



Service Description: Advanced Services – Fixed Price

Cisco Security Advisory Services: PCI-DSS Readiness Assessment

ASF-CORE-PCI-DSS

This document describes the fixed price Cisco Security Advisory Service: PCI – DSS Readiness Assessment .

Related Documents: This document should be read in conjunction with the following documents also posted at www.cisco.com/go/servicedescriptions/: (1) Glossary of Terms; (2) List of Services Not Covered. All capitalized terms in this description have the meaning ascribed to them in the Glossary of Terms.

Direct Sale from Cisco. If you have purchased these Services directly from Cisco for your own internal use, this document is incorporated into your Master Services Agreement, Advanced Services Agreement, or other services agreement covering the purchase of Advanced Services-based services with Cisco ("Master Agreement") If no such Master Agreement exists, then this Service Description will be governed by the terms and conditions set forth in the Terms & Conditions Agreement posted at www.cisco.com/go/legalterms. If you have purchased these Services directly from Cisco for resale purposes, this document is incorporated into your System Integrator Agreement or other services agreement covering the resale of Advanced Services ("Master Resale Agreement"). If the Master Resale Agreement does not contain the terms for the Purchase and Resale of Cisco Advanced Services or equivalent terms and conditions, then this Service Description will be governed by the terms and conditions of the Master Resale Agreement and those terms and conditions set forth in the SOW Resale Terms & Conditions Agreement posted at www.cisco.com/go/legalterms. For purposes of the SOW Resale Terms and Conditions this Service Description shall be deemed as a Statement of Work ("SOW"). In the event of a conflict between this Service Description and the Master Agreement or equivalent services exhibit or agreement, this Service Description shall govern.

Sale via Cisco Authorized Reseller. If you have purchased these Services through a Cisco Authorized Reseller, this document is for description purposes only; is not a contract between you and Cisco. The contract, if any, governing the provision of this Service will be the one between you and your Cisco Authorized Reseller. Your Cisco Authorized Reseller should provide this document to you, or you can obtain a copy of this and other Cisco service descriptions at www.cisco.com/go/servicedescriptions/.

PCI-DSS Readiness Assessment

Service Summary

Cisco will perform a Payment Card Industry ("PCI") Assessment of the Customer's Cardholder Data Environment ("CDE") to identify compliance deficiencies and provide recommendations to achieve compliance based on the then current PCI DSS Requirements and Security Assessment Procedures, shown at the PCI standards website located at https://www.pcisecuritystandards.org/pci_security/maintaining_payment_security.

The assessment will be performed at one (1) Customer business location and will include documentation review, up to 12 (twelve) key stakeholder interviews, and one (1) data or call center inspection.

Location of Services

Service will be delivered on-site at one Customer location.

Travel will be limited to no more than two (2) visits by Cisco of up to five (5) days total on-site at a single Customer location

Pre-Assessment Intelligence Gathering

Cisco Responsibilities

- Confirm that Customer has identified the people, processes and technologies that are considered in-scope in accordance with "Scope of PCI DSS Requirements" section of the current PCI DSS procedures document.
- Provide Customer a detailed checklist of required documentation for the purposes of this engagement.
- Review the Customer's PCI assessment and reporting requirements.

Customer Responsibilities

- Identify a project sponsor with responsibility for completion of the project and with the authority to make decisions concerning execution of the project.
- Provide a project manager to schedule stakeholder meetings and fulfill information requests.
- Prior to or at the project kickoff, Customer shall confirm access to resources identified as within scope, for the purposes of assessment against the PCI Data Security Standard.

- Provide Cisco with access to suitable office facilities for meetings, interviews, and facilitated sessions for work being conducted at the Customer location.
- Provide emergency contact information including name, title, e-mail, business and mobile phone numbers.

Assessment, Analysis & Testing

Cisco Responsibilities

- Perform analysis and document the scope for a PCI DSS Assessment by identifying the following:
 - Locations
 - Payment transmission connections
 - Payment channels
 - Personnel roles and responsibilities
 - Computer network segments
 - Cardholder data storage locations
 - Hardware and software
 - Service providers and third-parties
- Perform a detailed assessment of the Customer cardholder environment that will include:
 - Interviews with key Customer stakeholders
- Review of policies and procedures to identify existing gaps and remediation needed to meet PCI DSS compliance, based on the then-current PCI standards requirements as shown at the PCI standards website at https://www.pcisecuritystandards.org/pci_security/maintaining_payment_security.
- Conduct compensating controls analysis.

Post-Assessment

Cisco Responsibilities

- Develop strategic, operational, and tactical remediation action plan to address identified areas of non-compliance.
- Provide Customer with the PCI Compliance Readiness Assessment Report.
- Provide Customer an Executive Summary Presentation, not to exceed one (1) hour.

Customer Responsibilities

- Identify stakeholders to attend Executive Summary Presentation
- Review the PCI Compliance Readiness Assessment Report.

General Customer Responsibilities

- Customer represents and warrants that they have sufficient authority and the rights necessary for Customer to provide and/or facilitate Cisco's access to information, data, networks, systems, and media in connection with these Services.
- For all Customer requests under this Service Description that Cisco possess, access, or analyze particular media, computers, computer networks, communications networks, or other systems and equipment, to the extent Customer provides or facilitates Cisco's access thereto, Customer

represents, warrants and covenants that they have all necessary right, title, license, and authority to make such requests and grant such access, including all necessary permissions from third-party owners of licensed or shared resources.

- CUSTOMER IS RESPONSIBLE FOR OBTAINING ALL NECESSARY LICENSES, PERMISSIONS, AND CLEARANCES FOR CISCO TO ACCESS RESOURCES THAT ARE HOSTED, OWNED BY, OR SHARED WITH A THIRD-PARTY.
- Customer is responsible for provisioning of necessary test access, environments, VPN connections, user accounts, administrative access, or other required technical assets.
- All information (such as but not limited to: designs, topologies, requirements) provided by Customer is assumed to be up-to-date and valid for the Customer's current environment. Cisco Services are based upon information provided to Cisco by Customer at the time of the Services.
- Customer acknowledges that the completion of Services is dependent upon Customer meeting its responsibilities as indicated herein.
- Customer will identify Customer's personnel and define their roles in the participation of the Services. Such personnel may include but is not limited to: architecture design and planning engineers, and network engineers.
- Customer will ensure Customer's personnel are available to participate during the course of the Services to provide information and to participate in scheduled information gathering sessions, interviews, meetings and conference calls.
- Customer expressly understands and agrees that support services provided by Cisco comprise technical advice, assistance and guidance only.
- Customer expressly understands and agrees that the Services shall take place and complete within ninety (90) calendar days from issuing a Purchase Order to Cisco for the Services herein and any unused hours will expire.

Invoicing and Completion

Invoicing

Services will be invoiced upon completion of the Services.

Completion of Services

Cisco will provide written notification upon completion of the Services to Customer. The Customer shall within five (5) Business Days of receipt of such notification provide written acknowledgement of Cisco's completion of the Services. Customer's failure to acknowledge completion of the Services or to provide reasons for rejection of the Services within the five (5) Business Day period signifies Customer's acceptance of completion of the Services in accordance with this Service Description.

Assumptions and Exclusions

- Customer is solely responsible for determination and implementation of its network, design, business or other requirements and the implementation of any recommendations provided by Cisco. Cisco's recommendations are based upon Customer information provided to Cisco. Cisco shall not be liable for the accuracy or completeness of any Customer information contained in Cisco's recommendations.
- All documents will be provided in electronic form in the English language.
- Customer retains all responsibility for the security of Customer Technical Environment(s). Cisco shall have no responsibility for, or liability as a result of, any breach in security of Customer's Environment. Cisco cannot guarantee that Customer's security may or may not be

vulnerable from any included, omitted or overlooked instances whether or not presented in the Services or Deliverables associated with this Service Description.

- Security assessment services will not definitively prove the absence of vulnerabilities or definitively prove compliance (only readiness).