Cisco Managed Services for Enterprise Common Service Description

This Service Description is designed to provide a baseline understanding of and set expectations about the Cisco Managed Services for Enterprise, hereinafter referred to as the Service, provided by Cisco. It must be accompanied by the appropriate Cisco Managed Services Technology Addendum. The Technology Addendum describes exceptions, differences or details applicable to that business service Offer not held within this Service Description. Information within each Technology Addendum holds precedence over information within this Service Description.

Technology Addendum(s):

- Cisco Managed Services for **Enterprise Networks**
- Cisco Managed Services for **Collaboration**: Unified Communications/Unified Contact Center
- Cisco Managed Services for **Collaboration**: Business Video
- Cisco Managed Services for **Data Center**: Infrastructure
- Cisco Managed Services for **Data Center**: Virtual Desktop Interface
- Cisco Managed Services for **Data Center**: SAP HANA
- Cisco Managed Services for **Security**

This Service Description in conjunction with the corresponding Technology Addendum describes the Service you have purchased from Cisco. Please read this document carefully as it contains important information regarding the Service.

Direct Sale from Cisco

If you have purchased the Service 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 the Service 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 the 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 from your Cisco Authorized Reseller.

Cisco only offers the Service to supplement a current support agreement for Cisco products, and the Service is 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 the Service described below as selected and detailed on the purchase order for which Cisco has been paid the appropriate fee.

Cisco shall provide a Quote for the Service setting out the extent of the Service and the term for which Cisco shall provide the Service. 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 the Service for Managed Components.

Two managed service packages are available:

- Standard Managed Services
- Comprehensive Managed Services

The tables below indicate the service packages available for each Offer and the deliverables available with each service package.

Service Package	Option	Enterprise Networks	Collaboration	Data Center	Security
Standard		X	X	X	X
	Proactive Problem Management and Root Cause Analysis	X	X	X	X
	PSIRT and Field Notice Evaluation and Execution	X	X	X	Included in Standard
	Service Operations Oversight and Management	X	X	X	X
	Time to Restore SLA	X	X	X	X
Comprehensive		X	X	X	X

Activities / Deliverables	Standard Services	Optional Services	Comprehensive Services
Transition Services	X		X
Device Monitoring	X		X
Incident Record	X		X
Incident Notification	X		X
Incident Management	X		X
Incident Priority and Classification	X		X
Incident Investigation and Diagnosis	X		X
Incident Resolution and Restoration	X		X
Incident Escalations	X		X
Incident Closure	X		X
Incident Resolution	X		X
Change Management	X		X
Release Management	X		X
Configuration Management	X		X

Activities / Deliverables	Standard Services	Optional Services	Comprehensive Services
Service Level Objectives	X		X
Web Accessible Portal	X		X
Standard Reports	X		X
Advanced Reports			X
Proactive Problem Management and Root Cause Analysis		X	X
PSIRT and Field Notice Evaluation and Execution		X	X
Service Operations Oversight and Management		X	X
Time to Restore SLA		X	
Defined Changes		X	
Custom Scoped Elective Changes		X	
Ticket eBonding		X	

1 Transition Services

Transition Services are required for all Managed Services prior to the Service transitioning to the Service Delivery phase. The Service is considered to be in the Service Delivery phase when Managed Components are under management. Under management is completed at the end of Onboarding process. The Customer must place a Purchase Order with Cisco and attach the related Service Description or Statement of Work to initiate Transition Services. Service start date is that date reflected in a customer PO or supporting documents establishing the start of services. Service term includes both Transition and Delivery phases.

1.1 Cisco Cloud and Managed Service Platform (CMSP)

The Cloud and Managed Service Platform (CMSP) is a suite of management applications that provides monitoring for all Managed Components in your solution. The Service may require the installation of a CMSP on your Network in order to provide monitoring coverage.

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

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

The CMSP is configured with Customer-specific installation and monitoring data prior to being placed into service. Once installed, this CMSP is configured with the components under management as indicated via the Service Activation Kit (SAK) and builds the inventory report.

Cisco responsibilities:

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

- Installation of operating system and supporting applications on the CMSP
- 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 CMSP is an integral part of the Service and is installed for the term of the Service. During the term of the Service, the Customer is granted a nonexclusive and nontransferable license to use the hardware and the software resident on the CMSP solely on the respective CMSP 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 CMSP and any and all associated CMSP materials (devices and documentation) and connectivity devices to Cisco immediately upon expiration or termination of the Service.

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

Customer responsibilities:

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

The Customer is also expected to provide the following:

- Installation of the CMSP and Network connectivity per Cisco-supplied guidelines
- Communications facilities and services including internet and Network configuration, maintained for the term of the Service
- A resource to support the installation of the CMSP including:
  - Racking
  - Connection to Network
  - Power connection to UPS or other facility with continuous uninterrupted power
  - Power-up
- Suitable commercial power, and an uninterruptible power system (UPS) or other acceptable power back-up facilities providing a minimum of 1kVA dedicated for the CMSP and termination device.
- Training coordination support including identifying trainees and trainee contact information

1.2 Cloud and Managed Service Platform Configuration

During this configuration phase, Cisco assists in executing a discovery process for Managed Components per the Purchase Order. The Project Coordinator will communicate any discrepancies between discovered devices and devices entitled in the Purchase Order. Any Customer-requested

additions beyond the Managed Components entitled in the Purchase Order will be subject to incremental Service fees and additional Transition Service process intervals.

Cisco inputs Managed Component information into the service CMSP 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 CMSP. This completes the configuration of the CMSP.

1.3 Onboarding Process

Cisco responsibilities:

Onboarding is a phased process approach in which Cisco works with the Customer to prepare the Customer infrastructure for the Service.

Customer responsibilities:

The Customer shall provide training coordination support including identifying trainees and trainee contact information. To enable Cisco to provide the Service for Managed Components, Cisco requires the Customer to:

- Assign a project manager to represent the Customer during the Onboarding process
- Assign a technical lead to assist Cisco with establishing the Network access required for remote management
- Ensure the project manager and technical lead attend the Customer project kickoff meeting and training sessions
- Mutual agreement of date concerning completion of the Onboarding process

1.3.1 Kickoff Meeting

Cisco will assign a Project Coordinator to act as a primary point of contact during the Onboarding process. Within fourteen (14) 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 as well as all remaining activities within the Onboarding process are typically facilitated by the Project Coordinator in collaboration with Cisco Engineers assigned to the Customer account.

The Onboarding process 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 Management Connectivity
- Facilitating discovery of Managed Components into the Cisco infrastructure
- Creation of Services Manual

1.3.2 Management Readiness Assessment

Management Readiness Assessment is a review conducted by Cisco technical analysts that determines whether the Managed Components are in good working order prior to completion

of the Onboarding process. This requires that the Managed Components be fully configured, deployed and functioning properly prior to the commencement of the Service.

1.3.3 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 Onboarding process.

Cisco responsibilities:

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 POP 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.

Customer responsibilities:

- The Service is 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 the SAK. Customer must provide Read management access for components that are monitored only. Customer must ensure 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 the Service.
- In support of connectivity to the Cisco POP, Customer will be required to provide, in certain deployments, a mail relay server for communication back to Cisco.

1.3.4 Termination Device

Cisco responsibilities:

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.

Customer responsibilities:

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. Customer must return the Termination Device to Cisco immediately upon expiration or termination of the SOW or the Service. 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. Failure to allow timely access may invalidate Cisco SLAs and SLOs, if any, and delay restoration and performance of the Service.

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.
- 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 Onboarding activities.

1.3.5 Service Activation Kit

Reviewing the SAK components and key information is critical to success for the Onboarding process. 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 the Service.

Cisco responsibilities:

- Complete tasks defined in the SAK to enable CMSP 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 the Onboarding process.

Customer responsibilities:

Complete the SAK, which provides the key information critical to success for Onboarding Services 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 CMSP
- Device location and naming scheme
- Management IP addresses and system detail, SNMP community strings
- Configure Managed Components with access credentials such as SNMP community strings, user names, passwords, etc. (can be performed by Cisco for additional fees)
- 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.)

1.4 Customer Acceptance

Cisco will work with the Customer to validate that the Onboarding process is complete. Upon the date of Customer Acceptance, the Service transitions from Onboarding to the Service Delivery phase. All exceptions to the Service Delivery phase must be documented within the Transition Services material. Exceptions may include removing devices from SLO/SLA consideration due to inability to monitor or manage Managed Components effectively that are not under full management.

2 Standard Managed Services Package

This section will describe activities and deliverables provided within the Standard Managed Services Package.

2.1 General

Cisco responsibilities:

All Managed Services are provided remotely—not on Customer site—unless otherwise specified within this or relating documentation.

Customer responsibilities:

Cisco has a co-management approach to the Service, 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 Onboarding process.

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 a 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.

2.2 Software Updates for the Cloud and Managed Service Platform (CMSP)

The Service includes routine software updates for the CMSP. The Customer will receive an e-mail notification from Cisco that identifies the modifications included in the next release. Cisco will schedule a maintenance window for updating the CMSP. 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.

2.3 Device Monitoring

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

Activities:

- 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 Configuration Management Database (CMDB)
- Access provided via the Portal to ticketing and reporting details

2.4 Incident Record

An Incident Record is generated when the Cisco ticketing system captures alarm/event/correlation data and enrichment with relevant configuration Items information that results in the creation of an Incident Ticket.

Activities:

- Enrich alarm information with relevant configuration item information from the CMDB
- Enrich alarm information with relevant information from Cisco, where applicable
- Auto-close Incident Tickets based upon a configurable timer

Deliverable(s):

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

2.5 Incident Notification

Cisco will electronically notify (E-notify) designated Customer contacts for new Incidents or milestones achieved. Notifications 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 Portal.

Activities:

- Automatically E-notify specific Customer contact(s) based on Customer's notification requirements as agreed on during the Onboarding process

Deliverable(s):

- Incident Tickets per Customer's notification profile (Default)
- Log of E-notify records in the Incident Ticket
- Updated Incident information available via Portal

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

2.6 Incident Management

Incident Management is an ITIL process used by the Service to identify Incidents, restore service and remediate declared Incidents as quickly as possible and may involve implementing a temporary work-around. Cisco 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 Service Desk. For any high priority Incidents (system down, degraded performance, etc.), Customer should contact the Service Desk via telephone. Low priority Incidents should be reported by Customer to the Service Desk via the CMSP Portal.

Cisco responsibilities:

Upon automatic detection or manual submission of an Incident to the Service Desk, an Incident Ticket is created. The 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.

Customer responsibilities:

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 Service Package sections. The Customer must:

- Provide support contracts, Letters of Agency, and all other end Customer documentation and authorization required to facilitate Incident Resolution.
- Maintain hardware maintenance and/or software maintenance as may be applicable on all Managed Components identified in Purchase Order for the term of the Service.

2.6.1 Incident Priority and Classification

Incident Priority and Classification is considered a subset of Incident Management whereby Cisco Incidents are managed according to the Priority level as defined in the Service Level Objectives for Cisco Managed Services.

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
- Status report for prioritized Incident against its associated Service Level as defined in SLO Metrics section herein

2.6.2 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 isolate the root cause of the Incident, diagnose and match the Incident to a known error in the Cisco Managed Services knowledge base 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 Managed Service knowledge base

Deliverable(s):

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

2.6.3 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 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 engineer requires to restore functionality to a Managed Component or remediate an Incident on the Customer's Network.

The Service 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 remain open and will be worked by Cisco engineers until resolved, in accordance with the Priority level of the Incident.

Incident Resolution and Restoration may include Cisco 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 engineers may provide recommendations for remediation of an affected Managed Component.

If a configuration change in a Managed Component is required to resolve an issue or implement a work-around, the Cisco 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 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

2.6.4 Incident Escalation

Incident Escalation 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 Service Desk. Cisco 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 engineering resources to meet Service Level Objectives
- Escalate Incident as appropriate to the Cisco 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
- Notification (E-notify) for this Incident Ticket event milestone, if requested by the Customer

2.6.5 Incident Closure

Incident Closure is considered to be a subset of Incident Management whereby once Cisco 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 RFC to resolve the recurring Incident.

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

Activities:

- Confirm Incident is resolved
- Open a Cisco-recommended RFC if Incident re-occurs, depending on frequency and attributes of the Incident

Deliverable(s):

- Updated Incident Ticket to include closing notes
- Closed the Incident Ticket
- Notification (E-notify) for this Incident Ticket event milestone, if requested by the Customer.

2.7 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.

2.7.1 Change Management

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. 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.

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 pertinent architecture Technology Addendums.

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

Note: Only Standard Changes are included as part of the Managed Service Package. Elective Changes are a Managed Service option and can be provided for additional fees.

2.7.2 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 Product Security Incident Response Team (PSIRT) notices. Note, not all Cisco field notices or Cisco PSIRTs will be executed as part of Standard Changes. Field notice and PSIRTs will be evaluated by Cisco for the Service stability, vulnerability and security and executed at Cisco's discretion. A Cisco Engineer will submit an RFC to start the Change Management process. Standard Changes are included in the Standard Managed Services package.

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

For PSIRTs that may impact the stability of the Service, the Customer will be notified of details of the PSIRT notice describing the nature and impact. If Cisco deems it as important to improve the Service stability, Cisco will initiate Release Management activities to execute where necessary to address Service stability concerns, at Cisco's discretion.

Note: PSIRT notices that Cisco has identified as non-impacting to the Service stability, fall outside the scope of Standard Changes and are supported through Elective Changes outlined below.

A Ticket is created to track the resolution of a Change. In addition, 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 defines Cisco recommended changes which are part of Service:

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

2.7.3 Organize, Prepare, and Close

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.

2.7.4 Configuration Management

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

2.7.5 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 has been executed, the environment will be tested 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.

2.7.6 Applying Software Updates

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 an Elective Change element. If Customer requests Cisco to execute a Cisco Field notice and/or Cisco PSIRT that has been deemed as non-service affecting by Cisco, it will be treated as an Elective Change. If the Customer does not agree with the Cisco's evaluation of the Field Notice and/or PSIRT, it is the Customer's responsibility to demonstrate Service stability is jeopardized by not executing the Cisco Field Notice or PSIRT notice.

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.

2.7.7 CMSP Updates

CMSP updates are focused on the implementation of endpoint device or application software updates to the Customer's technology environment if deemed necessary by Cisco to maintain a stable managed environment. In addition, Cisco will periodically enhance functionality within the CMSP solution. Cisco will use reasonable efforts to provide 1 Week notice prior to the implementation of a CMSP update.

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

CMSP 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.

2.8 Account Oversight

- Oversight of P1 incidents and high visibility escalations, providing feedback and input as required to expedite the incident Monitoring of return materials authorizations (RMAs).
- Coordination and escalation with and to Cisco support organizations pertaining to managed environment – Cisco Technical Services and Cisco Advanced Services

2.9 Cisco Managed Services 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 Onboarding process, Customers receives accounts for authorized employees to access the Portal.

Information available from the 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 the Cisco Managed Service for multiple technologies.

2.10 Reports

The Standard Managed Services package includes the Standard level of reports. These reports will be made available on the Portal.

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

2.11 Managed Components Covered Under the Service

Cisco responsibilities:

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

Please note that while Cisco strives to deliver a Service 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 intends to bring newly released devices under management as soon as possible; however, some delays may occur due to device complexity or other factors outside of our control.

Customer responsibilities:

- Ensure that all Managed Components are in good working order prior to completion of the Onboarding process. This means that Managed Components are fully configured, deployed, and functioning properly prior to the commencement of the Service. Good working order status will be verified by Cisco during the Management Readiness Assessment process and using availability and performance reports during the Onboarding process. Required remediation steps are provided to Customer by Cisco.
- Perform 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 the Portal) in accordance with policies established.
- Allow Cisco to retain and publish aggregate statistics and metrics for non-identifiable trending analysis.
- Provide sufficient backup for all applications and operating systems. The Customer is responsible for ensuring the backups run successfully.
- Perform backup on devices not running Cisco Catalyst OS or Cisco IOS. The Customer is responsible for ensuring the backups run successfully.

2.12 Non-Managed Components

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

2.13 Service Support

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

- General CMSP assistance
- 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

2.14 Service Manual

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

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

2.15 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.

2.16 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 Appendix for a detailed description of the priority levels and SLOs.

2.17 Training

- Access to Technical Expertise/Knowledgebase for ad hoc requests pertaining to managed devices when necessary, shall be delivered remotely via video or meeting methods, such as WebEx.
- Instructional sessions on service operations and/or service consumption readiness. Leverage existing pre-recorded videos and documentation as available or remotely via video or meeting methods, such as WebEx.

2.18 Service Level Management

- Primary point of contact for operations and process issues
- Automated monthly operations reports in standardized format - status, track progress of open service requests, and other outstanding operational issues with the customer
- Quarterly Interactive Business Reviews (QBRs) in standardized format reviewing outstanding operational issues reporting on status and progress of P1 issues. Delivered over WebEx.

2.19 Optional Services for Standard Managed Service Package

The following options are available to be added to the Standard Managed Services package for an additional fee. These service package options are only available for the Standard Managed Services package and can be added independently of each other.

- Proactive Problem Management and Root Cause Analysis reports based upon an analysis of the following relevant to the Customer's infrastructure:
  - Configuration analysis
  - Incident trend analysis
  - Problem trend analysis

  A Cisco Engineer will create up to 8 Root Cause Analysis reports per year and provide them to the customer during one of the regularly scheduled Business Reviews. Customer must request the incidents for which they would like this service provided in advance of the meeting. P1 incidents or recurring P2 or P3 incidents will be reviewed.
- Proactive PSIRT and Field Notice Evaluation and Execution – Evaluate and Execute those PSIRT or Field Notices that affect Service stability or are applicable to the Customer's managed deployment.

  - PSIRTs
  - Field notifications
- Service Operation Oversight and Management providing Monthly Business Reviews (MBRs) in a custom format based on customer needs to address outstanding operational issues reporting on status and progress of P1 and P2 issues. Delivered over WebEx but may be delivered at Customer location if agreed to in advance.

3 Comprehensive Managed Services Package

All activities and deliverables defined and listed in the Standard Managed Services package are included as part of the Comprehensive Managed Services package. The objective of the Comprehensive Service Package is to ensure that the Service Customers are provided the high touch business and technical oversight to ensure technology solutions meet the Customer's business objectives. Listed below are the Activities and Deliverables for the Standard Service Package.

Activities

- Provide oversight of P1 and P2 Incidents and high visibility escalations, providing feedback and input as required to expedite the Incident.
- Perform Service level monitoring and reporting including Return Material Authorization (RMA) delivery performance reports delivered to Customer on an agreed-upon frequency, with follow-up within Cisco and with the Customer on identified gaps to help ensure improved performance.
- Acquire a good technical understanding of the Customer's Network.
- Provide advanced engineering support for troubleshooting issues related to the Service.
- Collaborate with Cisco Operations Manager on training sessions
- Participate in operational reviews facilitated by Operations Manager, provide engineering insight for dialog with customer
- Provide 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
- Fine-tune capacity/performance (targeted at infrastructure device level environmentals)
- Provide 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

Deliverables:

- 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 to manage Change Management initiatives undertaken by the customer and/or recommended by Cisco support teams
- Root Cause Analysis Reports – 8 reports per year

- Designated resource with a good understanding of the Customer's infrastructure

4 Optional Managed Services

The following additional activities and deliverables can be applied as options to the Service as part of ALL Managed Service Packages.

4.1 Elective Changes

Elective Changes are changes that are not the result of Cisco Incident and Problem Management processes or Cisco Managed Service recommended changes to address Field notices and Cisco PSIRTs. There are two types of Elective Changes available:

- 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 require 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.

All purchased support hours must be used within the contract term. 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.

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. 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 1/31/2015 and the new contract ends 3/31/2016, then the newly acquired support hours expire on 3/31/2016.

4.1.1 Defined Changes

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. The Customer identifies the needed type of change and submits a change requests on the Portal.

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 appendix. Cisco has categorized Defined Changes into types based on level of complexity and the amount of time required to complete the change. Additional details outlining the specific changes are available in the individual Technology Addendums. 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

Cisco may elect to offer additional services within its areas of competency in response to a Customer's request

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

- As Defined Changes are executed, support hours are deducted from the balance available to the Customer based on the type of change (see table above).
- 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. 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 for the purpose of upgrading a Managed Component for purposes not related to Incident or Problem Management or part of a Cisco Managed Services Release or Cisco Managed Services recommendation to maintain the Service stability. 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.
- Cisco Field Notices and PSIRTs that have been deemed as non-impacting to the stability of the Service but are requested by the Customer
- All changes not categorized as a Cisco Managed Services release.
- Examples of Cisco Custom Scoped Elective Change services are itemized in the specific Technology Addendums. Cisco may elect to offer additional services within its areas of competency in response to a Customer's request for service.
- Rollout and execution of Custom Scoped Elective Changes:
  - Rollout planning defines 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 Cisco Managed Services for Ticket eBonding

The optional eBonding service electronically bonds a Customer's Information Technology System Management (ITSM) tool (ticketing system) with the ticketing tools and platform used by Cisco for the delivery of Managed Services. This eBonding capability is enabled by Cisco ServiceGrid technology, a service integration platform in the Cisco-hosted cloud that seamlessly connects Customers to Cisco to enable a more automated and highly collaborative service experience.

The eBonding service includes:

- Access to the Cisco-hosted service integration platform (ServiceGrid) and ongoing Day-2 support to maintain a bi-directional ticketing exchange between the Customer and Cisco.
- Three specific ITIL-based workflow processes used in the delivery of the Service:
- Service Request Management workflow
  - Customer initiates creation of service request ticket in Cisco ticketing system from the Customer's ITSM system
  - Cisco initiates creation of service request for the Customer
- Incident Management workflow
  - Service requests opened through the eBonding service follow the normal Incident Management workflow and may result in the creation of a Change Ticket
  - Incident tickets created in the Cisco ticketing system will open a corresponding Incident ticket in the Customer's ITSM system.
- Change Management workflow
  - Change tickets created in the Cisco ticketing system will open a corresponding Change ticket in the Customer's ITSM system

  - Change tickets created through the eBonding service follow the normal Change Management workflow and may require Customer approval to be fully implemented
- Tickets eBonded across Cisco and the Customer's ITSM systems can be bi-directionally viewed, updated, and closed in the native ITSM system without the need for Web Portal, email or phone interactions

Customer responsibilities specific to e-bonding include:

- Meet pre-qualification requirements for the eBonding service as defined in Cisco Managed Services eBonding Technical Qualification Guide
- Assign a technical lead to review the Cisco Managed Services for Enterprise eBonding Onboarding Guide
- Collaborate with Cisco transition service resources to configure and test the eBonding solution
- Once all Transition Services configuration and testing activities have been completed in collaboration with the assigned Cisco project management / technical lead acknowledge and accept the eBonding solution is live and available for use in the delivery of the primary managed service(s) that Customer has purchased from Cisco.
- Note Transition Services must be purchased separately. Activation details are described in the applicable Cisco Managed Services for Enterprise eBonding Onboarding Guide.

Cisco responsibilities specific to e-bonding include:

- Assign a project management / technical lead to drive all Transition Services activities to enable the Cisco Managed Services for Enterprise eBonding managed service
- Align with Customer on the Transition Services timeline to configure and activate the eBonding solution
- Work directly with the Customer's technical lead to configure and test the eBonding solution
- Complete Transition Services project within agreed upon schedule and obtain acknowledgement from the Customer that the eBonding solution is active and delivering the functionality as defined in this service description

5 Services Not Covered

Services that are not expressly set forth in the applicable Service Description document are not covered under such Services Description including, without limitation, the following:

- Services for any hardware or software not considered part of generally available Products and Software releases/versions, unless agreed otherwise.
- Services that require specific nationality, citizenship, language or any security clearance (i.e., secret, top secret) in a foreign country by Cisco personnel or its subcontractors, unless otherwise expressly agreed by Cisco.
- Any customization of, or labor to install, software and hardware (including installation of updates).
- Furnishing of supplies, accessories or the replacement of expendable parts (e.g., cables, blower assemblies, power cords, and rack mounting kits).
- Electrical or site work external to the products.
- Any expenses incurred to visit Customer's location, except as required during escalation of problems by Cisco.

- Service for hardware that is installed outdoors or that is installed indoors but requires special equipment to perform such Service.
- Hardware replacement in quantities greater than three (3) FRUs, including those replacements due to pervasive issues documented in an engineering change notice or field alert unless Customer has troubleshot failed hardware down to the FRU level.
- Services performed at domestic residences.
- Support or replacement of Product that is altered, modified, mishandled, destroyed or damaged by one or more of the following: (i) natural causes; (ii) environmental failures; (iii) your failure to take any required actions; (iv) a negligent or willful act or omission by you or use by you other than as specified in the applicable Cisco-supplied documentation; or (v) an act or omission of a third party.
- Services or software to resolve software or hardware problems resulting from a third party product or causes beyond Cisco's control or failure to perform responsibilities set out in this document.
- Services for non-Cisco software installed on any Cisco Product.
- Any hardware or third party product upgrade required to run new or updated software.
- Erasure or other removal of any customer or third party data on Products (or parts thereof) returned, repaired or otherwise handled by Cisco.

Additional Services outside those expressly set forth are provided at the then-current time and materials rates.

Except as otherwise agreed, software entitlement, including media, documentation, binary code, source code or access in electronic or other form is not provided. In addition, except as otherwise provided, no right, use or license to our software is granted and you acknowledge and agree that you obtain no such rights.

Application Software is not supported as part of the SMARTnet or Small Business Support Services provided by Cisco and is only supported under the Software Application Services (SAS/U) or Essential Operate Services service description.

Appendix A: Service Level Objectives

This appendix describes the Service Level Objectives (SLOs) for the Cisco Managed Service for Enterprise Offers, including:

- Cisco Managed Service for **Enterprise Networks**
- Cisco Managed Service for **Collaboration**: Unified Communications/Unified Contact Center
- Cisco Managed Service for **Collaboration**: Business Video
- Cisco Managed Service for **Data Center**: Infrastructure
- Cisco Managed Service for **Data Center**: Virtual Desktop Interface
- Cisco Managed Service for **Data Center**: SAP HANA
- Cisco Managed Service for **Security**

These SLOs define the service level metrics that Cisco tracks for the Service. These objectives are divided into two major sections: Network Operation Center SLOs and Security Operations Center SLOs.

1 Network Operations Center Service Level Objectives

1.1 Incident Management

The monitoring and Incident notification work together with Incident Resolution processes to form the Incident Management service component. Incident Management restores Normal Service Operation within a reasonable time to contain the adverse impact on business operations, service quality and availability.

Cisco will:

- Utilize Incident remediation procedures to collect any additional data required to diagnose and match to Known Errors in our Knowledge Base
- Work to restore services within agreed service objectives, initiating Change Management as needed for restoration
- Coordinate the dispatch of support personnel to the Customer Premises to perform necessary onsite repairs as per the end-Customer maintenance and support contracts. This requires a signed Letter of Agency by the Customer.
- Remotely assist onsite personnel as needed to facilitate service restoration.
- Remotely facilitate hardware replacement and software updates determined to be required by Cisco.

1.2 Incident Prioritization

Cisco classifies and prioritizes Incidents according to 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
- Classify Incidents into fault or performance Incident categories as appropriate

Deliverable(s):

- Properly prioritized Incidents based on Incident Ticketing attributes
- Properly classified Incident based on the Incident Ticketing attributes

1.2.1 Impact Definitions

An Incident is classified according to its impact on the business (the size, scope, and complexity of the Incident).

Impact is a measure of the business criticality of an Incident or Problem, often equal to the extent to which an Incident leads to degradation of a service running on the Network. Cisco shall work with Customer to specify impact for each Managed Component during the Onboarding process.

There are four impact levels:

- **Widespread:** Entire Network is affected (more than three quarters of individuals, sites or devices)
- **Large:** Multiple sites are affected (between one-half and three-quarters of individuals, sites or devices)
- **Localized:** Single site, room and/or multiple users are affected (between one-quarter and one-half of individuals, sites or devices)
- **Individualized:** A single user or meeting is affected (less than one-quarter of individuals, sites or devices)

1.2.2 Urgency Definition

Urgency defines the criticality of the Incident or Problem to the Customer's business. Cisco shall work with the Customer to understand and set the proper urgency level.

Cisco Incident and Problem urgency levels are defined as follows:

- **Critical** – Primary business function is stopped with no redundancy or backup. There may be an immediate financial impact to the Customer's business. The Customer determines the issue as critical.
- **High** – Primary business function is severely degraded or supported by backup or redundant system. There is a probable significant financial impact to the Customer's business. The Customer perceives the issue as high.
- **Medium** – Non-critical business function is stopped or severely degraded. There is a possible financial impact to the Customer's business. The Customer perceives the issue as medium.
- **Low** – Non-critical business function is degraded. There is little or no financial impact. The Customer perceives the issue as low.

1.2.3 Priority Definitions

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

Cisco Incident Management priorities are defined as follows:

- **P1: Critical** – Cisco and the Customer will commit any necessary resources 24x7 to resolve the situation.
- **P2: High** – Cisco and the Customer will commit full-time resources during Standard Business Hours to resolve the situation.

- **P3: Medium** – Cisco and the Customer are willing to commit resources during Standard Business Hours to restore service to satisfactory levels.
- **P4: Low** - Cisco and the Customer are willing to commit resources during Standard Business Hours to provide information or assistance.

	IMPACT				
URGENCY		Widespread	Large	Localized	Individualized
	Critical	P1	P1	P2	P2
	High	P1	P2	P2	P3
	Medium	P2	P3	P3	P3
	Low	P4	P4	P4	P4

Cisco will downgrade the ticket priority in accordance with reduced severity of impact or Incident resolution. The case may be left open for a prescribed period while operational stability is being assessed.

Incident Ticket shall be closed by Cisco or Customer upon validation of issue remediation and the systems return to operational stability.

Ticket detail resides in a Knowledge Base which is used to support Incident Management and Problem Management processes.

2 Network Operations Center SLO Metrics

Service Level Objectives apply only to Managed Components that are managed exclusively by Cisco within the Service. Cisco adheres to the SLOs during the Service Delivery phase.[1] Within the SAK, the Customer and Cisco must document their agreement to formally acknowledge the completion of the Onboarding process. The Service Delivery phase commences upon mutual agreement between Cisco and the Customer that the Transition Services phase is complete and that the Service Delivery phase has been reached.

The following Incident metrics are tracked as Service Level Objectives:

- Time to Change (TTC)
- Time to Notify (TTN)
- Time to Restore (TTR)

[1] Cisco cannot adhere to the SLOs during the Transition Services phase. Within the Service Activation Kit, the Customer and Cisco must document the exit criteria for the Transition Services phase.

2.1 Time to Change (TTC)

Cisco has categorized 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 Customer schedule. A change request must be fully qualified and scheduled with the customer before the TTC metric starts. All Custom Scope Elective Change requests are scheduled events and follow Change Management procedures.

Additional details are available in the individual Technology Addendums and outline the specific change types. TTC SLOs are only available for Managed Enterprise for Collaboration: Unified Communications. The chart below provides a break-down of the available categories and durations for Small, Medium, and Large changes.

Category	Size
Type 1	Small
Type 2	Small
Type 3	Med
Type 4	Med
Type 5	Med
Type 6	Large
Type7	Large
Type 8	Large

Cisco SLOs for completing approved Change requests are as follows:

TTC Objective	Change Type*
3 Business Days	Types 1 and 2 Up to 12 changes per customer per business day
Within 5 business Days**	Types 3 and 4 Up to 6 changes per customer per business day
No SLO, scheduled	Type 5 - 8

*Note: See specific Technology Addendums for individual change type categories.
**Note: SLO time commences when all necessary detail to execute the change is available.

Business days are Monday through Friday, excluding Cisco-observed holidays.

SLO measurements exclude the following:

- Delays caused by Customer in executing the requested change (for example, waiting for response on change window)
- Any mutually agreed schedule of activities that causes service levels to fall outside of measured SLO defined obligations.
- Other factors outside of Cisco's reasonable control for which Cisco is not responsible

- Cisco or third party hardware dispatch and replacement
- SMARTnet cycle time (not included in the SLO measurement)
- Ticket closure time may be different than change completion time. For example, a Ticket may be kept open for review after the change has been executed.

Any Customer-requested changes that are considered by the Customer as “emergency” or “urgent” changes will be treated with a commercially reasonable effort by the Cisco NOC/SOC and will depend on Cisco NOC/SOC engineer availability at the time of submittal. Additional charges may apply.

2.2 Time to Notify (TTN)

Customers may have specific incident notification requirements for which the Service will offer a TTN objective. Cisco will respond to incidents raised through the management platform by electronically notifying a specified Customer contact(s) within the TTN timeframe. The Cisco SLO for meeting this objective is as follows:

- Electronic notifications may be generated automatically and sent to customer contacts as specified during the Transition Management phase.

TTN Objective	Incident Level
15 Minutes from ticket creation	All Priority Incidents

2.3 Time to Restore (TTR)

Incidents go through many stages with restoration being a primary objective. TTR tickets include all remote incident management activities (alarm or call receipt through restore, excluding maintenance or carrier cycle time). Time to Restore shall mean the time period from occurrence of the Incident until Cisco restores the Managed Component to a usable level of functionality.

Cisco SLOs for meeting this objective is as follows:

TTR Objective	Incident Level
4 Hours	P1 incidents
12 Hours	P2 incidents
72 Hours	P3 incidents
120 Hours	P4 incidents

SLO measurements exclude the following:

- Delays caused by Customer in resolving the qualifying issue (for example, waiting for response on change window or on-site resources)
- Any mutually agreed schedule of activities that causes service levels to fall outside of measured SLO defined obligations.
- Delays or faults caused by third party equipment or vendors, such as Carriers, in resolving the qualifying issue
- Other factors outside of Cisco’s reasonable control for which Cisco is not responsible

- Cisco or third party hardware dispatch and replacement
- Acquisition and installation time of new software to be installed on the Managed Component due to software defects or bugs
- SMARTnet cycle time is not included in the SLO measurement.

3 Security Operations Center Service Level Objectives

The nature of Security Operations differs from Network Operations sufficiently to demand separate SLOs. The SLOs for the following Cisco Remote Operations Security Services are described in the document below:

- Cisco Managed Services for Security

The following Incident metrics are tracked as SLOs specifically for Security Managed Services and pertain to security events and not fault events. A fault or performance event is specific to the availability and performance of the actual security device. A security event is defined as anything detected which is considered malicious in nature or intended to cause degradation to the network resources and / or assets.

Service Level Management for Cisco Managed Services for Security

Once the event is determined to be anomalous in nature or a security threat, that event is then classified within the Mean Time To Classify (MTTc) objective.

Security Incident Classification Codes:

- **Benign:** Traffic that is not harmful to network integrity
- **Attack:** An attempt to gain unauthorized access to protected data or deny access to networks
- **Denial of service (DoS):** An attempt to saturate the network resources
- **Malware:** Detection of software designed to infiltrate or cause damage to resources
- **Misuse:** Internal misuse of network and data resources
- **Recon:** Scanning a network for vulnerabilities
- **Suspicious traffic:** Not enough data available to rule out an attack and classify it as benign

APPENDIX B: 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 Managed Services 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.

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 Onboarding process.

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.

CMSP Disaster Recovery means the deployment of necessary CMSP elements to sustain Service in the event of a complete failure of the primary CMSP instance. Implementation may constitute deploying a geographically dispersed CMSP 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, 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, including but not limited to, phones calls, convergence calls, or voicemail services, over an IP enabled Network.

Impact means the effect that an 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.

Cloud and Managed Service Platform (CMSP) is a 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 the Onboarding process. 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 Cisco does not provide management services.

Normal Service Operation means service activities within Cisco service package as defined starting with Section 2, Standard Service package.

Offer means a distinct service for a specific technology or solution. Managed Enterprise Networks and Managed Collaboration are distinct and separate Offers.

Onboarding means a phased process approach in which Cisco prepares Customer infrastructure for the Service.

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 Onboarding process.

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 out the Ticket 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 Onboarding process.

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

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

Services Manual means a document that provides the Customer with a detailed job aid to be used as a guide once the transition phase ends

Services mean Cisco Managed Services which consist of the activities and the processes used by Cisco to monitor, manage and make changes to the Customer's 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 Managed Services 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 the Service commences.

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.

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.