HPE
POINTNEXT
SERVICES

HPE RISK ASSESSMENT SERVICE

Advisory and Professional Services from HPE Pointnext Services

SERVICE OVERVIEW

HPE Risk Assessment Service for cybersecurity is designed to assist organizations in obtaining a better understanding of the information security risk their assets may be exposed to in their operational environment and develop a strategy to either reduce or better manage it. No matter if your assets are located on-premises or on a private or public cloud, or you are in the process of planning to rehost or replatform your assets, let HPE help you understand and develop a plan to manage your information security risk. A risk-based approach and appropriate security measures not only reduce the ongoing operational security and financial risk related to information security but also allows organizations to react and adapt to changes at a much faster pace and thus create business advantages over competitors.

HPE Risk Assessment Service for cybersecurity is a customizable service based on the size of the environment (number of in-scope assets). Service duration can vary from one to four weeks and beyond. The assessment methodology for the HPE Risk Assessment Service for cybersecurity is developed based on the ISO/IEC 27001:2013 and ISO/IEC 27005. The service provides a comprehensive point-in-time assessment and analysis on threat, vulnerability, and risk associated with each in-scope asset including associated business process and existing controls of assets. The asset are evaluated against the organization's security objectives, which can be composed of legal, regulatory, and contractual requirements; organization's strategic and operational requirements; and security risks that are specific to the organization and/or type of business the organization conducts.

The following deliverables will be provided by HPE at the end of the assessment:

- Workshop documentation
- Asset evaluation report
- Risk assessment report
- Risk treatment recommendations and road map

Table 1 provides additional information on the features available under this service.

SERVICE BENEFITS

- Obtain information on the in-scope assets' risk potential likelihood and implication
- Understand the risk landscape related to your organization's strategies and goals
- Select, justify, and understand how to apply appropriate security controls to transform your security, help optimize your business, and manage risks inherent in the existing operational environment

SERVICE FEATURE HIGHLIGHTS

HPE Risk Assessment Service for cybersecurity is a business-led consultative engagement that consists of the following stages:

1. Risk assessment service preparation
2. Kick-off and context establishment
3. Asset evaluation
4. Risk assessment
5. Risk treatment

TABLE 1. SERVICE FEATURES

STAGE	DELIVERY SPECIFICATION
1—Risk assessment service preparation	**AN HPE SENIOR CONSULTANT WORKS WITH THE CUSTOMER TO:** • Define and agree preliminary scope of service • Agree on first draft schedule • Set up customer and HPE project team
2—Kick-off and context establishment	AN HPE SENIOR CONSULTANT WORKS WITH THE CUSTOMER TO: • Initiate the project with a kick-off meeting and organize remote follow-up and status meetings, including discussions of requirements • Identify and review service prerequisites and any actions required of the customer to meet those prerequisites • Identify stakeholders and potential resources required for the service and obtain their contacts • Create project schedule and schedule service activities THE HPE PROJECT TEAM: • Defines and confirms final scope of service, including assessment scope, rules of engagement, acceptance criteria, and others. • Works with the identified stakeholders to collect information on the in-scope assets. Information maybe gathered via existing documentation, interviews, or physical/remote observations. Information may include but not be limited to: – Business and IT strategic plans – Business and IT organizational charts – Security policies – Security procedures – Security program documents – Security product inventories – IT audit reports
3—Asset evaluation	The HPE project team: • Identifies the assets (business process, hardware, software, network, information, media, support service), which are part of the scope as identified during the context establishment phase. • Identifies data/service, which each asset processes, stores, or transfers, and evaluates asset value based on the confidentiality, integrity, and availability of the data/service • Documents the asset evaluation results in the asset evaluation report (in Microsoft® Word format)
4—Risk assessment	The HPE project team: • Performs risk estimation on the in-scope assets (qualitative or quantitative) – Threat rating for the assets – Vulnerability rating of the assets – Likelihood of the exploit – Risk impact rating • Documents the risk assessment results in the risk assessment report (in Microsoft Word format)
5—Risk treatment	The HPE project team: • Defines risk treatment options • Maps risk treatment options to identified risk (from Stage 3) • Recommends risk treatment controls for identified risk and documents the treatment suggestions in the risk treatment plan/road map (in Microsoft Word format)

COVERAGE

- Services will be provided during local HPE standard business days and hours excluding HPE holidays.

CUSTOMER RESPONSIBILITIES

- Provide complete and accurate responses to all queries from HPE
- Communicate openly about IT infrastructure governance practices and needs to support their business objectives
- Provide neutral and up-to-date information on in-scope subjects including but not limited to financial budgeting and service costing structure of the subject, asset protection controls on the subject and general security organization structure, and others
- Assign a contact person to organize project logistics
- Assign a project sponsor and be available for two to four hours per week to discuss logistics, preparation, outcomes, and data gathering during the engagement period
- Provide access to the right management level (functional management or higher)
- Ensure interviewees are available as per the mutually agreed upon interview schedule
- Provide all requested documents and artifacts as per the agreed upon project schedule and HPE document requests
- Provide subject matter experts (SMEs) as required to clear up any areas of confusion or uncertainty
- Perform other reasonable activities to help HPE identify or resolve problems as requested
- Provide a suitable work area for delivery of the service, including access to an outside telephone line, power, and any network connections required
- Allow HPE all necessary access to all locations and networks where the service is to be performed
- Review and approve deliverables

SERVICE LIMITATIONS

- Limitation of each service feature is outlined in the TABLE 1. Additional charges incur for any additional services required.
- Assessment finding and any associated recommendations are based on the accuracy and completeness of the information available at such time, along with the accuracy and completeness of any information provided by the customer during the information gathering activities of this service. HPE does not warrant that all security risks within the environment will be identified or that any recommended solution will prevent all identified security risks.
- The entire deliverable documentation created for this engagement will be available in Microsoft Word or PDF electronic format.
- Services are deemed accepted upon performance.

GENERAL PROVISIONS AND OTHER EXCLUSIONS

- Our ability to deliver this service is dependent upon the customer’s full and timely cooperation with HPE, as well as the accuracy and completeness of any information and data the customer provides HPE.
- HPE reserves the right to reprice this service if the customer does not schedule and provide for subsequent delivery within 90 days of purchase.
- HPE will not process personal data as part of this service.

SUPPLEMENTAL TERMS

The following supplemental terms apply to these services and take precedence in the event of any conflict:

- Upon receipt of an acceptable order, HPE will contact the Customer within seven (7) business days to organize a service delivery date. Service delivery dates are subject to resource availability and may be scheduled up to 30 days from the order acceptance date.
- The Customer must schedule and receive delivery of these services within 180 days from order acceptance. HPE reserves the right to reprice for services not scheduled and delivered within 180 days. Backorders or shipment delays may affect the delivery timeline. Orders for services will expire after 365 days (one year) from the order acceptance date for services not scheduled and delivered, and the Customer will not be entitled to a refund for the unused services.

ORDERING INFORMATION

Availability of service features and service levels may vary according to local resources and may be restricted to eligible products and geographic locations.

To obtain further information or to order HPE Risk Assessment Service for cybersecurity, contact a local HPE sales representative and reference the service name.

LEARN MORE AT

hpe.com/services/security

Make the right purchase decision.
Contact our presales specialists.

Chat **Email** **Call**

Share now

Get updates

Hewlett Packard
Enterprise

© Copyright 2019 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

This data sheet is governed by the Hewlett Packard Enterprise current standard sales terms, which include the supplemental data sheet, or, if applicable, the Customer's purchase agreement with Hewlett Packard Enterprise.

Microsoft is either a registered trademark or trademark of Microsoft Corporation in the United States and/or other countries. All other third-party marks are property of their respective owners.

a00067560ENW, October 2019, Rev. 1