Rules to Receive CPE Credit

Attending today's live session, you are eligible to receive 1 CPE credit per the following guidelines.

In order to receive these credits, the following items MUST be completed:

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

Vendor Due Diligence Site Visits

November 13, 2018

Mike Morris
Partner at Porter Keadle Moore
mmorris@pkm.com
(404) 420-5669

venminder

SESSION AGENDA

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

Learn when site visits are appropriate (and when they are not)

Scope and conduct site visits

VENDOR SITE VISITS – WHAT THEY ARE

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

VENDOR SITE VISITS – WHAT THEY ARE NOT

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

POLL QUESTION

Is your organization currently performing site visits for key vendors?

a. Yes
b. No
c. Not sure

WHEN ARE VENDOR SITE VISITS APPROPRIATE?

- Vendor refuses to provide due diligence documentation
- You are performing initial due diligence on a new vendor
- Vendor who are not providing information annually
- Remediation testing

WHEN ARE VENDOR SITE VISITS APPROPRIATE?

- 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
- There are clear control gaps in a vendor's SOC Report

WHEN ARE VENDOR SITE VISITS APPROPRIATE?

- 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

WHEN ARE VENDOR SITE VISITS APPROPRIATE?

Example:

- A vendor provides a payroll application
- SOC report is not available or does not include data handling/physical security
- Considered high risk due to the nature of information handles
- Onsite visit to determine data handling procedures and physical security are in place

POLL QUESTION

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

a. Yes
b. No
c. Not sure

WHEN ARE VENDOR SITE VISITS NOT APPROPRIATE?

- ✓ The vendor's controls are clearly documented in a current, "clean" SOC report
- ✓ A vendor's due diligence package is complete
- ✓ There are no noticeable gaps in the vendor due diligence information

WHEN ARE VENDOR SITE VISITS NOT APPROPRIATE – EXAMPLE

- ✓ Management is concerned with the physical security of a third party data center
- ✓ The data center provides a SOC 2 report that covers the Security, Availability and Confidentiality principles for the past 12 months
- ✓ The opinion within the SOC 2 was unqualified (clean)
- ✓ The scope of the SOC 2 adequately covers the areas of concern (i.e. camera coverage, access restriction, visitation procedures, etc.)

POLL QUESTION

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

a. Yes
b. No
c. Not sure

HOW TO PREPARE FOR A 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
- Perform planning to maximize your time on site

HOW TO PREPARE FOR A VENDOR SITE VISIT

CREATE A WALKTHROUGH SCHEDULE

Date	Contact	Process	Audit Steps	Estimated Time
10/1/2018	Bob Smith	Physical Security	1. Observe perimeter 2. Walkthrough data center 3. Inspect card key system users	20 minutes 20 minutes 40 minutes
10/1/2018	Sherry Jones	Insurance	4. Inspect insurance coverage	30 minutes
10/1/2018	Chris Johnson	Cyber Resilience	5. Inspect firewall/IPS configs 6. Review DNS configs 7. Inspect pen test report	30 minutes 20 minutes 30 minutes
10/1/2018	Bob Smith	Info Sec	8. Inspect Info Sec Program 9. Inspect incident response Plan 10. Inspect testing documentation	30 minutes 20 minutes 30 minutes
10/1/2018	Chris Johnson	BCP	11. Inspect BCP 12. Inspect BCP testing results	45 minutes 30 minutes

HOW TO PREPARE FOR A VENDOR SITE VISIT

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

HOW TO PREPARE FOR A VENDOR SITE VISIT

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.			

COMMON SCOPE AREAS

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

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 visit
- ✓ Send information requests ahead of time
- ✓ Allow yourself adequate time on site
- ✓ Confirm you will be provided access to the documents you will need
- ✓ Properly document your conclusions in a formal report

CONCLUSION

- ✓ Site visits can provide a process to perform due diligence on vendors that do not provide 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

Questions & Answers

mmorris@pkm.com

venminder

Thank You

venminder

www.venminder.com

Follow us on:

Porter Keadle Moore

CPAs | Advisors | www.pkm.com

www.pkm.com

Follow us on: