Service Description: Cisco Assurance Services/Operate Service

This document describes Cisco's Assurance Services/Operate Service.

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; and (3) Severity and Escalation Guidelines. 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, this document is incorporated into your Master Services Agreement (MSA) or equivalent services agreement executed between you and Cisco. In the event of a conflict between this Service Description and your MSA or equivalent services agreement, this Service Description shall govern.

Cisco's Assurance Services/Operate Service is intended to supplement a current support agreement for Cisco products and is only available where all Products in Customer's Network are Cisco-supported or supported by Cisco's Foundation Technology Service Provider Optimization Service. Cisco shall provide the Cisco Assurance Services/Operate service described below as selected and detailed on the Purchase Order for which Cisco has been paid the appropriate fee. Cisco shall provide a Quote for Services ("Quote") setting out the extent of the Services and duration that Cisco shall provide such Services. Cisco shall receive a Purchase Order that references the Quote agreed between the parties and that, additionally, acknowledges and agrees to the terms contained therein. Availability of Services described herein and service delivery may vary by geographical region.

Cisco can operate as a single Point of Contact or engage jointly with a third party whose responsibilities will be visible to the Customer. Appendix A provides additional information on multi-party engagements.

Cisco Assurance Services/Operate Service

Service Summary

The Cisco Assurance Services/Operate Service provides technology-specific help for Service Providers' support staff. Products supported under this service are limited to Cisco-supported products, as agreed with Service Providers.

The elements included in this service consisting of Incident Management, Problem Management, Proactive Change Management, shall be provided on-site or remotely from Cisco based service centers based on previous agreement with Customer.

Cisco Responsibilities

General Support

Cisco shall provide the following support for all Service modules selected by the Customer under the Cisco Assurance Services/ Operate:

- Designate a Network Operations Center (NOC) lead to act as the primary interface with the customer representatives including a Cisco project manager and an operations lead.
- Participate in regular visits with the Customer as required by the project manager both via phone or in-person quarterly and via phone weekly/bi-weekly/monthly based on customer request to review incidents, preemptive recommendations, contracted deliverables and activities, and to plan for next quarter. In person visits not to exceed four (4) on-site visits annually with an aggregate of eight (8) days. Additional visits will be mutually agreed at Cisco's then-current travel and labor rates.
- Consult with Customer networking staff in a series of meetings to develop a thorough understanding of Customer's Network design and implementation, with a focus on concerns such as resiliency, self-recovery, scalability, disaster recovery, business continuance, virtualization, application traffic requirements, and ability to handle increased traffic demands and prioritization via quality-of-service (QoS)
- Participate in periodic conference calls to review Customer's Network status, planning and the Services being provided.
- Monitor a Customer-specific Cisco email alias to facilitate communication with Cisco designated Services team.
- Network Consulting Engineer may utilize Customer provided data, scripts or internal tools to assist in collecting data from the network for device activation in the Cisco NOC tools.
- Provide real-time monitoring and measurement of network devices to detect events that are incidents and for preemptive problem management.
- Provide a service desk to interface with the Customer's service desk. This will be the single interface between the Cisco NOC team and the customer for all incidents.
- Provide real-time incident management to restore service as quickly as possible for Severity 1 and Severity 2 Incidents, as defined in Cisco's standard Severity and Escalation Guidelines. Incidents may be automatically created from network events by the Cisco's Proactive NOC platform or by the customer service desk.
- Provide real-time updates with the Customer operations team during severity 1 and severity 2 events. The update mechanism and process will be defined as an inter-team

process between Customer organizations and Cisco Assurance Services team.
- Cisco will follow mutually agreed change processes for implementing any changes as part of incident management.
- Provide real-time notification to Customer of mutually agreed events that may not have an immediate impact on network performance.
- Establish production connectivity between the customer network and the Cisco data center location using a secure VPN. Details to be worked between the customer and Cisco prior to go-live.
- Complete other startup activities as determined by teams during startup process to successfully monitor customer network. Activities include, but are not limited to, an operations readiness checklist to ensure that the customer network is ready for monitoring and Cisco operations.

Activation and Provisioning

- Provide **Activation and Provisioning**. Cisco will consult with Customer to provision and activate devices onto the production environment. Activation and Provisioning may include, among other activities, the following:
  - Review of end point service activation procedures.
  - Review of work orders for activation and provisioning of devices.
  - Support for activating the device.
  - Provisioning of the device.
  - Validating that the device is operational and ready to deliver service.

Incident Monitor & Notify

- Real-time email alerts capturing faults including event/incident information
- Monitoring of performance-related metrics and generating proactive alerts that identify potential future network performance issues
- Monitoring and notification via email alerts of availability-impacting events in real-time at device, network and service levels
- Monitoring of capacity-related performance and availability Key Performance Indicators (KPI) and generating alerts that predict potential future capacity issues
- Periodic reports of network monitored faults, including summary of analysis and recommendations
- Monthly/quarterly health trend reports demonstrating impact of recommendations for corrective action or optimization

Incident Management

- The objective of Incident Management is to restore service as quickly as possible (an incident is active until service is verified as restored). An incident is defined as any unplanned interruption to a service or reductions in the quality of a service—any event that could affect a service in the future is also an incident (e.g., redundant port fails).

- The order of steps for each incident (and some steps are not always necessary) are:
  1) Identification
  2) Logging
  3) Categorization
  4) Prioritization
  5) Initial Diagnosis
  6) Functional Escalation
  7) Investigation Diagnosis
  8) Resolution Recovery
  9) Closure

- Cisco NOC operators use their access to Customer's managed devices to investigate the incident and make any configuration changes required to restore service. Cisco operators will comply with mutually agreed requirements in terms of device access, change notice, and change control.

- In the event that the Customer has Cisco TAC support and RMA support, Cisco incident management includes calling the TAC, arranging for the part replacement, and verification of the replacement.

- Incident resolution may require Cisco NOC engineers working directly with Customer engineers to address fault and performance issues on the entitled managed component or to assist with remediation of capacity incidents detected on the Customer's network. The Customer is ultimately responsible for addressing any capacity issues flagged by Cisco NOC engineers.

- Cisco provides periodic reports of fault resolution with Root Cause Analysis ("RCA") down to a Cisco-specified level, and action reports for corrective actions.

- Cisco provides monthly and quarterly health trend reports (demonstrating impact of corrective actions). For the purpose of reporting, proactive events are those where an incident was detected by the NOC and resolved without any customer impact. Reactive events are those that are identified by the customer where the customer service desk notifies the Cisco NOC.

- Change management required for Incident resolution is included as part of this service.

Problem Management

- The objective of Problem Management is to identify underlying network problems before they cause events and avoid network incidents.

- Cisco will perform real-time monitoring of the Customer network including ICMP and SNMP polling and Syslog

collection. Information from the polling, SNMP traps, and received syslogs will be used for network optimization at the network (control plane) level for Cisco devices.

- Cisco NCEs will use this information to make actionable recommendations to the Customer to preemptively avoid problems in the network. Examples of these recommendations include, but are not limited to:
    - Redundant links are running over 50% utilization which would cause Customer impact in the event of one link failing. Recommended action would be to add link capacity or rebalance network traffic to other links.
    - Interface flapping. The interface may be "working," but is flapping excessively causing degraded service and indicative of a bad cable or impending hard failure. Recommended action could be to check the cable or contact the Cisco TAC.
- Memory utilization increasing and trending to memory exhaustion. Recommended action could be the addition of memory to the device, removing unused routes from the configuration, moving traffic to another device, or the need for another device.

Proactive Change Management

- Proactive Change management includes one software upgrade per year for devices under consideration. Cisco will provide design and upgrade leadership on devices under consideration. This will include:
    - Review with the Customer on their desired upgrade process
    - New features within upgraded feature-set
    - Potential caveats
- Cisco will perform the change including any change notification and fallback procedures. Cisco agrees to perform the changes at a time agreeable with the Customer.
- Change management required for Incident resolution is included as part of Incident Management.
- Change management for customer-requested changes can be included upon request and involves additional charges.

Configuration Change Management

- Implementation of corrective action to change software versions, software configuration, hardware attributes, and/or procedures. Service components include:
    - Configuration health checks
    - Configuration archive & restore
    - Configuration change execution
    - Configuration change reports
    - Configuration change scheduler

Customer Responsibilities

General Responsibilities

- Prior to performance of Cisco Assurance Services/Operate by Cisco, Customer must provide all required documentation as specified in Appendix B for Cisco approval.
- Ensure that the devices under scope of the service are functioning properly as per the criteria listed in Appendix B, as applicable.
- Designate at least one (1) technical representative in each area covered under the Cisco Assurance Services/Operate, who must be a Customer employee in a centralized Network support center (Customer's technical assistance center), to act as the primary technical interface to the Cisco Network Consulting Engineer(s). Customer will designate as contacts senior engineers with the authority to make any necessary changes to the Network configuration. One individual, who is a senior member of management or technical staff, will be designated as Customer's primary point of contact to manage the implementation of services selected under this Service Description (e.g., chair the weekly conference calls, assist with prioritization of projects and activities)
- Be responsible for following mutually agreed upon engagement processes.
- Be responsible for coordinating on-site activities.
- Provide direct and continuous remote network access to allow Cisco's service platform to gather appropriate information
- In the event Cisco provides Data Collection Tools or scripts located at Customer's site, ensure that such Data Collection Tools or scripts are located in a secure area, within a Network environment protected within a firewall and on a secure LAN, under lock and key and with access restricted to those Customer employees(s) or contractor(s) who have a need to access the Data Collection Tools and/or a need to know the contents of the output of Data Collection Tools. In the event Data Collection Tool provided by Cisco is Software (if mutually agreed for future deployments), Customer agrees to make appropriate computers available and download Software as needed. Customer shall remain responsible for any damage to or loss or theft of the Data Collection Tools while in Customer's custody.

- Provide configuration information and information on features implemented as needed.

- Notify Cisco Network Consulting Engineer of any major Network changes (e.g. topology, configuration, new IOS releases).

- Identify and communicate business requirements necessary for Cisco to monitor required Key Performance Indicators (KPIs) for each service.

- In the event the Network composition is altered after the Services selected under this Service Description have become effective, Customer is responsible to notify Cisco in writing within ten (10) days of the change. Cisco may require modifications to the fee if the Network composition has increased beyond the scope covered by the original pricing quote for Services.

- Create and manage an internal mail alias for communication with Cisco Network Consulting Engineer.

- Retain overall responsibility for any business process impact and any process change implementation.

- Be responsible for all issue resolutions requiring onsite field presence.

- Provide details of customer requirements on the program(s) it wants Cisco to manage.

- Provide access to all relevant Customer material, equipment, facilities and personnel required to manage the program(s).

- Provide information on current releases running in the Network and current configuration templates.

- Provide information on Customer business and technical requirements for new Software releases.

- Provide details of Customer requirements on the topics it wants to see covered through transfer and mentoring together with background information on the skill sets of the audience.

- Ensure that facilities and equipment are available to host the informal technical update sessions.

- Provide information on Customer certification process and lab testing process.

- Provide information on Customer change control process if change management is to be implemented by Cisco NOC personnel.

- Be responsible for implementing actionable recommendations provided by Cisco. Incidents that occur for which the underlying problem was preventable through implementing an actionable recommendation from Cisco will not be included as network events for SLA calculations.

Appendix A

Third Parties

The following shall apply only where Cisco and the Customer agree on a multi-contract engagement.

- For third-party devices that Cisco's Assurance Operate team manages, Cisco shall perform "tier-1" incident management. Should the prescriptive steps not restore service, Cisco's Assurance Operate team will escalate incidents to the customer help desk or the third-party support team for resolution. In the case of escalating to a third-party support team, Cisco's Assurance Operate team shall stay engaged through service restoration.

- The Customer shall be responsible for maintaining support contracts with third-party vendors for non-Cisco devices.

Appendix B

Readiness for Hand-off - Cisco Assurance Services/Operate

Network Operational Status
The customer will document an Operational Readiness Test (ORT) or similar process that certifies that the network is ready for operation. All network equipment will be installed and verified as operational.

Documentation

- Provide High Level Design and Low Level Design for the network including device names, IP addresses, SNMP passwords, configuration, and any other documentation.
- Provide as-built documentation including device names, IP addresses, SNMP passwords, device configurations, and any other network documentation.
- Provide POD-specific documentation.
- Provide as- built documentation:

Device Documentation and Configurations

- Configuration information for all devices
- Operations team access into all devices
- TACACS configured and functional
- Host Names must match "as built" documentation
- MOTD banner (if applicable) should be configured correctly

- Syslogs enabled on all devices and pointing to Cisco NOC
- SNMP traps enabled on all devices and pointing to Cisco NOC
- All devices reachable from the Cisco NOC for ICMP and SNMP polling