC 2 Attestation	ISO 27001/2 Certification	PCI-DSS Certification	HITRUST Certification	CMMC Certification
Design of controls at a point in time (Type 1) or the design and operating effectiveness of controls over a period of time (Type 2)	The design (Stage 1) and operating effectiveness (Stage 2) of your ISMS at a point in time	The design and operating effectiveness of control requirements at a point in time	The design and operating effectiveness of control requirements at a point in time	The design and operating effectiveness of control requirements at a point in time

# Standards-based assessment comparison – Who should obtain it?

SOC 2 Attestation	ISO 27001/2 Certification	PCI-DSS Certification	HITRUST Certification	CMMC Certification
Service organizations that want to provide customers/prospects with independent and objective assurance of their control design/operating effectiveness	Service organizations that want to provide customers/prospects with independent and objective assurance of their control design/operating effectiveness	Any merchant processing 20,000 to 1M Visa e-commerce transactions per year	Payers and subcontractors for major healthcare organizations	Prime contractors and subcontractors working for the DoD

# Standards-based assessment comparison – Timeline and Cost

SOC 2 Attestation	ISO 27001/2 Certification	PCI-DSS Certification	HITRUST Certification	CMMC Certification
3-12 months + 1-3 months to issue report	6-24 months	6-12 months	3-9 months	9-24 months
\$15K - \$100K+	\$15K - \$100K+	\$15K - \$100K+	\$50K - \$300K+	\$50K - \$300K+

# Standards-based assessment comparison – Controls/Requirements

SOC 2 Attestation	ISO 27001/2 Certification	PCI-DSS Certification	HITRUST Certification	CMMC Certification
60-100 controls to satisfy 35 trust services criteria	7 requirements (clauses 4 through 10 in the ISO 27001 standard) with 114 suggested controls	12 overall standards, with varying levels of requirements based on the merchant type/level	CSF consists of 19 control domains i1 assessment: 219 control requirements r2 assessment: 198-2000 control requirements	17 domains, with varying levels of requirements based on the CMMC maturity level



# Standards-based assessment comparison – Accreditation Body

SOC 2 Attestation	ISO 27001/2 Certification	PCI-DSS Certification	HITRUST Certification	CMMC Certification
U.S. CPA firms must be registered with the AICPA's Peer Review National Program in order to perform SOC 2 attestations	ANAB (ANSI National Accreditation Board) and the International Accreditation Service (IAS) are the two accreditation bodies in the US	PCI Security Standards Council	HITRUST Alliance	CMMC Accreditation Body (CMMC-AB)

# Standards-based assessment comparison – Auditor

SOC 2 Attestation	ISO 27001/2 Certification	PCI-DSS Certification	HITRUST Certification	CMMC Certification
CPA Firm	ISO 27001 Certified Assessor	Assessor, or QSA, or a PCI Security Standards Council Internal Security Assessor, or ISA, must perform an annual PCI DSS assessment	HITRUST Certified Assessor	C3PAO

# Standards-based assessment comparison – Result of Audit

SOC 2 Attestation	ISO 27001/2 Certification	PCI-DSS Certification	HITRUST Certification	CMMC Certification
Report and opinion on the design and/or operating effectiveness of controls	Audit report provided to the organizations and a certificate based on a Pass/Fail	Report on Compliance (ROC) and a certificate based on a Pass/Fail	Audit report provided to the organizations and a certificate based on a Pass/Fail	Audit report provided to the organizations and a certificate based on a Pass/Fail

# Standards-based assessment comparison – Expiration

SOC 2 Attestation	ISO 27001/2 Certification	PCI-DSS Certification	HITRUST Certification	CMMC Certification
SOC 2 logos expire 12 months after the issuance of the report	Recertification occurs every 3 years, but there are surveillance audits after year 1 and year 2 in between the recert	1 year from the date the certificate is issued	i1 assessment: 12 months r2 assessment: 24 months (with an interim assessment within 12 months)	3 years from the date the certificate is issued

# Standards-based assessment comparison – Frequency of Audit

SOC 2 Attestation	ISO 27001/2 Certification	PCI-DSS Certification	HITRUST Certification	CMMC Certification
Typically annual	Recertification audit every 3 years and surveillance audit (aka monitoring audit) annually between recertification audits	Annual	CSF consists of 19 domains i1 assessment: annual r2 assessment: biannual w/annual interim assessment	Every 3 years





# Discussion Points

Big Thinking. Personal Focus

- **Common SOC mistakes and misconceptions**
- Best practices for audit evidence and documentation
- Secrets of how we design and test controls
- Steps to achieve and maintain compliance, and how to hold vendors accountable
- PRO tips for simplifying SOC and the security circus.

# Knowledge Check – Spot the Lie

SOC 2 does not require MFA or penetration testing as controls.	Complementary subservice organization controls are only required if there are in-scope subservice organizations.	If a compliance automation platform “fails” a control, it’s not necessarily an exception in the SOC report.	Auditors do not want to find exceptions.
SOC 2 covers more than infrastructure and software controls.	Companies cannot use their vendor’s SOC 2 report as their own.	SOC reports do not provide a certification.	SOC 2 qualified opinions only apply to the specific criteria outlined in the opinion.
Exceptions remediated before the end of the audit period will still show as exceptions in the report.	SOC 2 Type 1 audits are not required to obtain a SOC 2 Type 2 report.	SOC audit testing periods can be 1 month.	SOC 2 Type 1 reports only test the design of controls.
Including the Privacy category in SOC 2 reports does not automatically prove GDPR compliance.	A SOC 2 report can be done in a few weeks.	SOC 2 Type 2 reports can have 5 exceptions and still not receive a qualified opinion.	SOC 2 is a reporting framework.
SOC 2 logo’s cannot be used 12 months after report issuance.	The points of focus are only a guideline and not a requirement.	All SOC audit firms are subject to the CPA peer review program.	SOC 2 is not specific to cloud service providers/customers (IaaS, PaaS, SaaS).

## Other SOC Misconceptions

- SOC 2 is only needed for marketing purposes
- More Trust Service Categories in a SOC 2 means more sales
- Exceptions result in qualified opinions
- SOC 2 reports are created equal
- The system description is not important
- Customers expect a perfect report
- Attestation standards tell auditors how to specifically perform their procedures
- A “clean” SOC report should make other standards-based assessments a breeze



# Discussion Points

Big Thinking. Personal Focus

- Common SOC mistakes and misconceptions
- **Best practices for audit evidence and documentation**
- Secrets of how we design and test controls
- Steps to achieve and maintain compliance, and how to hold vendors accountable
- PRO tips for simplifying SOC and the security circus.



## Accuracy and Relevance of Evidence

- Ensure evidence provided is within the audit period
- Observe the client generating any reports or ask client for screenshots (with timestamp) of the report parameters
- For population samples, we recommend using data no more than 30-45 days from the end of the testing period
- Point in Time Controls- Ensure that the date and time is displayed in screenshots



# Detailed Documentation of Audit Procedures

- Provide detailed and precise description of audit procedures performed, evidence obtained, and conclusions reached
- Sampling Completeness & Accuracy and Rationale
  - Completeness write up explains the source of the population and parameters used to generate the report. Additionally, there are WP references to show the completeness and accuracy.
  - Rationale indicates why the sample size was selected and explains the reasoning of why that size is appropriate.
- Documentation must support exceptions/issues discovered
- Audit work can be challenged / may be involved in potential litigation (content and wording is extremely important)

## Example of Sampling Documentation

CC1.4.3  
**Population Completeness**

On 4/17/2023, SD obtained the a current employee listing (WP 1.4.3a) from Rick Sanchez (Compliance Analyst) and determined the population to be complete and accurate. Specifically, we noted that the listing was generated directly from the HR management system and the parameters used indicated that "all" employees were included within the population (WP 1.4.3b).

CC1.4.3  
**Control Frequency**

Annually ▾

CC1.4.3  
**Control Risk Ranking**

Moderate ▾

CC1.4.3  
**Sampling Rationale**

Per SD SOC Sampling Methodology, a population that is between (25) and (200), coupled with a High risk ranking, utilizes a sample size that is the greater of (5) and (10%) of the total population. In this case, we chose a random sample size of (5), which is (17%) of the total population. See WP 1.4.3d for sample generation parameters and WP 1.4.3c for the sample generated using Fieldguide's sampling capability.

# Maintaining Independence

- It is critical that the auditor can assess an organization's controls and processes without bias or influence
- Avoiding conflicts of interest helps preserve the integrity of the audit process and enhances the credibility of the audit report
- The AICPA also has rules on maintaining independence
  - [AICPA's "Plain English guide to independence"](#)
    - **Independence of mind** is the state of mind that permits a member to perform an attest service without being affected by influences that compromise professional judgment, thereby allowing an individual to act with integrity and exercise objectivity and professional skepticism.
    - **Independence in appearance** is the avoidance of circumstances that would cause a reasonable and informed third party, who has knowledge of all relevant information, including safeguards applied, to reasonably conclude that the integrity, objectivity or professional skepticism of a firm or member of the attest engagement team is compromised.

Control management/ownership vs testing



# Discussion Points

Big Thinking. Personal Focus

- Common SOC mistakes and misconceptions
- Best practices for audit evidence and documentation
- **Secrets of how we design and test controls**
- Steps to achieve and maintain compliance, and how to hold vendors accountable
- PRO tips for simplifying SOC and the security circus.

# Secrets for Designing Controls

- Design controls according to the scope, with a risk-based approach
- Design controls to be questionnaire-compatible!
- Design controls at all 5 functions of security:
  - Identify
  - Prevent
  - Detect
  - Correct
  - Recover

# Secrets for Designing Controls

- When documenting controls, the details of the control must contain the following elements/attributes to evidence that the control is properly designed:
  - **What** is the purpose of the control/objectives to be realized (understand the difference between control objective and test objective)
  - **Who** (title, position, area, etc.) is responsible for executing the control
  - **How** does the mechanics of the control work / what are the executable tasks performed (include reports and other key information produced)
  - **When** is the control executed (timing / frequency)
  - **To whom** is information disseminated (reconciliations, management and exception reports, etc.) and/or what actions are taken to communicate/demonstrate the control was properly executed.



# Secrets for Designing Questionnaire-Compatible Controls- Example

Bad/Good examples of Password Control Activity

✘ Control Activity: The organization follows a strong password management configuration.

✔ Control Activity: The organization's password settings for the Network and Cloud Infrastructure are established to enforce the following:

- Passwords expire every 90 days
- Passwords must be at least 14 characters
- Complexity Requirements are enabled
- A user cannot reuse their last 6 passwords
- Account lockout after 3 invalid attempts
- Minimum password age is 3 days

# Secrets for Testing Controls

- Properly document test procedures and results
- Understand a failure/exception condition
  - Ask why to understand root cause
  - Does the explanation make sense
  - Understand the impact of the exception and remediation plans
- Document conclusion

## HOW MUCH DETAIL IS ENOUGH?

When you write procedures, focus on getting the job done – it should clearly establish the steps and concisely provide guidance to successfully complete the requirement.

The example below shows a good amount of detail that can serve as a handy reference for writing cybersecurity procedures.

### NOT ENOUGH

How to make a peanut butter and jelly sandwich

1. Put peanut butter on bread.
2. Put jelly on bread.
3. Eat.

Whoops!



VS

### JUST RIGHT

How to make a peanut butter and jelly sandwich

1. Place two (2) slices of bread on a plate.
2. Open the jar of peanut butter and use a butter knife to spread approximately two (2) tablespoons of peanut butter on one (1) slice of bread.
3. Open the jar of jelly and use a butter knife to spread approximately two (2) tablespoons of jelly on the other slice of bread.
4. Put the bread slices together with the peanut butter and jelly facing each other.
5. Take one (1) bite-sized portion, then chew and swallow.
6. Repeat Step 5 until sandwich is gone.

Yum!



# Secrets for Testing Controls

Difference between the Design and Operating Effectiveness

## Design Effectiveness

- Evaluates whether a control is appropriately structured and designed to achieve its intended objectives and effectively mitigate risks
- Focuses on the suitability of the control's design
- Point in time test
- Involves reviewing policies, procedures, documentation, etc., to determine if it aligns with control objectives

## Operating Effectiveness

- Assesses whether a control is functioning as intended and operating effectively to achieve its objectives on an ongoing basis
- Focuses on the performance and implementation of the control over a period of time
- Involves testing the performance of control activities through sample testing, inquiry, observation, etc
- Population completeness and procedures performed should be documented within each test script



# Discussion Points

Big Thinking. Personal Focus

- Common SOC mistakes and misconceptions
- Best practices for audit evidence and documentation
- Secrets of how we design and test controls
- **Steps to achieve and maintain compliance, and how to hold vendors accountable**
- PRO tips for simplifying SOC and the security circus.

# Steps to Achieve and Maintain Compliance

---

- Adjust scope based on planning meeting
- Update based on regular risk assessments
- Incorporate changes based on changing laws and regulations
- Maintain effective communication and collaboration with internal and external stakeholders
- Incorporate changes based on incoming questionnaires and client needs
- Testing period length and timing



# What are Compliance Automation Platforms?

---

- Built to help companies streamline the process of preparing for and maintaining controls associated with compliance frameworks
- SOC 2, ISO 27001, HIPAA, PCI, NIST
- Come with prebuilt control sets that companies check off.
- Facilitate compliance through integrations to cloud infrastructure, identity providers, HR systems and others that automatically check compliance with certain controls, policy templates, built in workflows like risk assessments, endpoint device monitoring agents, security awareness training.
- We currently partner with Hyperproof, Drata, and Tugboat Logic
- Other Considerations
  - Great for out-of-the-box compliance boost vs diminishing return in value/increasing costs
  - Their SOC 2 Type II Reports

# Where Do We Come in?

---

- Platforms help clients prepare but most rely on audit partnerships to refer their customers to companies like SD to complete the audits.
- Some companies have formed their own related audit firms in order to make a package deal – AICPA has not taken a formal stance, but there are significant risks from an independence perspective
- A significant risk to SD is over relying on the evidence provided by the platforms, in some cases we are relying on evidence not generated directly from the system being audited, so we need to take care to validate the completeness and accuracy of evidence produced by the automation platform.
- We take the approach of using information generated by the platforms to supplement our audit procedures. Our standard SOC 2 request list is 40 – 60% fulfilled by evidence generated from an automation platform. Our reliance varies greatly from platform to platform
- Audit firm selection

# How To Hold Vendors Accountable

---

- Ensure contractual agreements are:
  - comprehensive (roles and responsibilities, regulatory obligations, data protection requirements, etc.)
    - ABA templates
  - SMART (specific, measurable, achievable, relevant, and time-bound)
- Start with attestation and standards-based reports before adding your questionnaires
  - Push for 12-month report periods
  - Ask questions if there are any gaps in their report period
- Hold the vendor accountable to your organization's risk appetite!





# Discussion Points

Big Thinking. Personal Focus

- Common SOC mistakes and misconceptions
- Best practices for audit evidence and documentation
- Secrets of how we design and test controls
- Steps to achieve and maintain compliance, and how to hold vendors accountable
- **PRO tips for simplifying SOC and the security circus**

# How to Review SOC reports

---

- Issue Date – Was the report issued within the last 12 months or does it overlap with your audit period?
- Bridge Letter – If not does the bridge letter state no significant changes were made to the control environment since the report was last issued?
- Is the service auditor reputable?
- Period – does the period cover long enough to rely on the report?
- Categories – were any categories omitted that should have been included?
- Report Type – is it a type 1 (design) or type 2 (operating effectiveness)?
- Controls – were controls designed/operating effectively? Were there exceptions?
- Types of testing – inquiry, observation, OR inspection?

# How to review SOC reports cont.

- Opinion – was the opinion modified/qualified (same thing)? What remediation plans are in place and what add'l testing do we need to perform to obtain assurance?
- Scope – were the right services and locations tested as part of the report?
- Subservice organizations – which 4th parties were used and how do they impact your risk (CSOCs)?
- Complementary User Entity Controls (CUECs) – are there any controls you need to implement to ensure the service organizations controls are operating effectively?
- System description – Does it omit any significant information about the system or its operating environment(s)?
- <https://www.schneiderdowns.com/third-party-risk-management>
  - TPRM Resources
    - SOC Report Review Template
    - TPRM Policy / Charter Templates
    - Compliance and TPRM Guide with Framework Crosswalks

# Navigating the Security Circus

- Understand and appreciate the difference between an Assessment vs an Audit
- Attestations/certification are just one step in the TPRM assurance goal
- Invest 2:1 in relationships to software solution (internally/externally)
- Mindset shift to assume your vendor will be breached
  - Refocus on factors that actually reduce risk associated with using a third party
    - Can you protect your data from their breach (encryption)?
    - Can you protect your business operations from their breach (portability)?
    - Can you protect your prod environment from their breach (segmentation)?
    - Can you protect your tenant (hardening)?
    - Is their security enough (independently *audited* security)



# Thank You



SCHNEIDER DOWNS

Big Thinking. Personal Focus.

Working together every day to make our  
firm, clients and communities better.