KPMG Supplier Cyber Review Service

Description and Overview

FINAL

January 2020

What is the KPMG Supplier Cyber Review?

The increasing cyber security threat landscape, combined with ever more complex supply chains and increasing compliance and regulation requirements has pushed supplier cyber risk management back into the spotlight and to the top of Board agendas.

KPMG's Supplier Review service can help give you an understanding of the cyber risk within your supply chain by providing a quick assessment of the cyber capability of one of your key suppliers.

How can a Supplier Review help?

A KPMG Supplier Review can help your organisation to:

Take a proactive view on cyber risks in your supply chain

Understand the capability of a key supplier to protect information assets and its preparedness to respond effectively to cyber threats

Evaluate how that key supplier is managing their cyber security requirements to you

Demonstrate a successful, good practice methodology for how you could review your suppliers and build a sustainable supplier risk management program

How do we assess the cyber capability of a supplier?

KPMG views cyber security as more than a technology issue – the Supplier Review leverages KPMG's nine cyber domains, which together cover People, Processes and Technology:

01 **Leadership and Governance**

02 **Security Architecture**

03 **Security Operations**

04 **Information Risk Management**

05 **Third Parties**

06 **Cyber Resilience**

07 **Human Factors**

08 **Technical Security**

09 **Compliance**

How does the KPMG Supplier Cyber Review service work?

The Supplier Cyber Review service process is likely to take two weeks, and may involve a few hours of time for a small number of your supplier's stakeholders. There may also be a small amount of time required from your team.

Phase 1: Set up and contracting

You decide that you would like to take up KPMG's service.

You can contact KPMG directly through the Beazley Breach Solutions portal or via BBRinfo@beazley.com.

The following then occurs:

- You confirm which supplier you would like KPMG to review (you can provider several options).
- KPMG confirms whether they can perform the service.
- KPMG sends a standard engagement letter for you to sign.
- KPMG sends an overview of the service and what the process will entail to both you and the supplier.
- KPMG may arrange an initial call with you to discuss the supplier.

Phase 2: Supplier self-assessment

KPMG generates a questionnaire and provides instructions to the supplier on how to complete it, through a kick-off call between yourself, the KPMG consultant and the supplier.

This call will set expectations and clarify the scope of services.

The questionnaire captures some company information of the supplier (including the types of support that it provides to your organisation) and provides a cyber security self-assessment to help determine where KPMG will perform review activities during Phase 3.

Completion of the self-assessment by the supplier is required before Phase 3.

Phase 3: KPMG review and follow-up

KPMG conducts the review through telephone session(s) with the supplier, using the questionnaire answers from Phase 2 to lead the conversation.

KPMG will use a test plan to review the supplier and this may include review of supporting documentation, including attestation reports or cyber security contractual requirements.

Phase 4: Reporting and close-out

KPMG holds a closing meeting with the supplier to discuss initial findings and analysis.

KPMG will prepare a short report based upon the answers provided in the self-assessment questionnaire and information from the review in Phase 3.

This report will provide commentary and proposed recommendations on your supplier's cyber security.

KPMG will send you the report via email and organise a debrief phone call. The supplier will not receive the report by default but you may wish to send it to them and invite them to the debrief phone call.

Your responsibilities:

- Sign an engagement letter with KPMG during Phase 1 as KPMG cannot start work without this.
- Advise KPMG of which supplier you would like reviewed (and their details) and provide written confirmation that the supplier has agreed to the review.
- Advise KPMG of a single point of contact in your organisation who can liaise with KPMG throughout the service and coordinate supplier engagement.
- Respond to any ad-hoc requests from KPMG for additional detail during the service (e.g. details of how the supplier supports your organisation – this may include any contractual cyber security requirements that the supplier is obliged to meet).

The proposals set out in this document do not constitute an offer capable of acceptance. They are in all respects subject to satisfactory completion of KPMG's procedures to evaluate prospective clients and engagements, including independence and conflict checking procedures, and the negotiation, agreement, and signing of a specific engagement letter or contract. KPMG International provides no client services. No KPMG member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm.