Cisco Remote Management Services (RMS): Common Service Description

This Service Description describes the Services to be provided by the following respective Cisco RMS group (see the specific Technology Addendums (described below) for additional details).

Technology Addendum(s)

- Cisco Unified Communications/Unified Contact Center Remote Management Services
- Cisco Foundation and Wireless Technologies Remote Management Services
- Cisco Data Center and Applications Networking Remote Management Services
- Cisco Remote Management Services for Security
- Cisco Business Video Remote Management Services

This Service Description must be accompanied by the appropriate Remote Management Services Technology Addendum. The Technology Addendum will describe exceptions, differences or details applicable to that business service not held within this Service Description. Information within each Technology Addendum will hold precedence over information within this Service Description.

This Service Description is designed to provide a baseline understanding of and set expectations about the Services. Please read this document carefully as it contains important information regarding the Services you have purchased from Cisco.

Direct Sale from Cisco

If you have purchased these Services directly from Cisco, this document is incorporated into your Master Services Agreement (MSA), Advanced Services Agreement (ASA), or equivalent services agreement executed between you and Cisco. In the event of a conflict between this Service Description and your MSA, ASA or equivalent services 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 informational purposes only; it is not a contract between you and Cisco. The contract, if any, governing the provision of this Service is the one between you and your Cisco Authorized Reseller. Your Cisco Authorized Reseller should provide the contract to you. You can obtain a copy of this and other Cisco service descriptions at www.Cisco.com/go/servicedescriptions/.

Cisco Remote Management Services only supplement a current support agreement for Cisco products, and only available where all Managed Components in a Customer's Network are supported through a minimum of core services such as Cisco SMARTnet and Cisco Software Application Services or Cisco's Unified Communications Essential Operate Service, as applicable. Cisco shall provide Cisco Remote Management Services 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 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. Cisco only provides support of Managed Components.

The following two RMS service levels are offered:

- Monitoring Service
- Managed Service

The table below indicates what is included within each of the two services levels and the optional Services available.

Monitoring, Managed and Optional Services Summary (Table 1)

Activities / Deliverables	Monitoring Service	Managed Service	Optional Services	Required Optional Service
Management Readiness Assessment	✓	✓		
Device Monitoring	✓	✓		
Incident Record	✓	✓		
Incident Notification	✓	✓		
Incident Management		✓		
Incident Priority and Classification		✓		
Incident Investigation and Diagnosis		✓		
Incident Resolution and Restoration		✓		
Incident Escalations		✓		
Incident Closure		✓		
Incident Resolution		✓		
Root Cause Analysis Reports			✓	Customer Engineer Level I
Ticket Trending and Analysis			✓	Customer Engineer Level II
Review / Assess Cisco Field Notices (PSIRT)			✓	Customer Engineer Level II
Backup Management	✓	✓		
Web Accessible Portal	✓	✓		
Standard Reports	✓	✓		
Advanced Reports		✓		
Custom Reporting			✓	Operations Manager Level II
Customer Engineer Level I and II			✓	
Operations Manager Level I and II			✓	
Defined Changes			✓	Elective Changes
Custom Scoped Elective Changes			✓	Elective Changes
Regulatory Compliance Management			✓	Compliance Management Package
Policy Management			✓	Compliance Management Package
Software Image Management (SWIM)			✓	Compliance Management Package

1. Common Service Elements

This section will describe activities provided within both the RMS Monitoring and the Managed Service levels.

1.1. Cisco Management Application Platform (MAP)

The Management Application Platform (MAP) provides monitoring for all Managed Components in your solution. The Service may require the installation of a Management Application Platform (MAP) on your Network in order to provide monitoring coverage.

Note: Depending on the specific devices supported and services requested, multiple MAP terminal devices may be required to deliver the Service.

The MAP is a suite of management applications that may be deployed in a redundant configuration and consists of management software and hardware required for service delivery. The MAP is deployed in a single configuration instance or multiple instance configurations depending on the number, type, and location of the Managed Components. The MAP, or portions thereof, may exist on the Customer premise and/or the Cisco premise. The MAP configuration is determined by Cisco during the Transition Management phase.

The MAP is configured with Customer-specific installation and monitoring data prior to being placed into service. Once installed, this MAP will be configured with the components under management as indicated via the Service Activation Kit and build the inventory report.

The implementation of the MAP may include some or all of the following activities which may be accomplished remotely:

- Installation of operating system and supporting applications on the MAP
- Remote installation and testing of the monitoring application
- Shipment of servers, appliances and/or devices to the designated Customer location
- Installation assistance to Customer for the servers, appliances and/or devices
- Establishment of connectivity between the Customer site and Cisco
- Establishment of remote monitoring and management of the Customer's Network devices and applications from Cisco

The MAP is an integral part of the Service and is installed for the duration of Services. During the Service term, the Customer is granted a nonexclusive and nontransferable license to use the hardware and the software resident on the MAP solely on the respective MAP device(s) supplied and in accordance with the licensing terms of the MSA, ASA or equivalent services agreement between Customer and Cisco. The Customer must return the MAP any and all associated MAP materials (devices and documentation) and connectivity devices to Cisco immediately upon expiration or termination of Services.

Note: A redundant MAP solution will require additional scoping and is not covered as part of the Service. Additional MAPs are billable as part of a Disaster Recovery solution.

1.1.1 Software Updates for the Management Application Platform

The Service includes routine software updates for the MAP. The Customer shall receive an e-mail notification from Cisco which identifies the modifications included in the next release. Cisco will schedule a maintenance window for updating the MAP. If there are any Customer-specific considerations stemming from the upgrade, they will be communicated by Cisco and addressed as part of the upgrade process. Any software updates are executed under the Standard Change guidelines (see Section 4.10.2 below).

1.1.2 Management Application Platform Configuration

During this configuration phase, Cisco assists in executing a discovery process for Managed Components per Purchase Order. The Project Coordinator will communicate any discrepancies between discovered devices and devices on the Purchase Order. Any Customer-requested additions beyond the Managed Components defined on the Purchase Order will be subject to incremental Service fees and additional Transition Management intervals.

Cisco inputs Managed Component information into the service MAP database and configures system consoles and dashboards (per Purchase Order). Managed Components are organized into defined device groupings. Where appropriate, service, support and escalation processes are configured in the service MAP. This completes the configuration of the MAP.

1.2 Management Portal

Customers receive end-user accounts to access the Portal. Instructions to access and navigate the Portal are provided in the remote or video on demand (VoD) training sessions as well as in the Portal User Guide. The Portal user guide is available on the Portal.

During the initial setup phase, Customers receive accounts for authorized employees to access the Portal.

Information available from the Management Portal may include:

- Ticket identification number
- Ticket opened date and time
- Ticket description
- Cause of Incident
- Ticket status/details
- Sites/device(s) affected

Further details regarding specific activities on the Portal, if applicable, are defined in the specific Technology Addendums.

Note: This information may be presented in multiple Portals if the customer has purchased RMS for multiple technologies.

1.3 Reports

The RMS Service provides three levels of reporting, Standard, Advanced, and Custom.

- Monitoring Service Level includes the Standard level of reports. These reports will be made available on the Portal.
- Managed Service Level includes the Advanced level of reports. This will include the Standard Level reports along with an expanded set of reports.
- Custom reporting is only available as part of the purchase of the Operations Manager Level 2 Services option. Each Custom report is scoped and mutually agreed upon by the Customer and Cisco.

Note: See the specific Technology Addendums for more detail concerning the reports available for each technology.

1.4 Management Connectivity

Management Connectivity establishes bi-directional communication between the Customer Premises and Cisco allowing Management Data to be securely and consistently transmitted between Managed Components and Cisco.

Management Connectivity requires access to specific ports and protocols; such requirements will be reviewed with Customer during the Transition Management process.

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

- A dedicated circuit between 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.
- A virtual connection via a virtual private network (VPN) between Cisco Point of Presence and Customer Network.

Each option may 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 Service and number of Managed Components.

Redundant and/or additional circuits are an available option. Fees for any additional and non US or Canadian circuits are to be paid by the Customer.

1.5 Termination Device

Cisco will ship a Termination Device for installation at the Customer site. The Termination Device terminates the Management Connection. The Termination Device is a Managed Component supplied by Cisco and resides at the Customer Premises. The Termination Device must have Network access to Managed Components.

Unless otherwise agreed upon, title to all Termination Device(s) shall remain with Cisco. Customer must return the Termination Device to Cisco immediately upon expiration or termination of the SOW or Services.

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 Termination Device(s). Failure to allow timely access may invalidate Cisco SLAs and SLOs, if any, and delay restoration and performance of Services.

1.6 Transition Management

Transition Management is a phased process approach in which Cisco works with the Customer to prepare the Customer infrastructure for Services. The Customer must place a Purchase Order with Cisco and attach Cisco Service Description to initiate the Transition Management process. The Transition Management process concludes at the earlier of the date of Customer Acceptance or the date monitoring Services begin.

1.6.1 Kickoff Meeting

Cisco will assign a Project Coordinator to act as a primary point of contact during the Transition Management phase. Within thirty (30) days from receipt of a valid Purchase Order, the Project Coordinator will contact the Customer to schedule the kickoff meeting. The kickoff meeting is typically accomplished via a conference call with the executed contract detail and may include a Cisco partner. The kickoff meeting will indicate the initiation of the

kickoff phase. The kickoff phase, as well as all remaining phases within Transition Management, is typically facilitated by the Project Coordinator in collaboration with Cisco Engineers assigned to the Customer account.

This Transition Management phase may include the following activities:

- Reviewing Services purchased, as indicated on the Purchase Order
- Reviewing roles and responsibilities of Cisco personnel, Customer contacts, and Partner contacts (if applicable)
- Coordinating, scheduling, and executing the kickoff meeting
- Establishing Connectivity
- Discovery of Managed Components into the Cisco infrastructure
- Provision of service manual

1.7 Service Activation Kit (SAK)

Reviewing the SAK components and key information is critical to success for Transition Management. It is the Customer's responsibility to fill out all relevant data fields in the SAK, which include all necessary Network and Managed Component details that are required for activating Services.

1.8 Customer Acceptance

Cisco will work with the Customer to validate that the Transition Management phase is complete.

Upon the date of Customer Acceptance, the Service transitions from Transition Management to the Service Delivery phase. All exceptions to the Service Delivery phase must be documented within the Transition Management material. Exceptions may include removing devices from SLO/SLA consideration due to inability to monitor or manage Managed Components not under full management.

1.9 Managed Components Covered Under the RMS Service

Full details and product lists for Managed Components can be found in the documents specific to each technology that are referenced in the appropriate Technology Addendum.

Please note that while Cisco RMS strives to deliver a management platform that enables uniform capabilities across the product lines, an individual system's reporting and alarming capabilities ultimately determine what support can be provided on a product by product basis. This can vary from system to system and is limited by internal architecture and instrumentation.

Cisco RMS intends to bring newly released devices under RMS management as soon as possible, however, some delays may occur due to device complexity or other factors outside of our control.

1.10 Management Readiness Assessment

Management Readiness Assessment is an assessment conducted by Cisco RMS Engineering analysts that determines whether the Managed Components are in good working order prior to completion of Transition Management. This requires that the Managed Components be fully configured, deployed and functioning properly prior to the commencement of Incident and Problem Management Services.

1.11 Backup Management

Backup Management means the process and actions needed to backup and restore Cisco IOS/CatOS router and switches. Implementation may include backup policies outlining retention policies, ad-hoc configuration backups and restores as well as standard backup reports.

2.0 Monitoring Service Level

All activities and deliverables mentioned in Sections 3.0 through 3.4 are included within the Monitoring Service level. Under the Monitoring Service level within Cisco RMS, Cisco will provide the following support:

2.1 Device Monitoring

Device Monitoring allows the Cisco RMS monitoring system to indicate a fault condition, that a performance threshold was exceeded, or that an event has triggered an Incident.

Activities may include:

- Monitor (24x7x365) Managed Components of the Customer's Network
- Perform fault and performance device monitoring on the entitled Managed Components of the Customer's Network
- Detect Incidents
- Correlate Incidents where applicable

Deliverable(s):

- Confirmed Incidents logged in the Cisco RMS Configuration Management Database (CMDB)
- Provide access via the web Portal to ticketing and reporting details

2.2 Incident Record

An Incident Record is where the Cisco ticketing system captures alarm/event/correlation data and enrichment with relevant configuration Items information which results in the creation of an incident ticket.

Activities may include:

- Enrich alarm information with relevant configuration item information from the Cisco RMS CMDB
- Enrich alarm information with relevant information from Cisco, where applicable
- Incident tickets will be auto-closed based upon a configurable timer

Deliverable(s):

- Create Incident Ticket
- Post Incident Ticket online via the Portal for the Customer to view all Ticket handling activities and milestones

2.3 Incident Notification

Incident Notification is where Cisco will electronically notify (E-notify) designated Customer contacts for new Incidents or milestones achieved. E-notify are sent to any email address or email-capable mobile device and will include the Incident Ticket number. The Customer (or its preferred vendor) can always view Incident status and detailed information via the Cisco RMS Web Portal.

Activities may include:

- Automated E-notify to specific Customer contact(s) based on Customer's notification requirements as agreed on during the Transition Management process

Deliverable(s):

- Perform E-notify of Incident Tickets per Customer's notification profile (Default)
- Log E-notify records in the Incident Ticket
- Update Web Portal with Incident Information

Note: Cisco's primary means for incident notification is electronic mail

2.4 Service Support

Customer will be provided with a contact number to gain access to support for:

- General MAP Assistance
- Web Portal – Usage and Access Assistance
- Service Activities Assistance

Note: This Service is staffed to only answer questions about the use of the Service and is not a technical support service desk

3.0 Managed Service Level

Under the Managed Service level offered within Cisco RMS, Cisco will support all the capabilities provided by the common service elements of the Monitoring Service level plus the following:

3.1 Services Manual

The Project Coordinator will provide the Customer with a Services Manual which describes the operational support provided and provides the Customer with a detailed job aide to be used as a guide once the transition phase ends and Cisco begins the Service Delivery phase as of the Cisco specified date.

This Services Manual will include:

- Roles and Responsibilities of Cisco and Customer
- How to contact Cisco for assistance
- Service escalation guidelines
- Change and release management policies
- Standard notification procedures
- General support guidelines

3.2 Incident Management

Incident Management is an ITIL process used by Cisco RMS to identify Incidents, restore service and remediate declared Incidents as quickly as possible and may involve implementing temporary work-arounds. RMS will proactively monitor for key events and thresholds on Managed Components in the Customer Network. In the case of undetected events, Customers may declare an Incident by contacting the Cisco RMS Service Desk. For any high priority Incidents (system down, degraded performance, etc.), Customer should contact the Cisco RMS Service Desk via telephone. Low priority Incidents should be reported by Customer to the Cisco RMS Service Desk via the Cisco RMS Web Portal.

Upon automatic detection or manual submission of an Incident to the Cisco RMS Service Desk, an Incident Ticket is created. The Cisco RMS Service Desk is responsible for coordinating the management of the Incident, which includes communicating with the Customer throughout the Incident management process. This communication also includes notification to the Customer that the Incident has been resolved or remediated.

3.3 Incident Priority and Classification

Incident Priority and Classification is considered to be a subset of Incident Management whereby Cisco Incidents will be managed according to the Priority level as defined in the **Service Level Objectives for Cisco Remote Management Services document**. (http://www.cisco.com/web/about/doing_business/legal/service_descriptions/docs/Service_Level_Objectives_Remote_Management_Services.pdf). An Incident Priority level (as shown below) depends on a variety of factors including pre-defined Incident Ticket attributes such as business impact, and urgency.

Activities:

- Evaluate Incident severity and prioritize all Incidents into Priority 1 (P1), Priority 2 (P2), Priority 3 (P3) and Priority 4 (P4) Incident categories

Deliverable(s):

- Properly prioritized Incidents based on Incident Ticket attributes
- Report status prioritized Incident against its associated Service Level as defined in Section 4.9, Service Level Objectives section herein

3.4 Incident Investigation and Diagnosis

Incident Investigation and Diagnosis is considered to be a subset of Incident Management whereby Cisco engineers utilize Incident remediation procedures to collect any additional data required to diagnose and match the Incident to a known error in the Cisco RMS knowledge base. Cisco support engineers will work to isolate the root cause of the Incident. Cisco support engineers will update the Incident Ticket with information related to root cause isolation if any is performed and then proceed to the Incident Resolution and Restoration phase.

Activities:

- Collect additional data to properly diagnose root cause of the Incident
- Attempt to match Incident to a known error in the Cisco RMS knowledge base

Deliverable(s):

- Update Incident Ticket with root cause event information for Incidents
- Perform E-notify for this Incident Ticket event milestone (if requested by the Customer)

3.5 Incident Resolution and Restoration

Incident Resolution and Restoration is considered to be a subset of Incident Management whereby Cisco Customer engineers utilize Incident remediation procedures and work to restore Services within agreed service objectives, initiating any request for change (RFCs) as needed for restoration.

If an Incident has been isolated down to its root cause, Cisco RMS engineers will work to resolve the Incident. Resolution is complete when functionality is materially restored to the affected Managed Component(s) or a recommendation is made to the Customer to remediate the Incident. The resolution process includes any action the Cisco RMS engineer requires to restore functionality to a Managed Component or remediate an Incident on the Customer's Network.

Cisco RMS will utilize work-around solutions to restore all or partial functionality when full functionality cannot be restored within expected timeframes as defined in the Service Level Objectives section. When a work-around is utilized, the Incident will continue to remain open and will be worked by Cisco RMS engineers until resolved, in accordance with the priority level of the Incident.

Incident Resolution and Restoration may include Cisco RMS engineers working directly with the Customer's network IT team to resolve fault and performance Incidents on the entitled Managed Components or to assist with the remediation of incidents detected on the Customer's Network. Cisco RMS engineers may provide recommendations for remediation of an affected Managed Component.

Should Cisco RMS require a configuration change in a Managed Component to resolve an issue or implement a work-around, the Cisco RMS engineer will follow the Change Management Process established with the Customer.

Activities:

- Resolve fault and performance Incidents on Managed Components
- Remediate Incidents on the Customer's Network
- Submit, when needed, a Cisco-recommended RFC in accordance with the Change Management Process established with the Customer to implement a temporary work-around
- Dispatch third party vendors, as needed and appropriate, within the resolution steps prescribed by Cisco RMS and in accordance with the Cisco SMARTnet or other Cisco service terms on the affected Managed Components. As vendors are dispatched, the Incident Ticket will be updated with information related to the dispatch.
- Update Incident Ticket to include notes regarding fault and performance Incident resolution or recommendations for remediating Incidents.
- Perform E-notify for the respective Incident Ticket milestone, if requested by the Customer.

Deliverable(s):

- Updated Incident Ticket with resolution notes on faults and performance related Incidents

- Cisco-recommended RFC for Incident resolution or temporary work-around as determined by Cisco support engineers

3.6 Incident Escalations

Incident Escalations is considered to be a subset of Incident Management whereby Cisco escalation is driven by elapsed time against service level objectives for routing of Incidents to appropriate technical resources as required. A Customer may request escalation of an Incident Ticket at any time via the Portal or telephone call to the Cisco RMS Service Desk. Cisco RMS will refer Incidents to the Customer as needed and escalate the Incident with the Customer within the Customer's escalation guidelines until the Incident is resolved or remediated.

Activities:

- Ensure Incident is being handled by appropriate Cisco RMS engineer resources to meet service level objectives
- Escalate Incident as appropriate in the Cisco RMS engineer or with the Customer per the established escalation procedures

Deliverables:

- Updated Incident Ticket to include escalation notes
- Incidents resolved or remediated in accordance with Service Level targets
- Perform E-notify for this Incident Ticket event milestone, if requested by the Customer

3.7 Incident Closure

Incident Closure is considered to be a subset of Incident Management whereby once Cisco RMS declares an Incident resolved and verified, the Incident will be closed. In the event that the Incident re-occurs, a new Incident Ticket will be created to reflect the recurring nature of the Incident and aid in the identification of Problems. Depending on frequency, recurring Incidents may trigger the problem management process, which may include a Cisco- recommended request for change (RFC) to resolve the recurring Incident.

Any authorized Customer agent may also proactively request Incident Ticket closure via the Portal or telephone. Cisco RMS will review the request and work in conjunction with the Cisco RMS Service Desk to close the Incident Ticket or follow up with the Customer for more information as needed.

Activities:

- Confirm Incident is resolved
- If Incident re-occurs, depending on frequency and attributes of the Incident, open a Cisco-recommended RFC to resolve recurring Incident

Deliverable(s):

- Update Incident Ticket to include closing notes
- Close the Incident Ticket
- Perform E-notify for this Incident Ticket event milestone, if requested by the Customer.

3.8 Translation Support *(contact by phone only)*

Translation Support is delivered in the English language. For Customers who require telephone support in a language other than English, Cisco may provide telephone Translation Support. When a Customer calls Cisco, the Cisco Engineer will attempt to determine the language spoken and conference the appropriate translator into the call, when available.

3.9 Service Level Objectives (SLO)

Mean Time to Restore (MTTR), the time it takes to restore service after an incident, varies by Priority. Please refer to the **Service Level Objectives for Cisco Remote Management Services document** (http://www.cisco.com/web/about/doing_business/legal/service_descriptions/docs/Service_Level_Objectives_Remote_Management_Services.pdf) for a detailed description of the Priority levels and SLOs.

3.10 Change, Release and Configuration Management

Change, Release, and Configuration Management are a tightly integrated set of processes due to the interdependence of their process activities. The evaluation of a proposed change is strongly dependent on accurate configuration data. Approved changes are executed via the Release Management process, which is also strongly dependent on accurate configuration data for design and testing activities. Configuration Management activities must be invoked whenever changes are released to keep configuration data accurate.

3.10.1 Change Management

The objective of Change Management is to make necessary changes in an efficient and accountable manner. The purpose of Change Management is to make sure that changes to Managed Components are evaluated, coordinated, and communicated to impacted parties in an effort to minimize negative impacts of the change to Management Services. Change Management is the use of standard methods and procedures for authorizing, documenting, and performing all service-impacting changes to the environment or Managed Component.

Changes are divided into two categories: **Standard** and **Elective Changes.** Standard Changes are described below. Elective Changes are divided into two sub-categories, Defined Changes and Custom Scoped Changes. For more information about Elective Changes, please see the optional service elements at the end of this document and the Technology Addendums for the pertinent architecture.

Common activities relevant for both Standard and Elective Changes such as Coordination & Planning, Configuration Management and Release Management are described in this section.

Note: Only Standard Changes are included as part of the Managed Service level.

3.10.2 Standard Changes

A Standard Change is a Cisco recommended change that is often a result of Incident Management and Problem Management processes or a Cisco field notice or Cisco PSIRT. A Cisco Engineer will submit a Standard Change Request to start the Change Management process. Standard Changes are included in the Managed Service level.

Incidents/Problems will result in the creation of a Ticket which will initiate Change Management when Cisco deems it is required to resolve the Incident.

A Ticket will be created to track the resolution of a Problem. However, Cisco changes initiated as a result of a Problem may also be documented and added to Cisco's knowledge base for future use.

The following table delineates a Cisco recommended change (i.e., Standard Change) versus one that is considered an Elective Change:

Cisco Recommended Changes	
Changes Required To:	**Resulting in:**
Resolve an Incident	Logical or physical change
Respond to a critical vulnerability (Cisco recommended)	Logical change
Apply a signature update to a security Managed Component	Logical change

3.10.3 Coordination, Planning, and Closure

Approved changes will be coordinated, planned, and monitored in cooperation with the Customer. Once a Standard or Elective Change has been released and the configuration data has been updated, the change will be evaluated to determine the level of success in meeting the agreed to goals. This evaluation is used in an effort to improve Change Management. The Cisco engineer will confirm that all relevant stakeholders, including the Customer, have been notified that the change is complete. Once evaluation and notification have been completed, the change is closed.

- Rollout planning activities include defining the details involved in executing the change into the production environment. This includes setting the detailed timetable, securing a Customer change window if necessary, identifying and communicating to all stakeholders that need to be notified, and coordinating with Customer change procedures.
- Execution is the act of introducing the change into the production environment. Once the change has been executed, Configuration Management is initiated to record the changes to all impacted Managed Components.

3.10.4 Configuration Management

Cisco shall maintain an inventory of the Managed Components. This inventory detail includes certain configuration data and the levels of Service applied to each Managed Component. Refer to the respective Technology Addendums for other device backup strategies.

3.10.5 Release Management

Release Management is focused on the execution of approved changes.

Rollout planning activities include planning the details involved in executing the change into the production environment. This includes setting the detailed timetable, securing a Customer change window if necessary, identifying and communicating to all stakeholders that need to be notified, and coordinating with Customer change procedures. Once the approved change had been executed, testing of the environment and (if required) implementation of a back-out plan.

Execution is the act of introducing the Change into the production environment. Once the change has been executed, Configuration Management is initiated to record the changes to all impacted configuration items.

3.10.6 Applying Software Updates

Application of a software update on Managed Components is at the discretion of Cisco and related to the individual technologies. Software updates will be evaluated in an effort to minimize disruption to the stability of the current environment.

Software updates to remediate an Incident or Problem are handled as a Standard change. Software updates that are Customer-requested for the purpose of obtaining additional features or functions are considered discretionary and are handled as a Elective Change.

As part of the Software update process, Cisco will:

- Review Cisco Field Notices to determine impact and urgency to the Customer system and existing software levels.
- Remotely apply service pack updates to the Managed Components' operating system, system software, and applications (Cisco software only).
- Remotely apply software update to the Managed Components' operating system, system software, and applications (Cisco software only).
- Provide a Change Management Report that identifies work Ticket and number of hours spent on Ticket.

3.10.6.1 RMS Service Updates

RMS Service Updates are focused on the implementation of endpoint and infrastructure software upgrades to the Customer's technology environment if deemed necessary by Cisco to maintain a stable managed environment. In addition, Cisco may implement enhanced functionality within the RMS Management Application Platform releases. Cisco will use reasonable efforts to provide 1 Week notice prior to the implementation of an RMS Update.

Customers must hold proper licenses entitling them to any software upgrades suggested by Cisco.

RMS Service Updates are developed by and made solely from Cisco and may include new features or functions specifically for managed components in the covered environment. These updates may provide additional monitoring, management or other capabilities, (e.g., enabling additional monitoring for a new fault type).

Note: If required, Cisco may issue an emergency maintenance notification where the notification window could be shorter than normal.

4.0 Optional Services – Common to all Services

The table below illustrates the common optional Services available for purchase ala carte with the purchase of the appropriate RMS Service. Optional services common to all technologies are described below. Services that are technology specific are described in the corresponding Technology Addendum.

Service Activity	Pre-requisite
Operations Manager Level 1 & 2	Managed Service level
Customer Engineer Level 1 & 2	Managed Service level
Elective Changes	Managed Service level
Compliance Management	Managed Service level
E-Bonding	Managed Service level

4.1 Elective Changes

Elective Changes are changes that are ***not*** the result of Cisco Incident Management and Problem Management processes. There are two types of Elective Changes available:

- **Defined Changes**
- **Custom Scoped Elective Changes**

Defined Changes have a pre-determined "level of effort" and are described within the individual Technology Addendums. Custom Scoped Elective Changes are service requests that are outside the Defined Change list and will not have the "level of effort" estimate without a detailed review of the request and custom scoping of the effort required.

Customers purchase a number of support hours in blocks that can be used for Defined and Custom Scoped Elective Changes. The quantity of support hours to be purchased is determined by the Customer. The Customer must have a sufficient balance of support hours on account to cover their requested change. Additional support hours can be purchased in blocks, if required.

4.1.1 Defined Changes

Defined Changes are grouped into types based upon the level of effort required to complete the requested work. Additional details are available in the individual Technology Addendums and outline the specific changes. The chart below provides a break-down of the available categories and durations for Small, Medium, and Large changes.

Category	Duration	Size
Type 1	*30 Min*	*Small*
Type 2	*1 Hour*	*Small*
Type 3	*1.5 Hours*	*Med*
Type 4	*2 Hours*	*Med*
Type 5	*2.5 Hours*	*Med*
Type 6	*3 Hours*	*Large*
Type7	*3.5 Hours*	*Large*
Type 8	*4 Hours*	*Large*

A Defined Change is requested by the Customer and is often the result of needed changes in the Customer Network, Cisco business application, or the Customer business. Defined Changes are not the result of Cisco Incident Management and Problem Management processes. The Customer identifies the needed type of change and submits a change requests on the Portal.

Defined Changes are scheduled services that the Customer must request in advance of service delivery.

Available Cisco Defined Change Services and the level of effort for each type of change are itemized in the specific service Technology Addendum. Cisco may elect to offer additional Services within its areas of competency in response to a Customer's request for Service.

Defined Changes are debited from the Customer's balance of support hours, per the following:

- As Defined Changes are executed, they will be deducted from the support hours' balance available to the Customer.
- All purchased support hours must be used within the duration of the contract period. If a multiple year contract is purchased, then the support hours purchased must be used completely by the end of the contract. In the event that the Customer has support hours left over at the end of the contract and the Customer is purchasing additional year(s) of service, then, and only then, may the previous support hours be carried over for up to a period of six (6) months from the end of the respective term in which such unused support hours were purchased, after which such support hours will be forfeited and have no residual cash value.
- If the Customer has the need to purchase additional support hours then the unused support hours are added to the support hours in the new contract to form the new quantity of available support hours. The end date for the use of the support hours will be the date that is furthest in the future. For example, if the existing contract ends 1/31/2012 and the new contract ends 3/31/2013, then the newly acquired support hours expire on 3/31/2013.
- Defined Change categories and definitions are described in the appropriate Technology Addendums.

Cisco has categorized Defined Changes into types based on level of complexity and the amount of time required to complete the change. All change requests are scheduled events and are dependent on coordination with the Customer. Cisco Service Level Objectives (SLO) for executing approved changes are detailed in the **Service Level Objectives for Cisco Remote Management Services document** (http://www.cisco.com/web/about/doing_business/legal/service_descriptions/docs/Service_Level_Objectives_Remote_Management_Services.pdf)

Cisco's priority handling of urgent Defined Change requests is on an as-available basis. Cisco will use commercially reasonable efforts to respond to such requests. However, a priority handling request if accepted will be charged at a minimum of 1.5 times the standard rate.

Defined Change requests where requested time of service delivery is outside of Standard Business Hours will be billed at a rate of 1.5 times the standard rate if the time is accepted by Cisco. Defined Change requests to be delivered on Cisco-observed holidays will be billed at 2 times the rate if the change time is accepted by Cisco.

During the change process, the Customer is required to have authorized representative available Cisco may require that a Customer change representative be available during the change planning process, and an onsite technician who has access to the equipment room to be available during the execution phase.

4.1.2 Custom Scoped Elective Change Services

A Custom Scoped Elective Change is requested by the Customer and is often the result of changes in the Customer Network, business processes, or the Customer's business. Custom Scoped Elective Changes are not the result of Cisco Incident Management and Problem Management processes. The Customer identifies the requirement and submits a Change Request for the Custom Scope Elective Change on the Portal.

A Custom Scoped Elective Change request varies based upon the nature of the request made by the Customer. Each such Change Request will be scope based and the level of effort will be assigned in the subsequent statement of work (SOW) that is created to track and document the Change Request. Hours will be decremented from the block of support hours purchased by the Customer.

Custom Scoped Elective Changes are scheduled services that the Customer must request in advance of service delivery. Custom Scoped Elective Change service delivery response time will be defined in the subsequent SOW that is created.

Custom Scoped Elective Change Services may include:

- **Software Upgrades** are Customer requested services for the purpose of upgrading a Managed Component for purposes not related to Incident or Problem management or part of a Cisco RMS Release. Reasons for software upgrades may include the need to leverage a new feature or function available in a later release or the need to normalize versions within an environment. Customers must hold proper licenses entitling them to any software upgrades installed.
- All changes not categorized as an RMS Release.

Examples of Cisco Custom Scoped Elective Change services are itemized in the specific Technology Addendum. Cisco may elect to offer additional services within its areas of competency in response to a Customer's request for service.

Rollout & Execution of Custom Scoped Elective Changes:

- Rollout planning includes defining the details involved in executing the change into the production environment. This includes setting the detailed timetable including securing a Customer change window if necessary, identifying and communicating to all stakeholders that need to be notified, and coordinating with Customer change procedures.
- Execution is the actual act of introducing the change into the production environment. Once the change has been executed, Configuration Management is initiated to record the changes to all impacted configuration items.

4.2 Customer Relationship/Operations Manager – Levels 1 & 2

The role of the Customer Relationship/Operations Manager is to ensure that Cisco RMS Customers have a single point of contact for RMS related service needs. This role can be added onto your contract in one of two levels outlined below. Listed out are the deliverables for the two levels. The Level 2 CRM/Operations Manager will deliver upon all the Level 1 activities in addition to the items listed under "Level 2".

Level 1 deliverables

- **Located remotely** – not on Customer site
- **Designated** resource – has a good understanding of the Customer's infrastructure
- **8 x 5 in Customer HQ** time zone (US & Canada)
- **Prioritization and support** for business escalations
- **Monitoring of return** materials authorizations (RMAs)
- **Coordination of Cisco** support organizations, escalation process, and customer resources for service requests
- **Primary point of contact** for operations and process issues
- **Baseline documentation** of customer's operational processes and procedures

- **Weekly, monthly and quarterly operations reports** in standardized format; covers status, tracks progress of open service requests, and other outstanding operational issues with the customer
- **Quarterly Business Reviews** (QBRs) in standardized format based on customer needs to address outstanding operational issues and report status and progress delivered over WebEx. May be delivered at Customer location if agreed to in advance.
- **Instructional sessions** on service operations and/or service consumption readiness. Leverage existing pre-recorded videos and documentation as available

Level 2 deliverables (includes Level 1 deliverables)

- **Oversight of high severity** incidents and high visibility escalations, providing feedback and input as required to expedite the incident.
- **Custom reports** based on individual Customer needs and delivered to Customer on an agreed-upon frequency (weekly/monthly/quarterly). Custom reports based on agreed upon definition.
- **Service Level monitoring & reporting** including Return Material Authorization (RMA) delivery performance reports delivered to Customer on an agreed-upon frequency. Follow-up within Cisco and with the Customer on identified gaps to help ensure improved performance.
- **Customized training** to meet individual Customer needs. Identify and agree to Customer needs and create custom training sessions to meet those needs. Deliver training remotely.
- **Program manage change management** initiatives undertaken by the customer and/or recommended by Cisco support teams

4.3 Cisco RMS Customer Engineer – Levels 1 & 2

The role of the Cisco RMS Customer Engineer Levels 1 & 2 is designed to ensure that Cisco RMS Customers have a designated engineering contact for technical support. This individual has a technical understanding of the Customer's specific environment. It is a requirement of the Cisco RMS Customer Engineer role that the Customer Relationship/Operations Manager option be purchased. This option can be purchased in one of two levels outlined below. Listed out are the deliverables for the two levels. The Level 2 Cisco RMS Customer Engineer will deliver upon all the Level 1 activities in addition to the items listed under "Level 2".

Level 1 Deliverables

- **Located remotely** – not on Customer site
- **Designated** resource – has a good technical understanding of the Customer's Network.
- **8 x 5 in Customer HQ** time zone (US & Canada)
- **Advanced Engineering support** for trouble shooting issues related to the RMS Services.
- **Deliver Root Cause Analysis Reports -** 8 reports per year.
- **Participate in Monthly/Quarterly** operational reviews facilitated by Operations Manager, provide engineering insight for dialog with customer
- **Collaborate** with Cisco Operations Manager on training sessions

Level 2 deliverables (includes Level 1 deliverables)

- **Proactive Network Health Analysis** checks based upon an analysis of the following relevant to the Customer's infrastructure:

  - PSIRT's
  - Field notifications
  - Configuration analysis
  - Incident trend analysis
  - Tuning of capacity/performance (targeted at infrastructure device level environmentals)
- **Knowledge transfer sessions** on Customer installed base technology and operational best practices as identified by Cisco based on Cisco and industry standards
- Attend and/or review Customer's Change Advisory Board (CAB) meetings, activities, planning and scheduled projects
- **Provide advisory support** for change management

4.4 Compliance Management Package

The Compliance Management Package will include the capabilities described below.

Currently, the capabilities described in this section are only supported for a limited set of products. For a detailed list of supported products, please refer to:
http://www.cisco.com/en/US/products/ps6192/serv_datasheets_list.html

The Compliance Management package includes Software Image Management, Policy Management and Regulatory Compliance Management. An Operations Manager and Customer Engineer are both prerequisites for the Compliance Management Package.

4.4.1 Software Image Management (SWIM) is the identification and reporting of network device images currently running on the Network, automated network image upgrades and unauthorized image notifications. The following deliverables are associated with Software Image Management.

1. Upgrade analysis, image memory requirements identification and required device hardware and software resources verification
2. Addition and deletion of images in the software inventory repository
3. Schedule automated image upgrades and installation success verification
4. Network image installation and out-of-sync reports

4.4.2 Policy Management is the process of auditing, reporting, monitoring and applying configuration policies to Networks and device groups. These policies may include Customer defined policies, industry guidelines or Cisco best practices as described below.

Customer defined: Security controls that consist of internal policies, standards, directives and regulations

Industry Guidelines: National Institute of Standards and Technology (NIST)

Cisco Best Practices: Cisco SAFE, Cisco PSIRT

The following deliverables are associated with Policy Management:

- Audit and inventory of current applied Network or device based policies
- Enforcement and management of Customer-defined, best practice, or industry policies
- Scheduled network and device policy provisioning, changes, updates and reporting
- Periodic reporting of applied policies and current violations
- Monitoring and alert notification of policy violations and non-compliant devices

4.4.3 Regulatory Compliance Management is the process of auditing, reporting, monitoring and ensuring that Networks and Managed Components are in compliance with industry defined regulatory compliance mandates. A list of the currently supported regulatory compliance mandates can be found at http://www.cisco.com/en/US/products/ps6192/serv_datasheets_list.html. This package will provide support for up to two standards. The following deliverables are associated with Regulatory Compliance Management:

- Audit and inventory of current regulatory compliance mandate violations
- Periodic reporting of current network compliancy status and violations
- Monitoring and alert notification of device and network regulatory compliance violations
- Scheduled regulatory compliance policy provisioning, changes, updates and reporting Regulatory compliance mandate violation mappings to the defined regulatory citation

4.5 Customer Ebonding

Cisco RMS offers the capability of electronically bonding the Customer's ticketing system with Cisco's ticketing system. This optional service covers setup, activation and ongoing support. This will enable the Customer to integrate their existing ticketing system with the system used by Cisco RMS. This will allow for bidirectional ticket exchange, allowing the Customer to create and view tickets from either system.

All data is secured and encrypted according to industry best practices. Some configuration and testing must be completed by the Customer. There is a standard package of bonding fields and features as detailed in the customer ebonding detailed specification located here:
http://www.cisco.com/en/US/products/ps6192/serv_datasheets_list.html.

Support is provided directly through Cisco. Customers experiencing problems with the Service are instructed to open a Service request via the Portal or Service Desk phone number.

5.0 Customer Responsibilities

5.1 Management Connectivity

5.1.1 Termination Device

The Customer will maintain the Termination Device in good working order. The Customer shall not, nor permit others to, rearrange, disconnect, remove, attempt to repair, or otherwise tamper with the Termination Device.

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. Under no circumstances, will Cisco be held liable to the Customer or any other parties for the interruption of service, missed SLOs, or for any other loss, cost, or damage that is a result from the improper use or maintenance of the Termination Device.

Unless otherwise agreed upon, title to all Termination Devices shall remain with Cisco. Cisco expects that, at the time of removal, the Termination Device shall be in the same condition as when installed, with the expectation of normal wear and tear. Customer shall reimburse Cisco for the costs of any Termination Device that is deemed beyond normal wear and tear. 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, among other reasons, the inspection or emergency maintenance of Cisco-supplied Termination Device.

5.1.2 Install Termination Device

The Customer shall provide or perform the following with respect to the installation of the Termination Device:

An appropriate and secure rack-mount location for the Termination Device with suitable environmental conditions for computer operation.

- Install the Termination Device and Network connectivity per Cisco-supplied guidelines.
- Provide communications facilities and services, including internet and Network configuration. Communication facilities and services must be maintained for the duration of the Service term.
- Provide a resource to support the installation of the Termination Device. These activities include:
    - Racking the device
    - Connection to Network
    - Power connection to uninterruptible power system (UPS) or other facility with continuous uninterrupted power
    - Power-up

Provide suitable commercial power, and an UPS or other acceptable power back-up facilities providing a minimum of 1kVA dedicated for the Termination Device.

Provide mutual agreement of date concerning completion of Transition Management activities.

5.2 Training

The Customer shall provide training coordination support including identifying trainees and trainee contact information.

5.3 Transition Management

To enable Cisco to provide Services for Managed Components, Cisco requires the Customer to:

- Assign a project manager to represent the Customer during the Transition Management phase.
- Assign a technical lead to assist Cisco with establishing the Network access required for remote management.
- Project manager and technical lead attend Customer project kickoff meeting and training sessions.

5.4 Service Activation Kit

Complete the SAK, which provides the key information critical to success for Transition Management and includes by way of example and not limitation:

- Customer representative contact name
- Location of the site(s) to be managed
- Location of management applications
- Network connectivity detail for the MAP
- Device location and naming scheme
- Management IP addresses and system detail, SNMP community strings
- Telnet and password access
- Management system user names and contact detail
- Definition of Customer-specific support policies including:
  - Points of contact and profile data
  - Case category access
  - Notification policy
  - Escalation policy
  - Dispatch policy
- Managed Component support contract information (e.g., Cisco SMARTnet, etc.)

Complete tasks defined in the SAK to enable management access to managed systems which may include setting up SNMP, traps, system logs, etc.

Provide as-built documentation including detailed design, Network implementation plan(s), site survey(s), and bill of materials. Data and documentation will be obtained from Cisco Partner as necessary to facilitate Transition Management.

5.5 Install Management Application Platform

For those cases where the Cisco MAP or components of the Cisco MAP reside on the Customer Premises then the Customer must provide an appropriate secure rack-mount location for the Cisco MAP (or components) and termination devices with suitable environmental conditions for computer operation.

The Customer is also expected to provide the following:

- Installation of the MAP and Network connectivity per Cisco-supplied guidelines.
- Provide communications facilities and services including internet and Network configuration. Communication facilities and services must be maintained for the duration of the Service term.
- Provide a resource to support the installation of the MAP. These activities include:
  - Racking
  - Connection to Network
  - Power connection to UPS or other facility with continuous uninterrupted power
  - Power-up
- Provide suitable commercial power, and an uninterruptible power system (UPS) or other acceptable power back-up facilities providing a minimum of 1kVA dedicated for the MAP and termination device.
- Provide mutual agreement of date concerning completion of Transition Management activities.
- Provide training coordination support including identifying trainees and trainee contact information.

5.6 Service Connectivity and Network Access

Cisco RMS Services are delivered using a collection of protocols and ports. The Customer must allow the collection of data for Managed Components.

Customer must provide Read and Write management access to Managed Components as defined by SAK. Customer must provide Read management access for components that are monitored only. Customer must that access is implemented in a timely manner in accordance with the SAK. This includes SNMP, syslog, and other defined protocols as necessary to support Services.

In support of connectivity to the Cisco point of presence, Customer will be required to provide, in certain deployments, a mail relay server for communication back to Cisco.

5.7 Incident Resolution

The Customer must provide support contracts, Letters of Agency, and all other end Customer documentation and authorization required to facilitate Incident resolution.

Customer is required to maintain hardware maintenance and/or software maintenance as may be applicable on all Managed Components identified in Purchase Order for the duration of the contract.

As part of the Monitor Level of Service, the Customer is responsible for all Incident and Problem Management activities except for those activities specifically designated as provided by Cisco as indicated in the Monitor Section.

5.8 Managed Components

The Customer will:

Ensure that all Managed Components are in good working order prior to completion of Transition Management. This means that Managed Components are fully configured, deployed, and functioning properly prior to the commencement of Cisco remote management and/or monitoring services. Good working order status will be verified by Cisco during the management readiness assessment process and using availability and performance reports during Transition Management. Required remediation steps will be provided to Customer by Cisco. Customer is responsible for all activities required to bring Managed Components up to good working order, including but not limited to system administration, configuration changes, scripting, and MACDs (moves, adds, changes, and deletes). Necessary services may be acquired from Cisco as Elective Change Services.

- Approve all Standard and Elective Change requests prior to Cisco taking change action
- Provide physical security of the Managed Components.
- Contact Cisco to report Incidents via telephone or other means (such as Portal) in accordance with policies established
- Allow Cisco to retain and publish aggregate statistics and metrics for non-identifiable trending analysis.
- Sufficient back-up for all applications and operating systems. The Customer is responsible for ensuring the backups run successfully.
- Perform back-up on devices not running Cisco Catalyst OS or Cisco IOS. The Customer is responsible for ensuring the backups run successfully.

5.9 Non-Managed Components

The Customer is responsible for monitoring and managing the Non-Managed Components and applications.

5.10 Communication and Change Management

Cisco has a co-management approach to Management Services, allowing the Customer and other Customer-approved vendors to retain full Read and Write access to their Managed Components. 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 process. This process is reviewed and agreed upon by both parties prior to completion of the Transition Management phase.

The Customer will:

- Provide Cisco with changed data with respect to the Customer and Managed Components, as needed, via the Portal.
- Provide timely delivery of information required for configuration of Managed Components notification procedures.
- Submit maintenance window and other scheduled maintenance activity via the Portal, by telephone or email. Cisco requires a minimum of 72 hours advanced notification. Cisco will suppress Incident tickets during the scheduled maintenance period.
- Maintain sole responsibility for informing Cisco of Customer employee status changes to help ensure that Cisco maintains current Customer contact list.
- Provide and maintain a list of Customer employees authorized to request changes.
- Provide and maintain an escalation path within the Customer's employee base.
- Provide Cisco product training for end-users.

6.0 Services Not Covered

This Service Description should be read in conjunction with the **List of Services Not Covered** document posted at http://www.Cisco.com/go/servicedescriptions/, under the Technical Services section, which is hereby incorporated into, and made part of, this Service Description by this reference.

APPENDIX A: Glossary of Terms

Glossary of Terms should be read in conjunction with this Service Description. Capitalized terms not otherwise defined above have the meanings assigned to them in the Glossary of Terms.

Analog Telephony Devices refers to devices such as fax machines, modems, and analog phones connected to FXS or gateway ports and that require call processing by a managed Cisco Unified Communications Manager.

Technology Addendums refer to specific technology service descriptions that outline the unique Cisco RMS Service options available for individual product families (e.g., TelePresence).

Advanced Event Correlation (device-level, component-level, time-based) means the act of combining disparate data sources to obtain root cause.

Backup Management means the process and actions needed to backup and restore Cisco IOS router and switches. This may include backup policies outlining retention policies, ad-hoc configuration backups and restores as well as standard backup reports.

Carrier means a provider of data transport services.

Change Management means the process used by the Cisco to receive, authorize, execute, and communicate changes to Managed Components.

Cisco Field Notice means an electronic notification about product related issues.

Cisco Remote Operations Services (ROS) means the Cisco Services team that delivers Cisco Remote Management Services.

Configuration Management means the process to create and maintain an inventory of the Managed Components.

Customer means the entity purchasing Services for its own internal use either directly or through an Authorized Channel.

Customer Acceptance means a mutual agreement with Cisco to acknowledge completion of the Transition Management phase.

Customer Notification means a communication to inform the Customer that an Incident has been recorded.

Customer Premises means the physical Customer location where the Managed Components reside.

MAP Disaster Recovery means the deployment of necessary MAP elements to sustain a complete failure of the primary MAP instance. Implementation may constitute deploying a geographically dispersed MAP instance.

E-notify means the act of sending notification of Incidents and the status of Tickets electronically.

Elective Change means a change requested by the Customer and is often the result of changes in the Customer Network, business processes, or the business. Elective Changes are not the result of Cisco Incident Management and Problem Management processes.

Elective Change Request means any request for service made by the Customer or Partner, in electronic format (submitted via the Portal).

EOL – End of Life

EOS – End of Sale

Host Device means chassis.

IOS means Cisco Internet Operating System.

Unified Communications (UC) means the functionality of providing traditional voice services, to include but not limited to, phones calls, convergence calls, or voicemail services, over an IP enabled Network.

Impact means the effect that the Incident has on the Customer Network

Incident means any event that is not part of the standard operation of a service and that causes or may cause an interruption to, or reduction in, the quality of that service.

Incident Management means the process to detect an incident, notify the Customer about the incident and resolve the incident.

Incident Resolution means the process to restore services on Managed Components.

Intelligent Monitoring means advanced correlation and automation of tools and scripts to enable quick response to Incidents.

IT means Information Technology.

Known Error means Incidents with a defined root cause and resolution.

Letter of Agency means a letter which authorizes Cisco to act as the Customer's agent for purposes of ordering, facilitating, tracking and/or providing services with Carriers, maintenance contract providers, and other general-service providers.

Managed Component means an element for which remote IT-infrastructure management services are provided by Cisco.

Management Application Platform (MAP) is suite of management applications and tools that Cisco uses to deliver ITIL based Service Management.

Management Connection means the physical communication link between the Cisco and the Customer Premise.

Management Connectivity means a bi-directional communication between the Customer Premise and Cisco for Management Data to be securely and consistently transmitted between Managed Components and Cisco.

Management Data means events, alerts, performance information, traps and/or log messages that are collected by the Service Management Application.

Management Readiness Assessment means an assessment that determines whether all Managed Components are in good working order prior to completion of Transition Management. Requires Managed Components are fully configured, deployed and functioning properly prior to the commencement of Incident and Problem Management services.

Management Services means a service that provides Monitoring, Incident Resolution, Reactive Problem Management, service level management and Standard Changes to resolve all Incidents.

Monitoring means detecting events on Managed Components.

Network means a set of interconnected and interworking Cisco supported hardware and software that is implemented, operated, and supported by Customer from a single Network operations center (NOC).

Network Component means a device or link that makes up part of a Network.

Non-Managed Component means any element for which management services is not provided by Cisco.

Normal Service Operation means service operation within Cisco service levels as defined in Section 4 Service Level Management.

OSI means the Open System Interconnection Reference Model.

Partner means the third party contracted by Customer to act as its technical point of contact with respect to the Service and/or Product.

Patch means a small fix to a problem using a piece of software code.

Point of Presence means a carrier aggregation point for access to carrier-provided Internet and wide area Network services.

Portal means the online Web user interface supplied for Customers and Partners to receive and submit information to and from the NOC.

Primary Management Connectivity means the management connection provided by Cisco.

Priority means the level of effort that will be expended by Cisco and the Customer to resolve the Incident.

Proactive Problem Management means the process to prevent Incidents.

Problem means the underlying cause of one or more Incidents.

Problem Analysis means the activity of investigating problems to determine the root cause.

Problem Management means the process to find and resolve the root cause of a Problem and prevention of Incidents.

Problem Resolution means the process of providing remediation based on the root cause for unknown Incidents.

Project Coordinator means the Cisco project manager who is the single point of contact thru the Transition Management phase.

PSTN means Public Switched Telephone Network.

PVC means Private Virtual Circuit.

Quote means quote for services.

Reactive Problem Management means the Problem Management sub-process that primarily supports Incident Management. These processes are initiated when an Incident cannot be matched to a Known Error.

Read means the ability to view system logs, configuration files and other device and system-level information.

Release Management means the process focused on the actual implementation of approved Changes.

Reseller means the business that sold Cisco management to the Customer.

Resolved means to remedy the Incident and close the Ticket out in the system.

Remediated means a corrected fault or deficiency.

Self-Diagnostic and Business Rules Engine means the ability to gather further diagnostic data and provide additional actionable recommendations.

Service Description means Cisco will provide the Services and perform Cisco responsibilities described in the standard Cisco Service Description located at www.cisco.com/go/servicedescriptions/ (or such other location of which Cisco may notify Customer from time to time).

Service Activation Kit (SAK) means a document that is completed by the Customer during the Transition Management phase.

Service Delivery means the phase after Transition Management when Cisco begins to deliver Services.

Service Desk means a single point of contact for Customers for the Service.

Services mean Cisco Remote Management Services which consist of the activities and the processes used by Cisco to monitor manage and make changes to your Network, voice and application services.

Standard Business Hours means 8AM to 5PM in the time zone of the Customer's headquarters (US & Canada).

Standard Change means a Cisco RMS recommended change that is often as a result of Incident Management and Problem Management processes or Cisco Field Notice.

Standard Change Request means a request for change to solve an Incident or Problem.

Start Date means the date Services commence.

SLA means Service Level Agreement.

SLO means Service Level Objective.

SLM means Service Level Management.

Termination Device means Customer Premises equipment that terminates the Management Connection.

Ticket means the tracking mechanism for Incidents and service requests within the NOC. The NOC activities are detailed within the Ticket that contains the complete history of record for an Incident or service request.

Transition Management means a phased process approach in which Cisco prepares Customer infrastructure for the Management Services.

Ticket Trending means analyzing tickets and ticket trends so that proactive steps can be taken to reduce or eliminate potential future incidents from occurring in the Network.

VPN means Virtual Private Network.

Write means the ability to make and save changes to device configurations.