Rules to Receive CPE Credit

By attending today's session, you are eligible to receive 1 CPE Credit per the following guidelines:

In order to receive this credit, the following items MUST be completed:

- ✓ Each person wishing to receive CPE Credit must log into the session individually with their credentials
- ✓ You MUST answer ALL of the polling questions throughout the presentation
- ✓ You MUST be in attendance for the entire live session
- ✓ You MUST complete the follow-up survey regarding the session

venminder

Virtual Vendor Due Diligence Site Visits

PRESENTED BY

Mike Morris

Partner
WIPFLI
mike.morris@wipfli.com
(404) 420-5669

Mary Beth Marchione

RAS Senior Manager
WIPFLI
marybeth.marchione@wipfli.com
(404) 548-2825

October 29, 2020

Session Agenda

1

What's happening in the industry

2

Understanding what site visits are (and what they are not)

3

When virtual site visits are appropriate (and necessary)

4

How to prepare, conduct and scope site visits virtually

5

Sample virtual site visit questions

venminder

What's Happening in the Industry

- COVID-19 has led to an increase in work-from-home environments
- Site visits will take place interactively at this moment in time; virtual site visits are an option
- Site visits will return

venminder

Vendor Site Visits – What They Are

- A supplement to your vendor due diligence
- Evaluation of risk for a given vendor
- Way to gain comfort in policy and practices
- Typically a point-in-time assessment

venminder

Vendor Site Visits – What They Are Not

- Absolute assurance
- Typically not designed for operating effectiveness
- Replacement for overall due diligence, insurance or audit reports

venminder

Poll Question

Is your organization currently performing site visits for key vendors?

a. Yes
b. No
c. Not sure

venminder

When Vendor Site Visits Are Appropriate

- Vendor **refuses** to provide due diligence documentation
- You are performing **initial due diligence** on a new vendor
- Vendor who is **not providing information annually**
- **Remediation** testing
- A vendor is **missing critical elements** of their due diligence packages
- The scope of audit reports received **does not cover processes/services outsourced** to the vendor

venminder

When Vendor Site Visits Are Appropriate

- There are **clear control gaps** in a vendor's SOC Report
- The SOC Report provided is a **Type 1 Report**
- The vendor only provides a subservice provider's **SOC Report**
- The vendor's SOC Report contains significant **issues/deficiencies**
- A vendor's financial condition is **deteriorating**

venminder

Poll Question

Does your organization ensure that 'right to audit' clauses are in each contract your organization executes?

a. Yes
b. No
d. Not sure

venminder

Items to Consider During Site Visits

- The vendor's controls documented in a current, "clean" SOC report provide enough information for your organization to gain comfort service specific risks are addressed.

- The vendor's due diligence package includes documentation for the relevant audit areas, such the vendor's:
  - Audited Financials
  - Business Continuity/Disaster Recovery Plan
  - BCP/DR Testing details and results
  - Summary of penetration testing
  - Information Security Program
  - Incident Response Plan

venminder

Poll Question

Are you currently using critical vendors that do not provide a SOC report?

a. Yes
b. No
c. Not sure

venminder

How to Prepare for a Virtual Vendor Site Visit

- Review the vendor's risk profile and due diligence documentation
- Identify any gaps in the documentation
- Contact the vendor to set up the audit
- Agree upon the method and technologies used to conduct the audit
- Confirm the vendor will allow you to view documents through share screen/video technologies

venminder

How to Prepare for a Virtual Vendor Site Visit

- If you're using screensharing or video call technology, ensure it is a secure option
- Perform planning to maximize your time
- Be sure to set up meetings that are agreed upon with the key contacts
- Talk about expectations related to what you want to see during observations
- Talk about expectations related to screenshots, screen capture and recording

venminder

How to Prepare for a Virtual Vendor Site Visit

- Be creative
- Confirm meetings with key personnel in advance
- Confirm virtual site visit date with the vendor
- Send information request at least three weeks in advance

venminder

Create a Walkthrough Schedule

Here's an example of what it will look like:

Date	Contact	Process	On-Site Audit Steps	Virtual Considerations
10/1/2020	Bob Smith	Physical Security	1. Observe perimeter 2. Walkthrough data center 3. Inspect card key system users	1. Perform observations through secure live session with employee onsite. 2. Use screensharing to view camera footage – ensuring date and timestamp are indicated in view. 3. Use secure screen sharing to inspect card key system
10/1/2020	Sherry Jones	Insurance	4. Inspect insurance coverage	Use secure screen sharing to observe the insurance coverage.
10/1/2020	Chris Johnson	Cyber Resilience	5. Inspect firewall/IPS configs 6. Review DNS configs 7. Inspect pen test report	Use secure screen sharing to observe the configurations and reporting.
10/1/2020	Bob Smith	Info Sec	8. Inspect Info Sec Program 9. Inspect incident response Plan 10. Inspect testing documentation	Use secure screen sharing to inspect the policy documents and reporting.
10/1/2020	Chris Johnson	BCP	11. Inspect BCP 12. Inspect BCP testing results	Use secure screen sharing to inspect the policy documents and reporting.

Onsite Visit Procedure Example

CREATE A SPECIFIC AUDIT WORK PROGRAM TO FOLLOW

Step	Physical Security	Tested By/ Date	Conclusion	Notes
1.	Observe the server room to determine whether these are physical security controls (key locks, card key systems, etc.).			
2.	Observe the facilities to determine whether there are security cameras at entrance/egress points, especially the server room.			
3.	Observe whether visitors are identified and required to sign a visitor's log. Also determine whether visitors are required to wear badges that identify them as visitors.			
4.	Observe operational areas to determine that areas where critical processing is conducted are physically secured.			
5.	Inspect the Server Room Access List (system generated) to determine whether access is restricted to the server room based upon specific job responsibilities.			

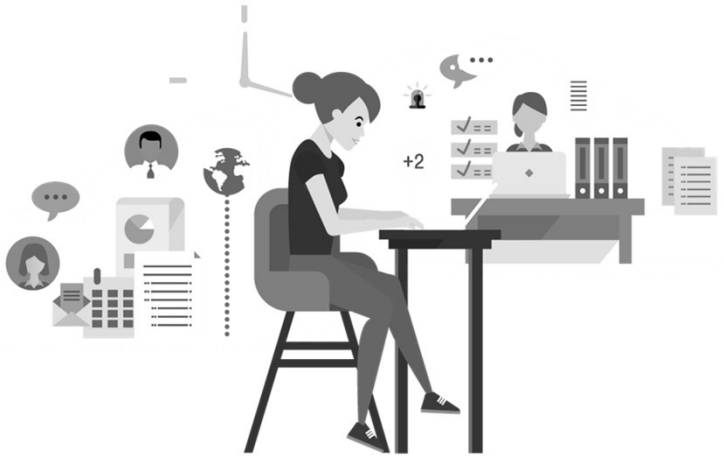
Virtual Site Visit Procedure Example

CREATE A SPECIFIC AUDIT WORK PROGRAM TO FOLLOW

Step	Physical Security	Tested By/ Date	Conclusion	Notes
1.	Observe the server room with employee via Facetime to determine whether these are physical security controls (key locks, card key systems, etc.).			
2.	Observe key facility areas through camera footage feeds to determine whether there are security cameras at entrance/egress points, especially the server room. Be sure to capture the date and time in the camera user interface. It may also be helpful to look back in time for activity if there is no activity during the live observation. This ensures the cameras are live.			
3.	Observe camera footage from entrance ways to determine whether visitors are identified and required to sign a visitor's log. Also determine whether visitor badges are present at the main entrance for visitors to wear.			
4.	Observe key operational areas through camera footage feeds to determine that areas where critical processing is conducted are physically secured.			
5.	Inspect the Server Room Access List (system generated) to determine whether access is restricted to the server room based upon specific job responsibilities.			

Common Scope Areas

- Business Continuity Planning
- Information Security
- Insurance Coverage
- Cyber Resilience
- Logical Security
- Physical Security
- Environmental Controls
- Data Backup
- Vendor Management
- Change Management



venminder

Sample Virtual Site Visit Questions

- How many physical locations do you currently have?
- Are most users working remote?
- How do employees access company systems?
- Do you provide employees with computers/hardware?
- What measures have been applied to ensure employee safety during the pandemic?
- What access restrictions are in place for remote workers?

venminder

Best Practices

- "Right to Audit" clauses
- Tailoring each audit to each vendor's risk profile
- Avoid scope overlaps
- Providing vendors sufficient notice prior to the site visits
- Send information requests ahead of time

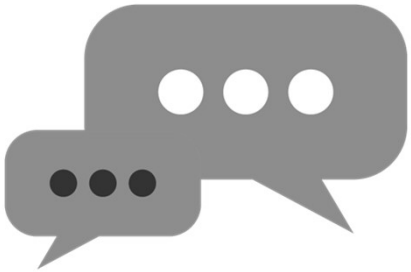
- Allow yourself adequate time in meetings
- Confirm you will be provided access to the documents you will need (especially in virtual setting!)
- Confirm individuals will perform observations through secure video call options
- Properly document your conclusions in a formal report

venminder

Conclusion

- Site visits can provide a process to perform due diligence on vendors that do not provide critical due diligence information
- These visits are appropriate if the vendor is missing due diligence information or refuse to provide information
- Properly scoping site visits can maximize your time and results
- Proper planning and communication are required to successfully perform site visits virtually

venminder



Questions & Answers

Post a Question:

www.thirdpartythinktank.com

THIRD PARTY thinktank

Email Us:

mike.morris@wipfli.com
marybeth.marchione@wipfli.com

Follow Us:

@venminder

venminder

Also Join Us At
Our Upcoming Webinars:

NOVEMBER 10, 2020
Understanding and Analyzing Vendor SOC Reports

DECEMBER 8, 2020
Third-Party Risk Management Best Practices for 2021

Click here to view our Webinars Page.

venminder

Thank You