DHG | IT advisory

Maintaining the SOC Environment During COVID-19

June 11, 2020

1

Today's Speakers

Ryan Boggs
Managing Director
DHG IT Advisory
ryan.boggs@dhg.com

Casey Grimes
Senior Associate
DHG IT Advisory
casey.grimes@dhg.com

DHG | IT advisory

2

2

Today's Agenda

- Basics of SOC Reporting
- Assessing the Impact
- Assessing Qualified Opinions
- Opportunities for Efficiency
- Q&A

DHG | IT advisory

3

3

Types of SOC Reports

- SOC 1: Report on Controls at a Service Organization Relevant to User Entities' Internal Control over Financial Reporting
- SOC 2: Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy
- SOC 3: Redacted SOC 2 – general use report
- SOC for Cybersecurity – cybersecurity risk management program

DHG | IT advisory

4

4

Types of SOC Reports

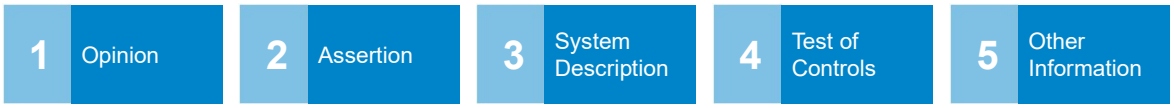
- Type 1: Point in time - design of the controls
- Type 2: Period of time - design and operating effectiveness of the controls
  - + 3 to 12 month period

DHG | IT advisory

5

5

Components of a SOC Report



DHG | IT advisory

6

6

DHG
DIXON HUGHES GOODMAN LLP

Polling Question 1

7

Assessing the Impact

- Work From Home (WFH) environment
- Unavailable staff
- Maintenance of processing
- Physical security
- Implementation of new technology and tools

DHG | IT advisory

8

8

Assessing the Impact

CHANGES TO CONTROLS	IMPACTED CONTROL AREAS
• Design • Frequency • Ownership • Type • Execution • Evidence	• Governance • Logical access • Monitoring • Management review • Information security • Business continuity

DHG | IT advisory

9

9

DHG
DIXON HUGHES GOODMAN LLP

Polling Question 2

10

Assessing the Impact - Responsibility

- Treat SOC reports like a project – Assign an owner!
- Ensure all controls have control owners
- Confirm controls with each control owner to assess impacts
- Ensure central repository for evidence

DHG | IT advisory

11

11

Assessing the Impact – System Description

- **Disclosure of significant changes that may be relevant to users**

- **Examples of significant changes:**
  - + Changes to the services provided
  - + Changes to IT and security personnel
  - + Changes to system processes
  - + Changes to legal and regulatory requirements
  - + Changes to organizational structure

DHG | IT advisory

12

12

System Description Example Elements

A. System Overview and Background
   i. Infrastructure
   ii. Software
   iii. People
   iv. Procedures
   v. Data
B. Customer Responsibilities
C. Relevant Aspects of the Control Environment, Risk Assessment Process, Information and Communication Systems, and Monitoring
D. Policies and Procedures
E. Communication
F. Physical Security
G. Logical Security
H. Monitoring

DHG | IT advisory

13

13

Assessing the Impact – Other Information

WHEN TO INCLUDE:

+ Significant changes between examination periods
+ Response to COVID-19 that doesn't impact description or controls
+ Deviation responses not audited by service provider

DHG | IT advisory

14

14

Assessing the Impact

- **Evaluate examination period – extended or modified**
  - + Requires Service Auditor to obtain reasonable justification

- **Changes to consider:**
  - + System description changes
  - + Control language changes
  - + Inherent risk changes
  - + Lack of evidence or different forms of evidence
  - + Deviations, deficiencies, or other matters

DHG | IT advisory

15

15

DHG
DIXON HUGHES GOODMAN LLP

Polling Question 3

16

Assessing the Impact – CUECs

- Controls that will be implemented by user entities to achieve the control objectives
- Assess changes to CUECs due to COVID-19
- Service organizations should ensure accuracy
- User entities must test CUECs if you rely on the SOC report

DHG | IT advisory

17

17

Example CUECs

SAMPLES:

+ User organizations are responsible for understanding and complying with their contractual obligations with Company.
+ User organizations are responsible for ensuring confidentiality of any user IDs, passwords, and encryption keys assigned to Company for accessing client data.
+ User organizations are responsible for immediately notifying Company of any actual or suspected information security breaches.
+ User organizations are responsible for performing annual user access reviews to Company services.

DHG | IT advisory

18

18

Complementary Subservice Organization Controls (CSOCs)

- **Controls that will be implemented by subservice organizations to achieve the control objectives**

- **Evaluate downstream controls through third party risk management**
  - + COVID-19 impacts
  - + New subservice organizations?

DHG | IT advisory

19

19

Assessing Qualified Opinions

- **What causes a qualified opinion?**

> Description > Design > Effectiveness

- **Qualified versus Adverse and Disclaimer opinions**

DHG | IT advisory

20

20

Assessing Qualified Opinions

SERVICE ORGANIZATION	USER ORGANIZATION
• Document mitigating controls • Provide response in Section Five • Communication with users • Bridge letters	• Document mitigating controls • Obtain remediation response • Obtain bridge letter • Request supporting evidence

DHG | IT advisory

21

21

DHG
DIXON HUGHES GOODMAN LLP

Polling Question 4

22

Opportunities for Efficiency

- Plan for remote testing
- Utilize technology
- Prepare for future outbreaks
- Communicate externally and internally

DHG | IT advisory

23

23

DHG
DIXON HUGHES GOODMAN LLP

Polling Question 5

24

Subscribe to Knowledge Share (KS)

Subscribe to receive relevant news, alerts & updates.

SUBSCRIBE

https://www.dhg.com/subscribe

DHG | IT advisory

25

25

DHG
DIXON HUGHES GOODMAN LLP

Q&A

Ryan.Boggs@dhg.com

Casey.Grimes@dhg.com

www.dhg.com/emergingstrong

26