Service Description: Advanced Services – Fixed Price

Cisco Network Optimization Service – Risk Assessment (ASF-CORE-RS-NOSRA)

This document describes Advanced Services Fixed Price: Cisco Network Optimizations Service – Risk 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 http://www.cisco.com/legal/advancedservices.html. 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: http://www.cisco.com/legal/advancedservices.html. 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/.

Cisco Network Optimization Service – Risk Assessment

Service Summary

The Cisco Network Optimizations Service – Risk Assessment service identifies areas for network performance improvements by analyzing the underlying infrastructure components of a Customer's network. It is accomplished by collecting and analyzing inventory and configuration data and by performing a series of interviews with the network engineering, infrastructure groups. The interviews and data collection enables Cisco to evaluate the Customer's current network infrastructure including hardware, software, network topology and design, protocol and configuration resiliency.

Deliverables

Cisco shall provide the following Deliverables:

- Risk Assessment Analysis
- Risk Assessment Report

Location of Services

Services will be performed as a combination of Remote and On Site at one Customer Site.

Risk Assessment Analysis

Cisco Responsibilities

- Schedule and conduct a project kick-off meeting in order to commence the Risk Assessment.
- Submit a Request for Information ("RFI") Document to Customer in order to gather Customer requirements for data collection.
- Work with Customer to schedule and conduct on site interviews with identified Customer personnel.
- Perform on site set up and configuration of Cisco Common Services Platform Collector ("CSPC") for inventory and configuration data collection. The CSPC is provided by Cisco with the features enabled as the default configuration in order to collect data upon installation. Such collections will continue until such time as the CSPC has been uninstalled.
- Conduct weekly status calls.
- Perform the Network Components analysis for up to 2000 devices, in which Cisco will evaluate Cisco devices, modules, and versions of software that are currently deployed in the production network.
- Perform the Network Topology Analysis for up to 300 devices, to be identified jointly between Customer and Cisco to enable the most appropriate representative model(s) to be created. Cisco will evaluate the hardware connectivity resiliency at each network which includes: a) Network Redundancy; b) Network Diversity; c) Network Hierarchy
- Perform the Protocol and Configuration Resiliency Analysis for up to 300 devices, to be identified jointly between Customer and Cisco team to enable the creation of an appropriate representative model(s). These devices will be the same that are reviewed during the Network Topology Analysis. Analysis includes, a) Layer II Protocol Resiliency; b) Layer III Protocol Resiliency; c) High Availability Features Resiliency
- Perform the Network Device Security Analysis in order to analyze various aspects of the Cisco network device level security, which includes but is not limited to the following: a) Review of Customer's Network device security goals and requirements; and b) Analysis of network device configurations focused on security hardening of individual devices, analysis of firewall rules for common configuration issues, and analysis comparing current practices to recommended best practices.

Customer Responsibilities

- Provide completed responses to the RFI Document five (5) Business Days prior to the commencement of the on-site interviews. Customer acknowledges that completion of Services is dependent upon receipt of the RFI Document within the five (5) Business Day period above.
- Customer acknowledges that completion of Services is dependent upon Cisco's use of the CSPC data collection tool. Customer can elect to disable collection features of CSPC or uninstall CSPC at any time. By performing these actions, Customer understands that Cisco may be unable to provide certain elements of the Service and Cisco will not be responsible for performance of any obligations associated with CSPC and the resulting level of service delivery may be limited to that obtained from information and interviews provided by Customer.
- By installing the CSPC, the Customer acknowledges understand and agrees that Customer Network Information will be transmitted and used to generate reports regarding Customer's network and equipment. Upon installation on Customer's network, CSPC will immediately begin communicating to a Cisco server via secure encryption to enable Cisco to discover information about the Products within Customer's network and such collections will continue until such time as the CSPC has been uninstalled or collection features disabled. For purposes of this Service Description, "Customer Network Information" means information about Customer's network that is collected, stored and analyzed in connection with the Service and may include, without limitation, the following information: configurations (including running configurations and startup configurations), product identification numbers, serial numbers, host names, equipment locations, IP addressed, system contracts, equipment models, feature sets, software versions, hardware versions, installed memory, installed flash, boot versions, chassis series, exceptions to such information (e.g., duplicate host name, duplicate IP address, device running interim release image), slot IDs, card types, card families, firmware versions, and other network and inventory information as deemed appropriate by Cisco
- Provide the following information five (5) Business Days prior to the installation of CSPC:
  a) Seedfile – Network Product list in Seedfile format containing SNMP Read Only (RO) community string, CLI (vty/enable or TACACS userid/pwd) and other login credentials as applicable for access to all Product(s) in the Network;
  b) SNMP strings – SNMP and Command Line Interface (CLI) access to all Product(s) in the Network;
  c) Telnet or SSH credentials with privilege level 15 device access

- Make Customer network available for installation of CSPC; provide a secure area with limited physical access; provide for secure installation behind the Customer's firewall; and provide for access to all devices on the Network.
- Perform any required modifications of firewall rules and/or access-lists to CSPC to access all devices on the Customer network

Risk Assessment Report

Cisco Responsibilities

- Complete the Risk Assessment Report(s) to include: a) Hardware EoX; b) Software Infrastructure Analysis; c) Software Security Alerts (PSIRT); d) Field Notices; e) Best Practice Configuration Analysis; f) Network Device Security Assessment.
- Develop an Executive Summary PowerPoint outlining the technical findings of the assessment(s).
- Provide the Risk Assessment Report(s) and Executive Summary PowerPoint to the Customer, and conduct a presentation of the technical findings from the assessment(s).

Customer Responsibilities

- Review draft of deliverables identified in Cisco Responsibilities in this section.
- Coordinate and schedule presentation of findings with key Customer stakeholders.

General Customer Responsibilities

- Customer will allow Cisco to both use the collected Customer Network Information and related data in connection with performance of the Service described herein, to recommend additional products/services to assist Customer in the execution of related activities and generally for commercial and business purposes to the extent such Customer Network Information cannot be attributable to the Customer. To the extent any Customer Network Information collected is deemed Confidential Information, Cisco will protect the information consistent with the terms of the Agreement between the parties and Cisco's data retention policy.
- 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.
- 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.
- 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.
- 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.

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.