



Cisco Remote Management Service - Remote IT-Infrastructure Management Services

1.0 Introduction

This document describes Cisco's Remote IT-Infrastructure Services for the Cisco Remote Management Service and the processes used by the Cisco NOC to provide basic management of a Customer Managed Components. This Service Description is designed to provide a baseline understanding of the activities and deliverables associated with the processes that make up Remote IT-Infrastructure Management and to set expectations about the Service. Please read this document carefully as it contains important information regarding the Services that you have purchased from us.

Capitalized terms are defined in the [Glossary of Terms](#).

Remote IT-Infrastructure Management Services for the Cisco Remote Management Service are divided into three major parts: Remote Management Activation, Remote IT-Infrastructure Management, and the Portal. In addition, there are Customer responsibilities that must be met to deliver the Service. Except where specified, all of the processes described in this document are delivered as part of Remote IT-Infrastructure Management. There are also specialized Services that build on the core Service. Specialized Services are purchased separately and are bundled with the core Service described in this document depending on the needs of the Customer and the technologies requiring management.

Core Service	Specialized Services
Remote IT Infrastructure Management Services	IP Telephony

2.0 Remote Management Activation

The Remote Management Activation is a process in which Cisco prepares a Customer's IT infrastructure for Cisco management. Over time, Cisco experts have determined the best practices for preparing a Customer's infrastructure and then created a framework from these best practices for use in managing and activating a Customer's IT infrastructures. Using our framework enables an efficient and low-impact effort of enabling a Customer's IT infrastructure to receive Cisco's management Services. This framework includes:

- Discovering the IT infrastructure.
- Planning the transition to management.
- Implementing management operations.

2.1 Discovering the IT Infrastructure

Discovering the IT infrastructure includes the pre-implementation activities that provide Cisco with a high-level understanding of the Customer's business and IT infrastructure needs. This assists our team in having an accurate understanding of the Customer's requirements before the planning and implementation processes begin.

Activities:

- Have initial engagement with the Customer.

Deliverable(s):

- Introduction package.

2.2 Planning the Transition to Management

The purpose of planning the transition is to prepare both the Customer and the NOC for a smooth management transition. This process involves collecting and validating all technical details required to enable remote IT infrastructure management, ensuring the Customer has a clear understanding of Service features, and establishing joint interaction methods. Each site will be assessed to ensure that no further work is needed before the site is turned up under management.

Activities:

- Establish key relationships with Customer.
- Work with the Customer to develop an implementation plan.
- Gather the key site information from Customer.
- Gather the key Managed Component information from Customer to provide management.
- Enter the Customer's Managed Component information into the applicable NOC databases.
- Define an escalation plan for the NOC and the Customer.
- Define the Change Management Process.
- Complete applicable Letters of Agency

Deliverable(s):

- Letter of Agency on file in NOC.
- Escalation plan published to Customer.
- Transition plan.

2.2.1 Remote-Infrastructure Operations Readiness Approval

Prior to implementing management operations, the NOC will either approve an existing managed site or make recommendations required for accepting a new managed infrastructure. If the necessary changes are not made, acceptance of the order may be withdrawn. If the Customer wishes to engage Cisco to implement the recommendations, a separate Agreement to make the changes may be required.

2.3 Implementing Management Operations

Implementing management operations involves executing the transition project plan developed in the planning the transition to management process. To provide a single point of contact to apply ongoing focus on established timelines and commitments, the NOC will appoint a designated project coordinator.

During this phase, the NOC will establish management connectivity and ensure Customer contacts are aware of how to interact with the NOC during delivery of the Service.

Activities:

- Establish management access for each Managed Component through the Customer provided site management channel. (See Section 5.2 - "Connectivity.")
- Review and verify the configuration of all Managed Components.
- Work with the Customer on any initial management configuration issues and/or changes required for successful management.
- Test and accept each Managed Component for ongoing operations management coverage.
- Begin ongoing Incident monitoring of Managed Components. (See Section 3.1 - "Incident Monitoring.")

Deliverable(s):

- Publish scheduled events on the Portal.
- Train Customer employees on use of the Portal.
- Provide the Customer with a complete inventory of Managed Components, published on the Portal.

As necessary for the NOC to perform its responsibilities as stated in this Service Description, the NOC will maintain an information repository of data with respect to the Customer and the Managed Components.

3.0 Cisco Remote IT-Infrastructure Management

Cisco Remote IT-Infrastructure Management serves as the core management process for all Cisco Managed Components. Additional specialized Services add to the processes described in this document and can be purchased separately.

All Services are designed to be delivered from the NOC and require remote access and control. These Services apply to infrastructure devices such as routers, switches, infrastructure application servers, and specialized security technologies such as firewalls and intrusion detection/prevention technologies. Certain Service components and specializations may only be applicable to certain devices.

The Service consists of the following Service components:

3.1 Incident Monitoring

The objective of Incident monitoring is to detect Incidents that initiate the Incident management process.

Selected elements of Managed Components will be proactively monitored for status 24 hours per day, 365 days per year. Where available, availability and performance indicators will be collected from Managed Components. When an Incident is detected, the Incident is correlated.

The Customer and the Partner may report Incidents on Managed Component(s) as Service requests. Service requests may be made on the Portal.

Activities

- Monitor (24x7x365) selected elements proactively on all Managed Components.
- Detect Incidents.
- Correlate Incidents where applicable.

Deliverable(s)

- Confirmed Incidents.
- E-notification of confirmed Incidents.

3.2 Incident Management

Incident management is the process the NOC uses to solve real-time Incidents in Customers' Managed Components. The goal of Incident management is to restore normal Service operation as quickly as possible with minimum disruption to the business and to strive for the highest levels of availability and satisfaction.

The Incident management processes include multiple levels of support provided by the NOC. It also includes creating, maintaining, and publishing documents that indicate the status of the Incident through the resolution and closure process.

3.2.1 Opening Incidents as Tickets

The NOC works through the Incident management process to resolve Incidents. Incidents are correlated and confirmed by the Incident monitoring process.

Activities:

- View Tickets online via the Portal.

- Perform E-notification for Ticket events, if requested by Customer.

3.2.2 Notification

Cisco E-notification is available for Customers to receive information about Tickets and Incidents for all Incident-management stages. Cisco also provides access to the Portal for status updates.

Activities:

- Perform E-notification for Ticket events, if requested by Customer.

3.2.3 Priorities

Tickets will be worked in order of priority. Priorities are set by the NOC on a per-Ticket basis depending on a variety of factors including: severity, scope of impact, and SLAs.

3.2.4 Isolation

The NOC will isolate and locate the cause of the Incident. Once isolation has occurred, the NOC will update the Ticket with information related to the isolation and then proceed to the resolution phase.

Activities:

- Update Portal Ticket to include isolation information.
- Perform E-notification for Ticket events, if requested by Customer.

3.2.5 Resolution

After the Incident has been isolated, the NOC will work to resolve the Incident. Resolution is complete when functionality is restored. The resolution process includes any action the NOC requires to restore functionality or implement a work-around.

The NOC will utilize work-around solutions to restore all or partial functionality when full functionality cannot be restored within SLAs. When a work-around is utilized, the Incident will continue to remain open and will be worked by the NOC until resolved.

- Should the NOC require a change in a Managed Component to resolve an issue or implement a work around, the NOC will refer to the Change Management Process, ([See Section 3.4 – “Change Management.”](#))

Activities:

- Resolve Incident
- Submit, when needed, a Change Management authorization request and referral to the Change

Management Process. ([See Section 3.4 – “Change Management.”](#))

- Update Portal Ticket to include resolution notes.
- Perform E-notification for Ticket events, if requested by Customer.

3.2.5.1 Dispatch

The NOC will dispatch vendors as needed and appropriate within the resolution steps prescribed by the NOC. As vendors are dispatched, the Ticket will be updated with information related to the dispatch.

Activities:

- Update Portal Ticket to include dispatch notes.
- Perform E-notification for Ticket events, if requested by Customer.

3.2.5.2 Escalations

The Customer or the Partner may request escalation of a Ticket on the Portal at any time.

Activities:

- Update Portal Ticket to include escalation notes.
- Perform E-notification for Ticket events, if requested by Customer.

3.2.6 Validation

After the Incident has been declared resolved by the NOC, the NOC will validate the Managed Component(s) to verify that the Incident has been resolved.

If the result of the validation verifies that the Incident has been resolved, the Ticket will be updated with information related to the validation. If the result of the validation reveals that the Incident has not been resolved, the Incident will be returned to the Resolution process for continued work until resolved. ([See Section 3.2.5 – “Resolution.”](#))

Activities:

- Update Portal Ticket to include validation notes.
- Perform E-notification for Ticket events, if requested by Customer.

3.2.7 Closing Tickets

After the Incident has been resolved and verified in the validation process, the Ticket closure procedure begins. Before the Ticket is closed, the Customer must agree that the Incident is resolved.

When the NOC declares the Incident resolved and verified, an E-notification is delivered to the Customer, and the Ticket is placed in a state of auto closure. If the Customer does not respond to the E-notification within the Customer-defined

timeframe, the Customer agrees that the Ticket will be closed without further action.

If the Customer wishes to hold closure of the Ticket before the auto-close window expires, the Customer may request through the Portal that the Ticket be held and then add additional information relevant to the Incident. The NOC will contact the Customer to request additional information as needed.

Any authorized Customer agent may also proactively request Ticket closure on the Portal for any Ticket. The NOC will review the request and close the Ticket or follow up with the Customer for more information as needed.

Activities:

- Update Portal Ticket to include closing notes.
- Perform E-notification for Ticket events, if requested by Customer.

3.3 Problem Management

Problem management is the process used by the NOC to identify and solve recurring problems. The objective of Problem management is to identify problems for the Incident management process to address, leading to a decline in Incidents from recurring problems.

The NOC will analyze Incident trends to identify patterns and systemic conditions. In the event a trend is detected, the results will be introduced into the Incident-management process for resolution.

Activities:

- Analyze trends for Incidents on Managed Components.
- Identify recurring Incidents and refer to Incident Management for resolution.

Deliverable(s):

- Creation of a Ticket on the Portal for the Customer to view.
- E-notification for Ticket events, if requested by Customer.

3.4 Change Management

Change Management is the process used by the NOC to ensure standardized methods and procedures for authorizing, documenting, and performing all changes. The objective of Change Management is to make necessary changes in an efficient and accountable manner, utilizing standard processes. For further information on Change Management, please refer to the [Cisco Change Management Services](#) description.

3.4.1 Change Origination

The first step in Change Management is the origination of a Service request. Change requests originate from two

categories: Cisco-recommended changes and Customer-requested changes. The change-origination process describes the handling of each change category.

For each change category, a Ticket is created or updated for the Customer to track the progress of the change.

Deliverable(s):

- Creation of a ticket on the Portal for the Customer to view.

3.4.1.1 Cisco-Recommended Changes

Cisco-recommended changes originate from the NOC. Before executing a Cisco-recommended change, the NOC will evaluate the change and make a recommendation to the Customer that includes the criticality and timeframe for implementation. The NOC will not execute a change until the Customer has authorized the change to be made.

Cisco-recommended changes include:

- Resolve an Incident.
- Respond to a critical vulnerability.
- Apply a signature update to a security Managed Component.
- Address a problem.

Activities:

- Provide the Customer with recommendations to make changes.
- Schedule recommended changes.

3.4.1.2 Customer-Requested Changes

Customer-requested changes originate from the Customer's authorized agents and employees.

The Customer can use the online Change Management Process on the Portal to request Customer-requested changes. The NOC will evaluate the change request and work with the Customer to schedule the change.

A process that includes costs, timeframes, and guidelines for the work to be completed governs all Customer-requested changes. These guidelines ensure that the NOC receives proper notice to arrange the required resources to complete the work and that the work is performed in a timely manner. The specifics of the Change Management Process, including any additional costs, are outlined in the Cisco change management document.

Customer-requested changes include:

- Physically Add, Delete or Change component on existing Managed Component.
- Change existing logical functionality (upgrades).
- Physically Move Managed Component.

- Add Managed Components.
- Addition of new functionality.
- Remove Managed Components.

Activities:

- Work with Customer to understand their Change Management Process.
- Provide a process for requesting changes via the Portal.
- Schedule change requests.

3.4.2 Executing changes

After changes are executed, the NOC will test the change and notify the Customer that the change has been executed. Once the Customer accepts the change, the Ticket will be closed. The status of changes can be viewed on the Portal.

Activities:

- Process and login requests via the Portal.
- Maintain a change database visible through the Portal.
- Assess impact of changes.
- Classify change requests.
- Authorize and schedule change requests.
- Coordinate changes.
- Update Portal Tickets to include change status.
- Review and close change requests.

Deliverable(s):

- Executed change.
- Portal Ticket updated with change notes.

4.0 Web Portal

Cisco provides an online Portal for Customers and Partners to review Tickets, Ticket metrics, and reports for their Managed Components. Additional reports may be included with the Service based on the Customer's contracted Services.

Deliverable(s):

- Portal logins for each of the Customer authorized employees.
- Inventory information on the Portal (as available).
 - o System description.
 - o Maintenance vendor.
 - o Maintenance coverage type and contract number.

- o Serial number.
- o IP Address.
- o Last date of configuration archival.

- Ticket information on the Portal (as available).
 - o Ticket identification number – The tracking number assigned by the NOC to each Ticket.
 - o Ticket opened date and time – The date the Ticket was opened.
 - o Ticket description – A brief description of the Incident(s) represented in the Ticket.
 - o Cause of Incident – Where known, the underlying cause of the Incident.
 - o Ticket status – The current status of the Ticket.
 - o Site(s) affected – Within the Ticket, the site locations where Managed Components are affected.
- Reports on the Portal (as available).
 - o Performance Analysis – Data analysis reports that graph key Managed Component metrics such as utilization and performance.
 - ☛ Daily.
 - ☛ Weekly.
 - ☛ Monthly.
 - o Monthly Engineering Analysis - An automated monthly report containing engineering recommendations including high and low exceptions.
 - o Availability – The uptime of Managed Components.
 - ☛ Individual Device – Availability for a single Managed Component.
 - ☛ Device Type – Availability for a group of Managed Components of the same type.
 - o Exceptions – High and low exceptions for utilization and errors.
 - ☛ Individual Device – Exceptions for a single Managed Component.
 - ◆ Daily.
 - ◆ Weekly.
 - ☛ Device Type – Exceptions for a group of Managed Components of the same type.

- ◆ Monthly High.
- ◆ Monthly Low.
- o Ticket Metrics.
 - ✦ Mean Time to Notify – The average time to notify the Customer of Tickets across a selected timeframe.
 - ✦ Mean Time to Test – The average time to test Managed Components during Incidents across a selected timeframe.
 - ✦ Mean Time to Isolate – The average time to isolate Incidents across a selected timeframe.
 - ✦ Mean Time to Resolve: Single Event – The average time to resolve single event Incidents across a selected timeframe.
 - ✦ Mean Time to Resolve: Multiple Events – The average time to resolve multiple event Incidents across a selected timeframe.
 - ✦ Ticket Cause Analysis – A graph of the causes of Incidents.
 - ✦ Ticket Origination Analysis – A graph of the originators of Tickets.
 - ✦ Ticket Volume: Top 10 Sites – Volume of Tickets across the most highly Ticketed sites.
 - ✦ Tickets: Open vs. Closed – Tickets opened and closed per day across a selected timeframe.
 - ✦ Work Ticket Summary – The Work Ticket Summary report shows a summary of work Tickets over a specified period of time. You can use the report to view all the non-outage related work performed during a given time period.

5.0 Cisco Provided Management Connectivity

Management Connectivity establishes bi-directional communication between the Customer premise and Cisco NOC for management data to be securely and consistently transmitted between Managed Components and Cisco. Management Connectivity is broken into three areas: [primary connectivity](#), [backup connectivity](#), and [overall security](#).

The Managed Component where the Management Connectivity channel terminates must have access to the remaining Managed Components. Management Connectivity requires access to specific ports and protocols; such requirements will be reviewed with Customer during the transition management process.

5.1.1 Primary Management Connectivity

Primary Management Connectivity will be provided by Cisco. At Cisco's discretion, one of two options will be selected based on the type of managed service.

- o A dedicated circuit between the Cisco Point of Presence (POP) and the Customer-designated handoff. The handoff will be at the Customer data center or other supported network termination point.
- o A virtual connection via a Virtual Private Network (VPN) between the Cisco POP and Customer network.

Each option will include a Cisco-provided termination device located on the Customer premises. The size of the connection between the Cisco POP and Customer handoff will depend on the type of managed service and number of Managed Components.

5.1.2 Termination Device

Management Connectivity typically requires that a Cisco-provided termination device, commonly referred to as Customer Premises Equipment (CPE), be installed at Customer site to terminate the Management Connection. CPE will be defined as any Managed Component supplied by Cisco that resides at the Customer Premises. Customer will use reasonable efforts to provide and maintain the CPE in good working order. The Customer shall not, nor permit others to, rearrange, disconnect, remove, attempt to repair, or otherwise tamper with CPE. Should this occur without first receiving written consent from Cisco, the Customer will be responsible for reimbursing Cisco for the cost to repair any damage thereby caused to the CPE.

Cisco, or its subcontractors, shall be allowed access to the Customer premises (location occupied by Customer or Customer's end user) to the extent reasonably determined by Cisco for the inspection or emergency maintenance of Cisco-supplied CPE.

5.1.3 Back-up Management Connectivity

Backup Management Connectivity and out-of-band access is required to provide continued managed service in the event that the primary Management Connectivity channel is unavailable.

Prior to the Go-Live Date, at each site where Managed Components are located, Customer must provide out-of-band access to Managed Components in the form of a 1FB phone line or dedicated Private Branch Exchange (PBX) extension with Direct Inward Dialing (DID) capabilities. The out-of-band access phone line must be connected to a Cisco-approved, dedicated dial modem provided by the Customer. Where out-of-band access is not provided, Service Level Objectives ("SLO") will not be provided for Managed Components.

There are two options for backup Management Connectivity:

- Dedicated Backup Management Connectivity

If Customer selects a Dedicated Management Connectivity option, the Dedicated Backup Management Connectivity channel should be physically diverse from the primary Management Connectivity channel. Physical diversity is defined as ensuring that the Dedicated Backup Management Transport Facility (Frame Relay, DS1, DS3, etc.) uses an alternate path and transits a different central office and “last mile” connection than Customer’s primary Management Connectivity provider. The Dedicated Backup Management Connectivity channel will terminate in an alternate Cisco POP from the primary Management Connectivity channel. If an Incident is detected, the Cisco service desk will provide and work Incident Management activities through the Backup Management connection until resolved. The Dedicated Backup Management Connectivity channel will be subject to the same minimum bandwidth requirements as specified based on the Service being provided.

- Virtual Private Network Backup Management Connectivity

If Customer selects a Virtual Private Network Backup Management Connectivity option, the Virtual Private Network Backup Management channel should be physically and logically diverse from the primary Management Connectivity channel. Logical diversity is defined as utilizing a different Tier 1 ISP than Customer’s primary Management Connectivity provider.

The Virtual Private Network Backup Management Connectivity channel will terminate in an alternate Cisco location from the primary Management Connectivity channel. If an Incident is detected, the Cisco service desk will provide and work Incident Management activities through the Backup Management connection until resolved. The Virtual Private Network Backup Management Connectivity tunnel will be subject to the same minimum bandwidth requirements as the primary Management Connectivity tunnel.

5.1.4 Customer Responsibilities - Connectivity

- Providing all reasonable access to premises where CPE and/or circuit are located.
- On day of termination, should Customer deny access to Cisco representative, being responsible for additional fees for further dispatches.
- Being responsible for provisioning and maintaining the electric power consumed by CPE.
- Providing out-of-band access to Cisco-provided CPE device

5.1.5 Cisco Responsibilities - Connectivity

- Ordering Management Connectivity circuit on behalf of Customer; size of circuit based on type of managed services and number of Managed Components.
- Shipping appropriate CPE to Customer site and arranging for a technician to install the CPE and terminate the Cisco-provided Management Connectivity circuit.
- Documenting and, if requested, providing circuit facility assignment information.
- Maintaining reasonable security provisions to secure the Management Connectivity.
- Performing a pre-implementation discovery, designed to provide Cisco with an understanding of the Customer network and environment.
- Providing a Quarterly Management Connectivity report.

5.1.6 Metrics

The following are the metrics that will be gathered for the Management Connectivity.

- Latency
- Errors
- Circuit capacity
- Backup connectivity test reports
- Availability

5.1.7 Security

The systems and processes used to provide managed services have been designed to be secure and stable. The approach outlined below describes Cisco’s preventative measures for aligning the systems at Cisco with appropriate security standards.

- Physical
 - Building Controls - Cisco utilizes a global Enterprise Lenel Security System that consists of Access Control and Video Management. All perimeter entrances are controlled/monitored by a card reader (with camera) or an Emergency Exit (door contacts with siren). The Access Controller communicates with the regional server via Cisco’s WAN. The CCTV video is digitally archived on Lenel Network Recorders (LNR).
 - Badge Access - All card readers require a Cisco Prox badge for access. A badge will only be issued to an employee or contractor after the individual completes an HR badge

application and passes a background check. At this point, the person is entered into the Cisco HR database. The HR database interfaces with the Lenel Access Control System to create the person's badge record.

- Physical separation - Cisco space is divided into 3 basic areas comprised of:
 - Public space – Lobbies that are occupied by a Lobby Ambassador (Receptionist), allow the public access during business hours. After hours, the perimeter lobby doors are under card reader control.
 - Cisco General Access – These areas are accessible to all Cisco employees and badged contractors.
 - Cisco Restricted Access – These areas are restricted to personnel that have a business need for badge access. Approval for badge access is evaluated and granted by the department/person that is the registered owner of the specific restricted area.
- Facilities Monitoring - All Cisco security systems are monitored by the corresponding regional Cisco Security/Facility Operation Center (SFOC). The SFOCs are staffed 24x7.
- Network Security - Networks are segmented and are under controlled access through the use of layer-2 through layer-7 control mechanisms. The Network is subdivided into the logical segments based on data criticality. Access to each Network is based on mandatory access controls that are based on the user role and business need. Network controls are reviewed on a periodic basis by both internal and external assessment teams.
- Operating System - Operating systems are controlled through centralized account management and accessed through encrypted channels. Each operating system build is based on a hardened systems image. Each image enforces minimum services and daemons for the function of the system and utilizes host-based anomaly detection systems to prevent malicious activity. Operating systems are reviewed on a periodic basis by both internal and external assessment teams.
- Applications - Applications are controlled through the use of user role-based access control and enforced through the use of strong password policies. Connections to applications are through encrypted channels. Applications undergo a periodic code review and threat assessment on a bi-annual basis.
- Data - Data access is enforced through the use of role-based access control lists that integrate with centralized account management systems. Data integrity and availability is controlled through a nightly

backup schedule. Data classification is based on the Cisco information classification policy.

5.1.8 Limitations

- Under any circumstances, Cisco will not be held liable to the Customer or any other parties for the interruption of Service, missed SLAs or Service Level Objectives ("SLO"), or for any other loss, cost, or damage that results from the improper use, maintenance of the CPE or delay in access to CPE.
- Unless otherwise agreed upon, title to all CPE shall remain in Cisco's possession. The Customer shall be responsible for provisioning and maintaining the electric power consumed by CPE. Cisco expects that, at the time of removal, the CPE shall be in the same condition as when installed, with the expectation of normal wear and tear. Customers will reimburse Cisco for the depreciated costs of any CPE that is deemed beyond normal wear and tear.

6.0 Customer Provided Management Connectivity (Optional).

In the event Customer elects to assume responsibility for providing Management Connectivity, Customer must comply with the following requirements:

To ensure that the NOC is enabled to provide Services for Managed Components, Cisco requires Customers to supply information, communications, and connectivity. These requirements are critical to the NOC to provide optimal, and in some cases any, Services.

6.1 Equipment

- Customer is responsible for providing and maintaining the hardware and software to be managed as Managed Components including maintenance coverage on the Managed Components.
- Customer is responsible for the physical security of the Managed Components.
- Customer must agree to allow Cisco to retain and publish aggregate statistics and metrics for non-identifiable trending analysis.
- Customer is responsible for providing back-up procedures and configuration data for Managed Components that do not have configurations that can be archived remotely. The NOC will work with the Customer to provide back-up procedures for these Managed Components so that these configurations are available for recovery from disk drives on other servers or on-site tape systems at the Customer's premises. The Customer is responsible for ensuring that these backups run correctly.
- If the Customer requires Cisco to provide optional staging Services, or requires equipment to be sent to Cisco, the Customer agrees to ship equipment via pre-paid freight to and from the Cisco locations.

6.2 Connectivity

- The Customer is responsible for providing one or more management channels, such as a frame relay PVC or a dedicated VPN tunnel, to a Managed Component at a site of the Customer's network. The size of the management channel can vary depending on the number and type of Managed Components and the Services purchased.
- The Customer should provide out-of-band access to Managed Components in the form of a 1FB phone line or dedicated PBX extension with DID capabilities prior to the installation date at each site where Managed Components are located. The out-of-band access phone line must be connected to a dedicated dial modem provided by the Customer or purchased from Cisco.
- The component where the management channel terminates must have access to the other managed devices.
- Cisco's Remote IT-Infrastructure Management Service is delivered using a collection of protocols and ports. All of these designated entities are required in order to receive Cisco's full suite of management Services.

6.3 Access to Managed Components

- The Customer is responsible for providing appropriate access to all Managed Components.
- The Customer must agree to non-disruptive inquiries for inventory asset discovery of Managed Components.
- Customer must be willing to use an access-control server to ensure configuration changes are logged in environments where multiple parties share access to Managed Components.
- Customer must provide appropriate access to managed devices to allow remote archiving of IOS device configuration files. Remote archiving enables Cisco to rapidly recover from device corruption or failure.
- Customer is responsible for providing technical or non-technical "virtual arms and legs" at remote sites to assist the NOC in tasks that cannot be performed remotely.

6.4 Support for Non-Managed Components

- Cisco does not provide any support for Non-Managed Components. Cisco has a professional Services process for handling support requests.

- The Customer is responsible for managing any Non-Managed Components.

6.5 Communications

- Customer is responsible for working with Cisco to allow Cisco's Change Management Process to work within the confines of the Customer's Change Management Process. Cisco takes a co-management approach to managed Services allowing Customers and other Customer-approved vendors to retain access to the Customer's devices. Because multiple parties can make changes to the environment, Cisco requires that anyone with access to the Customer's environment follow a consistent and documented Change Management Processes. This process will be reviewed and agreed upon prior to completion of the implementation process.
- Customer is responsible for supplying the NOC with changed data with respect to the Customer and Managed Components, as needed, via the Portal.
- Customer is responsible for the timely delivery of information required for configuration of Managed Components-notification procedures.
- Customer should notify the NOC 72 hours in advance of any scheduled maintenance
- Customer maintains sole responsibility for informing Cisco of Customer employee status changes.
- Customer is responsible for providing and maintaining a list of Customer employees authorized to request changes.
- Customer is responsible for providing and maintaining an escalation path within the Customer's employees.

6.6 Training

- Customer is responsible for end-user training on application functionality.

For more information on Change Management, please refer to [Cisco Change Management Services](#) for Cisco Remote Management Service.

-END-