Trustwave®

SERVICE DESCRIPTION

Managed Vendor Risk Assessment (MVRA)

Overview

Trustwave's Managed Vendor Risk Assessment (MVRA) ("**Service**") provides a lightweight cybersecurity risk assessment of one or more Client vendors, based on such vendors' services, security maturity, and information responsive to a Trustwave provided questionnaire. Trustwave delivers a report describing areas of information security control weaknesses as well as recommended remedial activities required to bring the vendor within Client's risk tolerance levels. The following description sets out the parameters of the Service, as may be further modified by an applicable SOW or Order Confirmation between Trustwave and Client.

Delivery Phases

The MVRA process consists of the following three high-level phases:

Phase 1 – Project Management

Key activities completed in the Project Management phase include:

- Meeting with Client personnel to establish project roles and responsibilities
- Developing a project management plan and socializing it with the Client for review and acceptance
- Communicating with the Client project manager as required
- Agreeing on reporting frequency and delivery method

Phase 2 – Program Design, Configuration, & Operationalization

Trustwave will perform this phase only the first time Client purchases the Service and provided that Client purchases the CPS-ADVISORY-MVRA-NEWCLIENT SKU in addition to the Service.

Key activities completed in the Program Design, Configuration, & Operationalization phase include:

- Review the current state of Client's vendor risk assessment program
    - Review formal or informal processes in place and vendor risk process documentation
    - Review existing questionnaires and requirements to integrate with existing processes
    - Review known vendor portfolio
    - Confirm that necessary vendor information (e.g., up to date contact details) is available for vendors subject to assessment
    - Confirm the process Client will use for completing a triage assessment for each of the vendors prior to onboarding the vendor for assessment. Client will provide this triage

    assessment to Trustwave along with the required onboarding information. Trustwave will rely on the triage assessment as accurate reflection of the risk or importance of each vendor to Client.

- Define assessment structure and operating model
    - Define the vendor onboarding process, agreeing:
        - Process for Client to onboard vendors for assessment to the MVRA platform
        - Introduction and communication to vendors prior to assessment process commencing
        - Support and Q&A process for supporting vendors through the assessment and response process
        - Reporting requirements, such as the inclusion of vendor risk profile metrics, controls, and recommendations
    - Provide process documentation, user guides, and vendor questionnaires to Client
- Deploy and configure MVRA platform
    - Provision an account for Client in the MVRA platform
    - Design and configure vendor questionnaires as required
    - If Client has a bulk vendor list for assessment (>20 vendors), build timeline or schedule for completion of vendor risk assessments, prioritizing perceived high-risk vendors
    - Provide Client with email content to advise onboarded vendors of the upcoming vendor risk program
    - Deliver staff training (up to 4 x 1-hour sessions) to run Client staff through the system

Phase 3 – Vendor Risk Assessment

Key activities completed in each Vendor Risk Assessment include:

- Execution and Management of Vendor Risk Assessments
    - Receive vendor information from defined onboarding process
    - Distribute Trustwave's Vendor Cyber Security Assessment Questionnaire (VCSAQ) to vendors
    - Receive vendor responses to VCSAQ including associated supporting files
    - As necessary and within the Timeline Limitations specified below, follow up with vendors to obtain the necessary responses and supporting files
    - Complete vendor risk assessment by reviewing vendor responses to questionnaire and evidence files submitted by each vendor. Following this review, each vendor will receive a risk rating. Any borderline issues will be discussed and agreed with the Client prior to report generation.
    - Generate required reporting as agreed in Phase 2. The report delivered to the Client will capture the outcomes of the assessment, in an easily interpreted format.
    - Submit report to Client for review
- Deliver all components of the process in line with the Service Level Targets (SLTs)

Assessment Credits

The Phase 3 of the Service operates on a credit structure. Client's credit package will be indicated in the applicable SOW or Order Confirmation between Client and Trustwave. Each credit ("**Assessment Credit**") entitles Client to a single Vendor Risk Assessment. Client is able to purchase additional Assessment Credits within the Term. Each Assessment Credit is subject to the Credit Term indicated below. However, the Credit Term is superseded by the Term and all Assessment Credits will expire upon expiration of the Term.

Package Type	Number of Credits	Credit Term
Micro	10	3 months
Small	20	6 months
Medium	50	12 months
Large	100	12 months
Extra Large	150	12 months

Service Level Targets & Timeline Limitations

Trustwave will aim to deliver the Services on the following estimated timelines:

Activity	Timeline	Vendor Responsibilities	Client Responsibilities
Assessment questionnaire sent to vendor	2 business days from correct onboarding by Client	N/A	• Correct vendor triage information and contact details have been provided to Trustwave • Vendor has been notified of upcoming assessment
Respond to vendor or Client questions	1 business day from receipt of query	N/A	N/A

Submit draft vendor risk assessment report to Client	8 business days from full completion of questionnaire and provision of evidence	• Vendor has completed questionnaire • Vendor has provided requested assurance evidence • Quality of vendor’s response meets necessary requirements	N/A

Timeline Limitations

Client agrees and acknowledges that SLTs for each activity and the overall end to end process are subject to, and each timeline shall not commence until, the completion of Vendor or Client Responsibilities listed above, as applicable.

Following Up & Abandoned Reviews

Once Client onboards a vendor and Trustwave issues such vendor a VCSAQ, the associated Service Credit for that vendor review is used and cannot be re-used for another vendor. Removal or cancellation of a vendor review after the issuance of the VCSAQ is considered a completed review.

If a vendor has provided an inadequate response (e.g., lacks detail or does not appear to answer the question), Trustwave will follow up with the vendor for clarification via the MVRA Platform. Timeframes for follow up are as follows:

Initial VCSAQ Process

- 2 weeks (10 business days) after sending the initial VCSAQ to the vendor, Trustwave will follow up if no response is received.
- After 1 additional week (5 business days), Trustwave will follow up a second time if a response has not been received from the vendor.

Post-VCSAQ Response Process

- 1 week (5 business days) is allowed for a vendor to respond to a request for clarification or additional information in relation to a specific query, after which Trustwave will follow up.
- After 1 additional week (5 business days), Trustwave will follow up a second time up if a response has not been received from the vendor.

Limits on Following Up & Subsequent Escalation Process

Trustwave will follow up a maximum of twice per query. If Trustwave cannot elicit a satisfactory response within 10 business days, the assessment for that vendor will be placed on hold and the issue escalated to the Client’s designated business owner for action. Reporting will recommence upon successful resolution and notification to Trustwave by Client, or where Client directs Trustwave to complete the process with only partial or no resolution.

Maximum Time Limits & Abandoned Reviews

Maximum time limits in the review process are:

- 8 weeks from the date of the initial VCSAQ being sent to the vendor

Should this time limit lapse, the assessment report for that vendor will be finalized with available information and no further updates will be completed by Trustwave.

Client Obligations

For Trustwave to provide this Service, Client will:

- establish contact with and remain available for communications from Trustwave;
- establish communication and escalation plans with Trustwave;
- review, provide feedback, and agree to PMP;
- provide contact details of and access to key stakeholders within Client's organization;
- provide logistics support for booking in meetings, coordinating workshops, and arranging access to required documentation or personnel;
- provide the necessary documentation and interview access so as to support off-site delivery of the Service by Trustwave consultants who may be based in the same or different countries to the Client;
- review and accept the end user license agreement (EULA) of the MVRA platform;
- make available resources needed for Service activities; and
- participate in and understand materials explained during calls, meetings, interviews, workshops, discussions, facilities inspection, and controls analysis.

Client acknowledges:

- the Service may consist of onsite and remote consulting activities;
- the Service does not include in-depth testing or review of vendor system settings, configurations, or observation of implemented processes and procedures;
- the Service is an assessment of vendor security maturity and is not an assessment of any specific vendor technology solution;
- the Service does not include visits to third parties or vendor sites;
- Trustwave will perform the Service in the English language;
- Trustwave will not create or modify Client documentation as part of the Service;
- Trustwave will not provide remediation services as part of the Service;
- Trustwave will not offer any legal guidance or counseling; and
- the quality and accuracy of the Service is dependent on the provision of accurate information to Trustwave by Client and by vendors.

Client is responsible for:

- making its own assessments and judgements regarding the configuration and suitability of its security solutions, including where Client obtains advice and consultancy from Trustwave;
- effectively onboarding vendors including accuracy completing 'baseline risk assessment' prior to onboarding;
- establishing a contractual framework with vendors within which the vendors are able to provide security relevant documentation to Trustwave for assessment;
- making its own business decisions about technology security;
- making its own business decisions about the suitability of the Findings.co platform for storage of Client vendor security assessment data;
- assessing its risks and deciding the most appropriate security solution;
- having personnel who have the ability to assess the advice received from third parties as it relates to you and your business;
- its own security and access management;
- its data backup, retention, and deletion;
- its data recovery, disaster recovery and business continuity management;
- making decisions on location of data and transferring data, particularly in relation to personal information; and
- its redundancy of networks or systems and support obligations.

Trustwave Obligations

For this Service, Trustwave will:

- allocate a lead consultant and supporting consultant (as necessary) to deliver the Service;
- establish contact and remain available for communications from Client;
- establish communication and escalation plans;
- provision an account on the MVRA platform for Client, noting that Client will be required to accept the EULA for using this platform;
- follow agreed engagement processes between Trustwave, Client and vendors;
- define a high-level project management plan including milestone dates, key steps, estimates for duration, change management process, key contact details, and resource requirements;
- schedule and conduct kickoff, periodic status, and closeout meetings, as appropriate;
- deliver the Service and document the findings of the Service in a report; and
- present the reports to Client electronically.

Definitions

All capitalized terms not defined in this document have the meanings ascribed to them in Trustwave's Master Terms and Conditions available at https://www.trustwave.com/en-us/legal-documents/contract-documents/ or in the applicable Statement of Work or Order Confirmation between Trustwave and Client.