Trustwave®

SERVICE DESCRIPTION

Cyber Advisory Diagnostic Services

Overview

Trustwave's cyber advisory diagnostic services ("**Service**") provide Client with desktop reviews based on interviews and documentation analysis. 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.

Service Features

The Service includes one (1) or more of the following diagnostics (one (1) or more, "**Diagnostics**", and each, a "**Diagnostic**"). The applicable Diagnostic(s) will be indicated in a SOW or Order Confirmation between Client and Trustwave.

Security Maturity Diagnostic

This Diagnostic provides a review of Client's organizational or divisional security program maturity and current operating effectiveness. Trustwave will provide Client with a gap analysis report and strategic roadmap along with tactical recommendations to achieve the Client's target state and mitigate cyber risk.

Supply Chain Risk Diagnostic

This Diagnostic provides a review of the current state of Client's cyber supply chain risk management maturity and operating effectiveness, both in terms of the products and services it uses, and the products and services it supplies to downstream customers. Trustwave will provide Client with a gap analysis report and strategic roadmap outlining the path to an agreed target state.

Cloud Security Diagnostic

This Diagnostic provides a review of the maturity of Client's existing cloud computing security strategy, including a review of Client's cloud security policy, procedures, architecture, privileged access, data protection, and core security controls against industry best practices. Trustwave will provide a gap analysis report and strategic roadmap outlining the path to a target maturity state of cloud security and tactical recommendations to assist Client in mitigating cyber risk.

Note that for clarity, the Service does not include active security assurance of any controls by Trustwave, or remediation by Trustwave of any gaps, vulnerabilities or findings it identifies as a result of supplying the Service.

Delivery Phases

Trustwave separates each Diagnostic into three (3) delivery phases: information gathering and kickoff, analysis, and reporting.

Each Diagnostic includes up to twenty (20) working days of effort, generally split evenly between two (2) Trustwave consultants (a lead consultant and a supporting consultant). Delivery typically takes place over four (4) to six (6) weeks from the Service kickoff date ("**Kickoff**"). Notwithstanding the above, a project management plan ("**PMP**") agreed between Client and Trustwave will guide specific timelines for a given Diagnostic.

Technical extensions designed to test or verify Client controls reviewed during the Service (separately scoped and quoted in the applicable SOW or Order Confirmation) can be included when required to gain additional validation of control efficacy.

Phase 1: Information Gathering & Kickoff

Trustwave will work with Client to gather information that describes Client's security control environment covered by the Diagnostic. This task will include:

- An initial presentation delivered by Trustwave to explain the Service delivery process
- Development and delivery of an initial PMP by Trustwave to Client, outlining the Service delivery timetables, communications approach, key contact points, change management process, and other project management items (as needed)
- Trustwave requesting documentation from Client
- Trustwave requesting interviews with relevant Client stakeholders
- Trustwave following up on documentation review and interviews (as necessary) to clarify any inconsistencies or gaps

As a part of Phase 1, Trustwave may research industry trends and risks relevant to Client.

Phase 2: Analysis

Trustwave will examine applicable Client-provided documentation and interview notes to assess Client's current state of cybersecurity maturity and to identify relevant risks within the scope of the Diagnostic. Trustwave bases its maturity assessment on a modified capability maturity model integration (CMMI) model reflecting the following maturity levels:

1. Incomplete
2. Initial
3. Managed
4. Defined
5. Quantitatively Managed
6. Optimizing

Trustwave's assessment will also incorporate specific targeted reviews of evidence or other service artifacts Trustwave requests and receives from Client.

Security Maturity Diagnostic

The following additional Phase 2 tasks are only included in the Security Maturity Diagnostic:

- Trustwave will examine documents provided by Client and review them for gaps, omissions, inaccuracies, issues, and risks, and identify points of interest for further investigation/questioning to help determine Client's current security maturity. Trustwave will provide Client with a documentation and evidence request list for the specific documents Trustwave will need upon Service commencement which may include among other items:
    - Security policies, standards, and procedures
    - Business plans, analysis and other artefacts (e.g., asset registers and data flow diagrams) that may have security implications
    - Technical evidence (e.g., past security test results, change management logs and threat and vulnerability registers)
    - Prior security audits, assessments, or reviews.
- Trustwave will conduct interviews with relevant Client stakeholders to:
    - Review preliminary findings from the documentation review
    - Identify and assess the effectiveness of security controls relating to the NIST CSF subcategories
- Trustwave will assign a process maturity rating for each of the NIST CSF subcategories using a CMMI 0-5 score
- Trustwave will document preliminary findings/recommendations based on critical omissions and control weaknesses
- Trustwave will conduct a current state maturity workshop with Client to:
    - Discuss current observations and NIST CSF Current State Dashboard
    - Discuss likely recommendations and potential roadmap work packages
    - Agree to a timeline for the roadmap.
- Trustwave will develop a CMMI goal state maturity level for each of the NIST CSF subcategories, considering current state of security maturity
- Trustwave will develop recommendations to help reach the target state for each of the NIST CSF subcategories.

Supply Chain Risk Diagnostic

The following Phase 2 tasks are only included in the Supply Chain Risk Diagnostic:

- Trustwave will examine Client's current state cyber supply chain risk management maturity both as a consumer and as a provider of services
- Trustwave will review Client's inbound supply chain risk management documentation

- Trustwave will conduct inbound supply chain risk management (SCRM) interviews with Client stakeholders (e.g. owner of vendor security assessment process or procurement manager)
- Trustwave will test Client's vendor triage process.
- Trustwave will assess sample vendor reviews.
- Trustwave will conduct an initial risk and NIST CSF current state workshop for inbound SCRM processes with Client stakeholders to discuss current observations for focus areas, current NIST CSF maturity state and agree on a target NIST CSF maturity state.
- Trustwave will review outbound SCRM documentation (e.g. past completed questionnaires, external facing cyber security materials).
- Trustwave will conduct outbound SCRM response process interviews with Client stakeholder(s) – (e.g., IT Security Manager or External Comms/Marketing).
- Trustwave will conduct an additional outbound SCRM workshop providing a high-level analysis of the information received and reviewed to date with Client stakeholders, including reviewing the current approach to handling vendor risk questionnaires and merit in alternative approaches.
- Trustwave will capture notes, observations, gaps, issues, and risks, in a Diagnostic Data Collection & Analysis spreadsheet.
- Trustwave will identify gaps, issues and risks and points of interest for further investigation/questioning.

Phase 3: Reporting and Final Presentation

Trustwave will produce a separate strategic roadmap report for each Diagnostic Client purchases. For each report, Trustwave will set up a meeting with Client to obtain feedback/input on the roadmap report, which will then be finalized based on this feedback.

Trustwave will then deliver a final project presentation to relevant Client stakeholders, summarizing findings and recommendations from the roadmap report and answering outstanding queries. Client will make itself reasonably available for such meetings.

Security Maturity Diagnostic

For the Security Maturity Diagnostic, the roadmap report will include:

- Executive summary
- Assessment approach
- Methodology
- Current state analysis
- Observations and risks
- Market sector research
- Goal state analysis
- Metrics

- Work packages & recommendations
- Tactical & strategic maturity improvement roadmap
- Appendices

Cloud Diagnostic

For the Cloud Security Diagnostic, the roadmap report will include:

- Current state of maturity assessment for the Diagnostic
- Target state of maturity for the Diagnostic
- Any identified gaps between the current state and target state, along with recommendations to help close the gaps
- Security program recommendations, comprising of an analysis of any identified gaps and suggested priorities to help close the gaps
- Actions, grouped into work packages, with high level effort and resource estimates
- A list of potential “quick wins” available to Client to help achieve a rapid uplift in process maturity, effectiveness, or risk mitigation.

Supply Chain Risk Diagnostic

For the Supply Chain Risk Diagnostic, the roadmap report will include:

- Key industry trends and drivers for change over the next 3-5 years
- Detailed supply chain risk management recommendations, including:
  - Current state of maturity assessment for the Diagnostic
  - Target state of maturity for the Diagnostic
  - Any identified gaps between the current state and target state, along with recommendations to help close the gaps
  - Aggregated and sequenced recommendations based on a 2-3 year roadmap timeframe, grouped into ‘themes’ or work streams’ with high level effort and resource estimates, and any opportunities for ‘quick wins’ to help achieve a rapid uplift in process maturity, effectiveness, or risk mitigation.

Obligations and Acknowledgments

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;
- 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 system settings, configurations, or observation of implemented processes and procedures;
- the Service does not include visits to third parties or direct engagement with third parties. All information will be obtained directly from Client;
- Trustwave may request evidence from Client's systems and processes as required to prove compliance with any specific requirements. Client agrees to provide all such evidence in a timely manner;
- 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 Client's provision of accurate information to Trustwave.

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.
- making its own business decisions about technology security;
- 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;
- 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;
- interview and collect information from applicable Client personnel;
- deliver the Service and document the findings of the Service in a report; and
- present the report to Client.

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.