



Cisco Offer Based Channel Model Audit and Policies Document

Table of Contents

Introduction	3
▪ Purpose	3
▪ Terms and Definitions	3
Requirements Overview Tables	4
▪ Prequalification Requirements	4
▪ Core Program Requirements: Pre-Sales/Plan, Design and Implement	5
▪ Core Program Requirements: Service Support	6
▪ Core Program Requirements: Service Delivery	7
Detailed Program Requirements	8
▪ Prequalification Requirements	8
▪ Core Program Requirements: Pre-Sales/Plan, Design and Implement	16
▪ Core Program Requirements: Service Support	20
▪ Core Program Requirements: Service Delivery	27
Audit Process and Methodology	31
▪ Audit Scheduling	31
▪ Role of Audit Participants	31
▪ Audit Closure and Follow Up	32
Appendix 1: Sample Audit Agendas	33
▪ Gold/Silver Certification: Cisco Collaborative Services Program, Shared Support Program, Reseller Support and SIS	33
▪ Gold/Silver Certification: Cisco Branded Resale and Packaged Services Program	34
▪ Master Unified Communication Specialization	35
▪ Master Security Specialization	36
▪ Managed Services Certification	37
Appendix 2: Program Policies	38
▪ Program Policies Overview Table	38
▪ Detailed Program Policies	40

Introduction

The industry is changing, customer needs are evolving, and the ways in which Cisco® and our partners drive growth and differentiate ourselves is changing. We're in the midst of an industry evolution in which the network is becoming the platform for all communications, collaboration and interactions. This evolution is creating unprecedented growth opportunities for Cisco and our partners. Customers are demanding integrated technology skills breadth, technology skills depth, and a full-lifecycle-services approach to implementing more sophisticated solutions. Business models are changing to meet customers' needs and to adapt to the different ways in which they want to buy products and services. The industry-leading Cisco Channel Partner Program enables partners to drive growth and differentiate their business by extending their capabilities to meet these customer requirements. As a result, partners can be providers of integrated networking solutions, highly specialized solutions, or both.

The Cisco Channel Partner Program is a value-based program centered on the partner's ability to deliver business solutions built upon Cisco's technologies. The program rewards partners for the value they bring to our joint customers and recognizes the differing models by which partners are doing business through Resale, Managed Services, and Outsourcing. Additionally, Cisco recognizes partners that have made an investment in multiple countries as being Multinational, and partners that meet the Global requirements are recognized as a Global Partner.

Certification level is based on offer types which provide a clearer definition of each level and its value to customers.

Credibility: As one of the strongest brands in the world, the Cisco name lends enormous credibility to companies that achieve Cisco Certified Partner status. Customers feel more comfortable and secure purchasing from a Cisco partner.

Quality Standards: Cisco is the only company that hires and funds an objective third party to conduct annual audits of its silver and gold partners. These audits help ensure that only the highest quality partners are part of the program and that partner companies meet uniform standards set by Cisco.

Partner Locator: This valuable online tool allows customers to search globally for partners who are qualified for specific sales situations. The Partner Locator also features information about partner qualifications, certifications, and specializations.

Technology Learning: Partners can access the latest networking technologies through a variety of learning tools to stay at the leading edge of their respective markets.

Best Practices: Partners can capitalize on Cisco best practices such as regular customer satisfaction surveys. Partners have access to the same tools that Cisco uses to enhance its own customer satisfaction.

Prequalification Requirements

This table provides an overview of requirements only. See linked requirements for details.

Requirement	Description	Gold	Silver	Master UC	Master Security	Managed Services (MSCP)
Agreements/Contracts	Must have the appropriate purchasing/support agreements	✓	✓	✓	✓	✓
Specializations	Must have qualifying Specializations	✓	✓	✓	✓	N/A
Personnel	Must have certified personnel as determined by specialization roles and program rules	✓	✓	✓	✓	✓
ATP	Must be part of Cisco Authorized Technology Provider (ATP) Program	N/A	N/A	✓	N/A	N/A
NOC	Must have a Network Operations Center	N/A	N/A	N/A	N/A	✓
Support Lab	Must have support labs (*CSSP only)	✓*	✓*	✓	✓	✓
Customer Satisfaction	Must participate in CSAT program	✓	✓	N/A	N/A	N/A
Service Offerings	Must provide Service Descriptions, Service Level Agreements (SLAs) and contractual descriptions of offerings	N/A	N/A	✓	✓	✓
Customer Reference Accounts	Must provide evidence of customer sales, with supporting reference documentation	N/A	N/A	✓	✓	N/A
Vulnerability Assessment	Must provide evidence of a process for conducting a Vulnerability Assessment	N/A	N/A	N/A	✓	N/A
Service Attach Rate	Must demonstrate a minimum 40% Service Attach Rate (*CBR only)	✓*	✓*	N/A	N/A	N/A
Revenue from Services	Must recognize a minimum of at least 15% of revenue from services (*CBR only)	✓*	✓*	N/A	N/A	N/A

Core Program Requirements

These tables provide an overview of requirements only. See linked requirements for details.

Pre-Sales/Plan, Design and Implement						
Requirement	Description	Gold	Silver	Master UC	Master Security	Managed Services (MSCP)
Demonstration	Ability to demonstrate the product/service for a specific customer case	✓	✓	✓	✓	N/A
Project Management	Evidence of a process for managing customer projects	✓	✓	N/A	N/A	N/A
Capacity Planning	Evidence of ongoing resource/capacity evaluation and planning	N/A	N/A	✓	✓	✓
Design	Evidence of design activity, including design reviews, records	✓	✓	✓	✓	✓
Quality Assurance	Evidence of acceptance testing procedures	✓	✓	N/A	N/A	N/A
Hiring and Training	Evidence of training plans and records for relevant processes and tools	✓	✓	✓	✓	✓

Service Support						
Note: If partner maintains current registration to ISO 20000, these requirements do not apply. Certification must be valid for at least one year from the date of Cisco's on-site audit.						
Requirement	Description	Gold	Silver	Master UC	Master Security	Managed Services (MSCP)
<u>Incident Management</u>	Evidence of service support for detected and/or reported incidents, including escalation if necessary	✓	✓	✓	✓	✓
<u>Problem Management</u>	Evidence of root cause analysis and problem resolution (*CSSP only)	✓*	✓*	✓	✓	✓
<u>Configuration Management</u>	Evidence of configuration control	N/A	N/A	✓	✓	✓
<u>Change Management and Release Management</u>	Evidence of change control and hardware/software release control	N/A	N/A	✓	✓	✓
<u>On-Site Response/Troubleshooting</u>	Evidence of processes for providing on-site troubleshooting (*CSSP only)	✓*	✓*	✓	✓	✓
<u>Remote Troubleshooting Access</u>	Tools for remote access for troubleshooting purposes	N/A	N/A	N/A	N/A	✓

Service Delivery						
<p>If partner maintains current registration to ISO 20000, these requirements do not apply, except for the Metrics requirements, which must be met for all programs, and POS Data Reporting, which must be met for Managed Services certification.</p> <p>If partner maintains current registration to ISO 27001, the requirements for Security Management do not apply.</p> <p>Certification must be valid for at least one year from the date of Cisco's on-site audit.</p>						
Requirement	Description	Gold	Silver	Master UC	Master Security	Managed Services (MSCP)
Service Level Management	Evidence of performance monitoring and reporting (*CSSP only)	✓*	✓*	✓	✓	✓
Security Management	Evidence of security policies and processes	N/A	N/A	✓	N/A	✓
Service Continuity/ Disaster Recovery	Evidence of processes for disaster recovery in order to ensure continuity of service	N/A	N/A	N/A	N/A	✓
Point of Sale (POS) Data Reporting	Evidence that POS data is reported and matches customer order	N/A	N/A	N/A	N/A	✓
Metrics	Targets and metrics for monitoring performance	✓	✓	✓	✓	✓

Direct competitors of Cisco Systems will not be granted Specialized or Certified Partner status pursuant to the World Wide Channel Partner Program. Direct competitors may participate as registered partners. Any entity that is owned or controlled by a competitor may not participate as Specialized or Certified Partners. Ownership or control is defined as 51% or more.

Detailed Program Requirements

Prequalification Requirements

Agreements/Contracts
Gold
<p>Direct partners must have a valid resale support agreement with Cisco, including Cisco Branded Resale, Cisco Collaborative Services, Cisco Shared Support Program or SIS. The support agreement must be accompanied by a valid Cisco product purchasing agreement.</p> <p>In the Europe and Emerging Market regions (except LatAm), indirect partners must have either a Reseller Support Agreement or be registered in the Enhanced Cisco Packaged Services Program, or in the Pay For Performance program. In all other geographic regions, indirect partners are required to offer Cisco Packaged Services to customers wishing to purchase service and support.</p> <p>Partners who transition from one type of support contract or agreement to another during the certification term should contact their Channel Certification Manager (CCM) to understand the impact on certification requirements.</p> <p>For direct partners, lack of a valid support agreement may result in immediate de-certification. This also applies to indirect partners in the Europe and Emerging Market regions (except LatAm).</p> <p>For partners that have both Cisco Shared Support Program/Cisco Collaborative Services and Cisco Branded Resale agreements, the Cisco Shared Support Program performance metrics will be used for certification purposes.</p>
Silver
Same as Gold
Master UC
Partner must have a direct contract with Cisco.
Master Security
Same as Master UC
Managed Services
Partner must have a fully executed Systems Integrator Agreement (or equivalent) or Indirect Channel Partner Agreement with Cisco.
Specializations
Gold
Partner must have all four of the following specializations: Advanced Routing and Switching, Advanced Security, Advanced Unified Communications and Advanced Wireless LAN.
Silver
<p>Option 1:</p> <ul style="list-style-type: none"> ▪ Any two of the following Advanced specializations: Advanced Routing & Switching, Advanced Security, Advanced Unified Communications, and Advanced WLAN <p>Option 2:</p> <ul style="list-style-type: none"> ▪ Express Unified Communications plus one of the above listed Advanced specializations, excluding the Advanced Unified Communications specialization
Master UC
Partner must have Advanced UC Specialization
Master Security
Partner must have Advanced Security Specialization
Managed Services
N/A

Personnel
General Note: All Cisco certified personnel requirements must be satisfied by a unique full-time, regular employee <i>residing in the country where certification/specialization is sought</i> and in good standing with Cisco. The only exception to this is for CCIEs. Partners may employ full-time contracted employees (not to exceed 50 percent of the required number of CCIEs) to fulfill the CCIE certified personnel requirements. Persons who are certified at a higher level and not counted toward any part of the requirements may be used to meet lower-level certified personnel requirements within a given specialization (network/ internetworking or design). To fulfill the sales expert (CSE) requirement, the extra personnel must pass the sales expert exam. A CCIE utilized from a CSC cannot fulfill roles in specializations. All specializations roles must be filled in the country where certification/specialization is sought.
Gold
Partner must have a minimum of 12 unique full-time employees, including minimum 4 CCIEs and up to 4 Cisco Sales Experts (CSEs). Individuals may also be allocated to specialization roles within program allowances if qualified to fill them; see http://www.cisco.com/web/partners/pr11/pr8/pr27/partners_pgm_requirements.html#certified
Silver
Partner must have a minimum of 6 unique full-time employees, including minimum 2 CCIEs and up to 2 Cisco Sales Experts (CSEs). Individuals may also be allocated to specialization roles within program allowances if qualified to fill them; see http://www.cisco.com/web/partners/pr11/pr8/pr64/partners_pgm_requirement_summary.html
Master UC
Partner must have personnel to satisfy the roles for Advanced UC, plus: <ul style="list-style-type: none"> ▪ 1 CCIE Voice ▪ 1 PMP/Prince II
Master Security
Partner must have personnel to satisfy the roles for Advanced Security, plus: <ul style="list-style-type: none"> ▪ 1 CCIE Security ▪ 1 PMP/Prince II and 1 of the following third-party industry certifications: <ul style="list-style-type: none"> ▪ GCIH (GIAC) ▪ GSNA (GIAC) ▪ CISM (ISACA) ▪ CISA (ISACA) ▪ GCSC (GIAC) ▪ GSLC (GIAC) ▪ GCIA (GIAC) ▪ GCFA (GIAC) ▪ GSEC (GIAC) ▪ GCFW (GIAC)
Managed Services
Partner must have <ul style="list-style-type: none"> ▪ Qualified personnel for network design and security, as evidenced by the partner's documented description of staff qualifications ▪ Field personnel with the required field expertise (including backup), available in each region in which the service is supported. Field expertise must include on-site support when required to resolve issues, including on-site assistance to implement and evolve the service. ▪ NOC staff, including the appropriate skilled staff (either in-house or out-tasked), to ensure that NOC service is available 24x7x365

Cisco Authorized Technology Provider (ATP) Program

Gold
N/A
Silver
N/A
Master UC
Partner must be in the ATP Unified Contact Center Enterprise or Cisco Rich Media Communications program.
If you are not currently a qualified ATP-UCCE or ATP-RMC partner, please contact your Cisco Sponsor to determine your eligibility for being invited into one of these two ATP programs, which have their own set of stringent acceptance requirements.
Master Security
N/A
Managed Services
N/A

Network Operations Center (NOC)
Gold
N/A
Silver
N/A
Master UC
N/A
Master Security
N/A
Managed Services
Partner must have their own Network Operations Center (NOC) through which Managed Services are provided to a minimum of 10 end users.
<ul style="list-style-type: none"> ▪ Partner may outsource elements of their network operations to third parties, provided they meet the requirements outlined at http://www.cisco.com/go/mscp ▪ The Network Operations Center (NOC) must operate on a 24x7x365 schedule. The NOC must follow operations and service delivery methodologies based upon accepted international industry standards such as ISO/IEC 20000 which reflects best practice guidance contained within the Information Technology Infrastructure Library (ITIL) Framework, and other IT Service Management frameworks. ▪ Network operations must have access to and be supported by laboratory facilities for equipment homologation, technical support personnel training, problem simulation and resolution ▪ Partner must demonstrate how all network events are synchronized and time-stamped to ensure accurate measurement of network events.

Support Lab
Gold (CSSP/Collaborative Services only)
Partners with a Cisco Collaborative Services, Shared Support Program, Reseller Support or SIS agreement must have a support lab in the country seeking certification.
<ul style="list-style-type: none"> ▪ The lab equipment must be set up in a network topology, and must be used for proof of concept, post-sales support and training. It may also be used for pre-sales demonstrations. ▪ Remote access to the lab, or a process for troubleshooting, must be available and will be verified at the time of the audit. ▪ The lab equipment is not to be used for demonstration or evaluation on customer premises. ▪ Evidence of a process, procedure or guideline for using the lab must be shown at the time of the audit. ▪ Leased equipment may be used toward the lab and must be present at the time of the audit. ▪ Lab equipment must be sourced from either Cisco direct, or from an authorized Cisco source. ▪ Not for Resale (NFR) equipment must be present at the time of the audit. The Program

Manager will provide the auditor with the NFR list in advance of the audit.

- Partner must ensure that lab is in compliance with the program requirements during the time period between audits. Cisco reserves the right to visit the lab at any given time between the audits.

Does not apply to Cisco Branded Resale or Packaged Services partners.

Silver

Same as Gold

Master UC

Same as Gold, plus

- Must be accomplished with internal infrastructure; may not be outsourced

Master Security

Same as Gold, plus

- Must be accomplished with internal infrastructure; may not be outsourced

Managed Services

Same as Gold, plus

- Must be accomplished with internal infrastructure; may not be outsourced

Customer Satisfaction

Gold

Partner must actively participate in the Cisco partner customer satisfaction survey.

- Partner must use the Cisco Partner Access onLine (PAL) customer satisfaction tool on a regular basis (at least quarterly) to send surveys to current customers (within the past 12-24 months) and assess and act upon customer satisfaction results. The PAL tool can be found at <http://www.cisco.com/go/pal/>
- Partner must meet valid response targets based on new certification or recertification. A “valid response” directly correlates to a unique individual’s reply to the survey sent. A respondent reply is counted once, whether they answer only pre-sales questions, only post-sales questions, or both pre-sales and post-sales questions. Total valid responses from all sources can be from a combination of customer invitations provided by the partner (“Total Valid Responses from Surveys You Have Sent”) and/or Cisco high-touch sales representatives (“Total Valid Responses from Surveys Sent by Other Sources”).
- Evidence of results analysis and reinforcement of best practices for customer satisfaction must be captured by the partner, including evidence of a closed loop process for addressing customer issues raised in customer satisfaction surveys. Analysis must include review of the loyalty segmentation and pre- and post-sales Excel spreadsheets.

For new certification audits the following requirements apply:

- A minimum of 15 total valid responses from all sources in each country or country group where the partner is seeking certification. If the number of valid responses is less than 15, an onsite audit will be delayed until the requirement is achieved.
- New partners must achieve at least 95 percent of the theater CSAT target to qualify for certification.
- The definition of a “new” partner as it relates to the enforcement of the CSAT requirement is a partner that has not been certified at any level within the previous six months.
- Silver partners moving to Gold certification must have 30 valid responses.
- Premier partners moving to either Silver or Gold certification must have a minimum of 15 valid responses and meet the theater customer satisfaction target.
- If a partner falls out of compliance with the program requirements and is de-certified within six months of submitting a new certification application, they will be treated as a re-certifying partner and will be responsible for meeting the CSAT requirements.
- Measurement will be based upon results within the preceding 12 months from the anniversary date.

For re-certification audits, the following requirements apply:

- To ensure a reasonable and statistically significant measurement, a minimum of 30 total valid responses is required from all sources in each country or country group where the partner is seeking re-certification.

<ul style="list-style-type: none"> Partner must achieve the theater CSAT target to qualify for re-certification. Measurement is based on results from the prior 12 month period from the anniversary date. If partner meets the 30 required valid responses but the PAL CSAT score fails to meet the theater objective, partner must provide a get-well plan detailing action and timelines that will ensure that the partner will achieve the CSAT requirement within the subsequent six months. Failure to meet the 30 valid responses will be considered lack of participation and is grounds for de-certification. In this case, the partner may not be eligible to participate in a get-well plan (based upon the discretion of the Cisco Certification Manager). Failure to achieve the commitments stated within the get-well plan will result in decertification.
Silver
Same as Gold
Master UC
N/A
Master Security
N/A
Managed Services
N/A

Service Offerings
Gold
N/A
Silver
N/A
Master UC
<p>Partner must provide Service Descriptions, Service Level Agreements (SLAs) and contractual descriptions of operating procedures for the services provided.</p> <ul style="list-style-type: none"> Service Descriptions must be customer-facing. The range of devices (e.g. CallManager, Unity, Routers, Switches, etc) covered under the offer must be sufficient to fulfill the deliverables and service described in the Service Descriptions and the obligations in the SLA. Comprehensive monitoring policies must be applied to the devices to fulfill the obligations under the Service Descriptions and SLAs. Clear delineation must be made in the documents between the responsibilities and obligations of the partner, the customer and any third parties.
Master Security
<p>Partner must provide Service Descriptions, Service Level Agreements (SLAs) and contractual descriptions of operating procedures for the services provided.</p> <ul style="list-style-type: none"> Service Descriptions must be customer-facing. The range of devices (e.g. Cisco Security Agent [CSA], Cisco Security Monitoring, Analysis and Response System [CS-MARS]) covered under the offer must be sufficient to fulfill the deliverables and service described in the Service Descriptions and the obligations in the SLA. Comprehensive monitoring policies must be applied to the devices to fulfill the obligations under the Service Descriptions and SLAs. Clear delineation must be made in the documents between the responsibilities and obligations of the Operate Service Provider, the Customer and any third parties.
Managed Services
<p>Partner must submit a nominated list of all Managed Services within the partner's Cisco offer portfolio via the program application. This list must include the Managed Service name and applicable MSCP service category. For each service, Cisco requires a complete list of the countries where that service is offered to customers. Managed Service literature (marketing and technical descriptions) should be uploaded into the application tool in PDF or Microsoft Word format. See http://www.cisco.com/go/mscp for offer portfolio.</p>

Customer Reference Accounts
Gold

N/A
Silver
N/A
Master UC
<p>Prior to the audit being scheduled, the partner must submit documentation for five reference accounts demonstrating complex deployments including 3rd party integration. Each submission must contain the following:</p> <ul style="list-style-type: none"> Customer Reference Validation Cover Sheet and Checklist: http://www.cisco.com/web/partners/program/specializations/ucom/master/requirements.html Copy of customer acceptance documentation <p>Partner should work with the Cisco Systems Engineer (SE) to collect and submit these documents into the CSApp tool. The SE must verify the Customer Reference documentation prior to uploading into CSApp.</p> <p>Partner may use the same Customer Reference account for re-qualification if there is a new sale within that account that meets the current criteria.</p>
Master Security
<p>Same as Master UC, except:</p> <ul style="list-style-type: none"> Partner may use same customers for Vulnerability Assessment and Customer Reference Accounts Customer Reference Validation Cover Sheet and Checklist can be found at: http://www.cisco.com/web/partners/program/specializations/security/master/requirements.html
Managed Services
N/A
Vulnerability Assessment
Gold
N/A
Silver
N/A
Master UC
N/A
Master Security
<p>Partner must upload a template for completing a Vulnerability Assessment; the template must meet the requirements as listed at http://www.cisco.com/web/partners/program/specializations/security/master/requirements.html</p> <p>Partner must present evidence at the on-site audit of three completed Vulnerability Assessments. These customers may be from among the five deployment customer reference accounts or they may be different customers. Evidence of a completed Vulnerability Assessment must include all requirements as listed in the Vulnerability Assessment Checklist at the above link.</p>
Managed Services
N/A
Service Attach Rate
Gold (CBR/Packaged Services only)
<p>Cisco Branded Resale and Packaged Services partners are required to have a minimum service attach rate of 40 percent during the prior four Cisco quarters. For partners who have not previously been Gold or Silver certified, the Service Attach Rate requirement may be met by achieving a rate of 40 percent within the past 12 months.</p> <p>The Service Attach Rate is calculated as follows:</p>

Attach Rate % =	Total \$ value of service sold (attached) in the measurement period*	x 100
	Total \$ value opportunity of service sales in the measurement period**	

* Numerator: Service dollars attached	Service coverage attached in the current measurement period. Service coverage dollars are translated to SMARTnet NBD U.S. list price
** Denominator: Service dollar attach opportunity	Service coverage dollars available for attach in the current measurement period. Service coverage dollars are translated to SMARTnet NBD U.S. list price

More information on the Service Attach Rate definition and calculation can be found at <http://tools.cisco.com/CustAdv/PP/smHelp.do?programNameCd=P4P#IAR>

The following requirements apply to the Service Attach Rate:

- RMAs and spares are not included in this measurement.
- For partners that do not have a direct purchasing agreement with Cisco, the partner will be asked to demonstrate that they have achieved a 40 percent service attach rate during the prior four quarters. The attach rate for indirect partners may be evaluated based on Cisco distributor point of sales reports, when available.
- In the Europe and Emerging Market regions (except LatAm), partners that do not have a direct purchasing agreement with Cisco must be registered within the Cisco Enhanced Packaged Services Program and achieve the Level 1 Service Performance metrics during the prior four quarters.
- Direct service attach rate performance data can be found using the PMC tool within the metrics area at: <http://tools.cisco.com/CustAdv/PP/smIntroduction.do>

Does not apply to Cisco Collaborative Services, Shared Support Program, Reseller Support or SIS partners.

Silver
Same as Gold
Master UC
N/A
Master Security
N/A
Managed Services
N/A

Revenue from Services
Gold (CBR/Packaged Services only)

Cisco Branded Resale and Packaged Services partners must generate at least 15 percent of revenue from services during the prior two quarters, including the resale of Cisco branded services. For example:

- Total product revenue (from the networking products division) for the past two quarters
- Total services revenue (from all services sold, including Cisco SMARTnet® and professional services).

The Revenue from Services rate is calculated as follows:

Revenue from Services % =	Total revenue of service sold(Managed, Professional Service, & SMARTnet	x 100	= 15%
	Total product revenue of the networking division		

Revenue from Services must meet the following requirements:

- The percentage of revenue from all services against the product revenue must be at least 15 percent.
- Partner must provide documented evidence that they have met or exceeded this requirement.
- Measurement must be specific to the division engaged in providing networking services or solutions in the country applying for certification.

Does not apply to Cisco Collaborative Services, Shared Support Program, Reseller Support or SIS partners.

Silver
Same as Gold
Master UC
N/A
Master Security
N/A
Managed Services
N/A

Core Requirements: Pre-Sales/Plan, Design and Implement

Demonstration
Gold
<p>Partner must select and perform a live demonstration of a solution based on a Cisco technology. This demonstration will display the partner's ability to demonstrate a solution to a potential customer. Partners cannot present the same demonstration two years in a row.</p> <p>If the lab equipment is at a different location, adequate access to perform a credible demonstration must be shown.</p> <p>At the time of the audit, the auditor will validate the partner's demonstration process, including:</p> <ul style="list-style-type: none"> ▪ Demonstration facility and equipment quality ▪ Demonstration equipment present at time of audit ▪ Assurance that the demo equipment is sufficient for the partner to effectively demonstrate Cisco solutions ▪ Process to reserve a demonstration room and specific technology ▪ Assignment of pre-sales technical staff <p>The recommended method for demonstrating a technology or a solution is to create a customer scenario situation in a presentation format. In this scenario, the auditor is a customer who wants to understand the value of buying this solution from this partner.</p>
Silver
Same as Gold
Master UC
<p>Same as Gold, but must use provided UC customer scenario and must meet pre-defined demonstration criteria; Master UC demo will be evaluated and scored as described in the Master UC Demo Checklist:</p> <p>http://www.cisco.com/web/partners/downloads/partner/WWChannels/technology/ipc/master_uc_demo_checklist.pdf</p>
Master Security
<p>Same as Gold, but must use provided Security customer scenario and must meet pre-defined demonstration criteria; Master Security demo will be evaluated and scored as described Master Security Demo Checklist:</p> <p>http://www.cisco.com/web/partners/downloads/partner/WWChannels/technology/security/master_demo_checklist_security.pdf</p>
Managed Services
N/A
Project Management
Gold
<p>Partner must provide evidence of the following:</p> <ul style="list-style-type: none"> ▪ Customer Communication Plan: Methodology for notifying customer of any changes during the project ▪ Site Survey: Methodology to assess customer facilities, data infrastructure and applications ▪ Network Readiness Assessment Plan <p>Partner must provide evidence of the following as it relates to conducting on-site service:</p> <ul style="list-style-type: none"> ▪ Statement of Work: Methodology articulating what is to be accomplished, each party's responsibilities, assumptions each party is working under and what constitutes a successful engagement ▪ Site Survey: Methodology to assess customer facilities, data infrastructure and data applications ▪ Network Readiness Assessment Plan: Methodology to assess the existing network architecture ▪ Security Policies and Procedures: Methodology to assess the customer's security policies and

<p>procedures</p> <ul style="list-style-type: none"> Security Readiness Assessment: Process and methodology to evaluate the customer's existing network for security readiness, including assessment of software operation procedures and security management procedures <p>The audit will also include the following:</p> <ul style="list-style-type: none"> Review of selected Project(s) related to a Cisco Advanced Technology: e.g., Advanced UC or Advanced Security or Advanced Wireless or Advanced Routing and Switching or a combination of these technologies SOW: Two SOWs to be shown Project Schedule Project Organization Skills Level Required Customer Communication Plan Site Survey Project Profitability Process Security Policies and Procedures Security Readiness Assessment Project Closure/Completion, including User Acceptance Test End Customer Training Process Project's Customer Satisfaction/Feedback Post-Project Review and Lessons Learned: Records of a post-project review and documentation of lessons learned to be shown.
Silver
Same as Gold, except:
<ul style="list-style-type: none"> Security Readiness Assessment not required
Master UC
N/A
Master Security
N/A
Managed Services
N/A

Capacity Planning
Gold
N/A
Silver
N/A
Master UC
<p>Partner must maintain a documented process for monitoring and reporting the availability, capacity and performance of internal monitoring, tracking and notification systems.</p> <ul style="list-style-type: none"> End-to-end availability of all systems impacting customer monitoring, tracking and notifications must be tracked and reported internally. Records must demonstrate that system availability is tracked and reported. Internal systems must be managed by a documented change control process. Resource capacity must be documented and reviewed monthly to determine whether appropriate capacity is available to support forecasted increases in managed devices. Records of monthly reviews must be maintained. System performance records must include uptime, unscheduled outages and scheduled outages, and must be maintained for at least 12 months.
Master Security
Same as Master UC
Managed Services
Partner must demonstrate that a process is in place to understand the business level requirements of the customer that may affect service requirements. Evidence of business capacity planning must

be maintained, including reports.

Partner must demonstrate the ability to monitor service performance trends to ensure that SLAs can continue to be met as service needs increase. Evidence of service capacity planning must be maintained, including reports.

Partner must demonstrate the ability to track performance trends of the internal network infrastructure that may affect service delivery. Evidence of network infrastructure capacity planning must be maintained, including reports.

Design
Gold
Partner must provide evidence of a process to build a network design for a prospect and to perform a design review. Partner must provide two Statements of Work (SOW) at the time of the audit.
Silver
Same as Gold
Master UC
Same as Gold
Master Security
Same as Gold
Managed Services
Same as Gold

Quality Assurance
Gold
Partner must provide evidence of a process to ensure project success with respect to profitability and customer satisfaction, including acceptance testing procedures to assess the overall functionality of the network and to ensure network is ready to hand off to an operational service.
Silver
Same as Gold
Master UC
N/A
Master Security
N/A
Managed Services
N/A

Hiring and Training
Gold
Partner must provide evidence of a hiring and training program, including training plans defining the required competencies and skill levels for all personnel. Training plans must address: <ul style="list-style-type: none"> ▪ New hire training requirements ▪ Ongoing training and sharing of best practices ▪ Training for sales and technical personnel on new products, protocols and features ▪ Solution selling to business decision makers ▪ Hiring and retention of Cisco Certified personnel <p>Partner must also provide evidence of a customer training process.</p> <p>Records of internal and customer training must be maintained.</p>
Silver
Same as Gold

Master UC
Same as Gold
Master Security
Same as Gold
Managed Services
Same as Gold

Core Requirements: Service Support

Incident Management
Gold
<p>Cisco Collaborative Services, Shared Support Program, Reseller Support or SIS partners must provide 24x7 Customer Service (over Internet-based systems, phone, fax, page or email). The partner's customer service number must be an in-country number (preferably toll-free) responded to in the local language.</p> <p>Partner's Call/Contact Center must meet the following requirements:</p> <ul style="list-style-type: none">▪ The support organization must employ a duty manager.▪ For support calls, problem severity and priority are to be established by the customer.▪ After hours support must be provided. If the partner does not maintain a staffed call center on a 24-hour basis, there must be documented procedures for after-hours and holiday support. If the support telephone number for after-hours support is different from the number used during normal hours, the partner must detail how customers are provided the after-hours support number. Support engineers are required to have write access to the call-tracking system to log the after-hours calls.▪ All calls must be logged immediately after the initial communication with the customer. <p>Partner must have a computer-based call tracking (case management) system that meets the following requirements:</p> <ul style="list-style-type: none">▪ Partner engineers must be able to communicate with the partner's call tracking system from all locations, including customer premises, either by an Internet connection or dialup modem connection.▪ Support engineers must have write access to the call tracking system to log after-hours calls, or there must be a process to provide input to the call tracking system. All calls must be logged immediately after the initial communication with the customer. <p>Details on the call-tracking system can be found on the Certification Audit Documents web page.</p> <p>Partner must make contact in the local language with the customer within one hour of receiving an e-mail, voicemail, fax, page or Internet-based notification of an issue. The call-back must be from a technical support engineer and not a non-technical resource.</p> <p>The above requirements for Call/Contact Center and Case Management do not apply to Cisco Branded Resale and Package Service partners.</p> <p>All partners must provide evidence of a documented and robust incident escalation process that escalates incidents through the partner management structure and, when necessary, to Cisco.</p> <p>The following criteria must be addressed by the partner's escalation procedures:</p> <ul style="list-style-type: none">▪ Definition of customer calls by priority▪ Timeframe for each level of escalation by priority▪ Timeframe for escalation to Cisco by priority (if necessary)▪ Process for escalation of incidents within the partner▪ Process for the escalation of incidents by the partner to Cisco (if necessary) <p>A recommended set of prioritization standards has been established to ensure that appropriate service levels are provided to customers based on incident severity; see the Certification Audit Documents web page.</p> <p>Escalation process must include automated alerts.</p> <p>Partners with CSSP agreements must provide four cases (two of which are escalated to Cisco, and two of which are resolved by the partner) at time of audit. CBR partners must provide three cases</p>

for review, if such cases exist.

Some activities related to Incident Management may be outsourced; see [Outsourcing Policy](#).

Silver

Same as Gold, except:

- Service must be available 8x5 (no after hours support is required)
- Escalation alerts may be manual.
- Incoming calls are not required to be logged immediately after customer communication.

Master UC

Same as Gold, plus:

Partner must maintain a documented process for pro-active monitoring, tracking and notification of system fault and performance data.

- System must poll for core monitoring data within a range of less than five minutes.
- Declared incidents must be accessible to customers on a real-time basis.
- Fault and performance data must be stored and be accessible online for a period of at least 12 months.
- Notification processes must allow customers to select notification by at least two methods; these must include email and phone notification. Customers must be able to establish their own notification preferences. Records of customer notification preference must be maintained.

Partner must report fault and performance data internally and to customers.

- Real-time fault reporting must be available to customers, including the ability to track the progress of ongoing faults and review details of recent faults online.
- Historical queries must be available for a period of not less than six months.
- Performance reports must be available on a monthly or more frequent basis, and must include basic performance statistics including but not limited to interface utilization, CPU utilization and interface errors.

Partner must maintain a documented process for detecting, recording, logging, prioritizing, isolating, diagnosing and resolving incidents that are system generated or as a result of a customer call.

- Incidents for managed events must be detected within five minutes.
- All detected incidents must be recorded and logged such that they can be queried for a period of up to 90 days.
- For automatically generated incident tickets, partner must demonstrate the ability to notify customers via their preferred notification method in not more than 15 minutes (see Metrics).
- Methods must be established for troubleshooting and isolating of incidents; a log showing isolation status must be maintained.
- Documented procedures must be maintained for resolution of known errors, and for engaging Problem Management in troubleshooting of unknown errors.

A periodic review of customer feedback must be conducted to determine whether incidents are escalated according to the documented process. A documented closed loop corrective action process must be in place and must be initiated when discrepancies are found; records of such actions must be maintained.

Partner must maintain a documented process for updating stakeholder groups on status of existing and open incidents.

- The frequency with which stakeholders are updated on the status must be determined and documented, and must be based on severity, business impact and/or SLA.
- Methods must be established for stakeholders to provide input on existing and open incidents, and for Incident Management personnel to review and respond to stakeholder input. The frequency for responding to stakeholder input must be determined and documented, and must be based on severity, business impact and/or SLA.

Partner must maintain a documented process for incident closure.

- Authorities for incident closure must be defined, documented and communicated.
- A summary of the incident and details of incident resolution must be generated at the time of incident closure, as well as categorization of the incident based on pre-defined categories.

Partner must maintain tools for fault and performance monitoring that are capable of retrieving fault and performance data from applications and infrastructure.

- Tools must be of a highly available design and must feed into the call tracking/case management system.
- Documented instructions or other information describing how to use the tools must be maintained.
- Users must demonstrate knowledge and awareness of the tools and their capabilities

Partner must ensure that tools used allow for correlation of technology domains; that is, the tools must include features that correlate faults according to root cause and allow for root cause analysis.

All activities must be accomplished with internal infrastructure; may not be outsourced.

Master Security

Same as Master UC, except

- Notification for automatically generated incident tickets must take place in no less than 60 minutes (see also [Metrics](#))

Managed Services

Same as Master UC, plus:

- Procedures for trouble ticketing (incident handling) must account for the use of third parties and/or field operations.
- The Network Operations Center must be able to correlate problems from all countries for which the customer locations are supported.

Problem Management

Gold (CSP/Collaborative Services only)

Cisco Collaborative Services, Shared Support Program, Reseller Support or SIS partners must maintain a documented process for handling problems, including incidents for which there is no known solution (handed off from Incident Management), and proactively identified incident patterns (e.g., multiple incidents on the same device within a time period).

- Root cause must be identified, validated and documented, and stored in a knowledge base of known errors.
- Guidelines must be established for when to provide root cause analysis results to stakeholders; a template must be provided for documenting and communicating root cause analysis results.
- Records of closed loop corrective action must be maintained for all problems, including recommendation to stakeholders of appropriate problem remediation steps. Open corrective actions must be reported on an on-demand basis.

Partner must maintain a searchable knowledge database of known errors.

- Knowledge base must be widely used within Incident and Problem Management.
- All articles in the knowledge base must have a documented review process, including an assigned Subject Matter Expert (SME).
- All articles in the knowledge base must be reviewed and re-approved at least once per year; any article not reviewed and approved once per year must be automatically removed or marked in the database as "out of date."
- Documented instructions or other information describing how to use the knowledge base must be maintained, including procedures for adding, removing and modifying articles.
- Users must demonstrate knowledge and awareness of the knowledge base and its capabilities; records of user training must be maintained.

Partner must maintain a documented process for identification and remediation of recurring problems.

<ul style="list-style-type: none"> Records must provide evidence of trend analysis and initiation of preventive actions as appropriate to resolve recurring problems. Preventive actions must include development of remediation procedures and follow up to monitor the effectiveness of actions taken. <p>Partner must maintain a documented process for creating change requests and referring requests to Change Management. Process must include detailed instructions for when and how to hand off requests for change (RFC), including handling emergency requests for change.</p> <p>Partner must demonstrate that tools used to identify problem signatures are capable of correctly identifying problems. Documented instructions or other information describing how to use the tools must be maintained. Users must demonstrate knowledge and awareness of the tools and their capabilities.</p> <p>Does not apply to Cisco Branded Resale or Packaged Services partners.</p> <p>Some activities related to Problem Management may be outsourced; see Outsourcing Policy.</p>
Silver
Same as Gold
Master UC
Same as Gold, except <ul style="list-style-type: none"> All activities must be accomplished with internal infrastructure; may not be outsourced.
Master Security
Same as Master UC
Managed Services
Same as Gold

Configuration Management
Gold
N/A
Silver
N/A
Master UC
<p>Partner must maintain a documented process for managing and controlling configurations.</p> <ul style="list-style-type: none"> Configuration Items (CIs) to support specific managed services must be defined. Methods for recording and maintaining configuration information must be established. <p>Partner must maintain a documented process for managing transitions to customer environments and for boarding of new customers.</p> <ul style="list-style-type: none"> A data collection tool must be maintained for capturing the critical Configuration Items for transitioning a new customer. Roles of on-site versus offsite resources and personnel must be defined for collecting configuration information for new customer deployments. <p>Partner must maintain a documented process for planning and documenting configuration changes within the Configuration Management system.</p> <ul style="list-style-type: none"> Methods for assigning Configuration Item stakeholders and their role in updating Configuration Item information must be defined. Configuration Item lifecycle stages and status codes assigned to each stage must be defined. Configuration baselines must be established and documented to accurately capture the structure and detail of the product or system prior to a change being made. Methods must be defined for distinguishing between types of physical and logical relationships and for ensuring that relationships are maintained when changes are made. Documented configuration change plans must be maintained. <p>Partner must maintain a Configuration Management Database (CMDB) that provides for effective</p>

<p>management of configurations.</p> <ul style="list-style-type: none"> ▪ The scope and architecture of the CMDB must be defined, including how data entities and their relationships are modeled, and what documentation is included in the CMDB. ▪ Methods must be defined for how relationships are maintained between Configuration Items and request for change (RFC) numbers, change numbers, problem numbers and incident numbers. ▪ Documented instructions or other information describing how to use the CMDB must be maintained, including procedures for populating and maintaining the database. ▪ Users must demonstrate knowledge and awareness of the CMDB and its capabilities; records of user training must be maintained. <p>Partner must maintain a documented process for conducting audits of the CMDB to identify any discrepancies between “as discovered” and “as expected” configurations.</p> <ul style="list-style-type: none"> ▪ Specific audit tools must be used to analyze Configuration Items and report on discrepancies; this must include the use of configuration baselines to detect discrepancies. ▪ Situations under which audits are routinely conducted must be defined. ▪ Any discrepancies found in audits must be corrected using the Change Management process; methods for requesting such changes must be defined.
Master Security
Same as Master UC
Managed Services
Same as Master UC

Change Management and Release Management
Gold
N/A
Silver
N/A
Master UC
<p>Partner must maintain a documented process for managing changes, including methods for assessing, planning and approving Requests for Changes (RFCs).</p> <ul style="list-style-type: none"> ▪ Process must address Move, Add, Change, Deletes (MACDs). ▪ Partner must demonstrate how Change Manager and Change Advisory Boards are used to manage changes, including how routine activities are analyzed and assessed before they are treated as standard changes. ▪ Definitions for standard and non-standard changes must be established. ▪ Completed scheduled changes must be updated in the CMDB. <p>Partner must maintain a documented process for maintaining traceability for all changes related to additions, modifications or deletions of any software or hardware, including version and release control.</p> <ul style="list-style-type: none"> ▪ RFC creation must include recording of identification number, association to problem or known error, description of relevant Configuration Items, change justification, Configuration Item versions to be changed, RFC submitter and contact information. ▪ Change records must be updated after the change is executed. <p>Partner must maintain a documented process for controlling software patches and system upgrades.</p> <ul style="list-style-type: none"> ▪ Process must define how software patch and system upgrades are requested by the RFC process, how they are categorized as either major or minor releases, and what types of development, test and production environments are used to execute the release of software. ▪ A Definitive Software Library (DSL) must be maintained, including archived versions. ▪ Releases of software patches and system upgrades must be updated in the CMDB. <p>Partner must maintain a documented process for accommodating customers’ unique change control processes.</p>

- Unique customer requirements must be documented in a Change Control Profile, including specific procedures to be followed, maintenance windows, emergency contact and notification information, information about customer specific change procedures and advisory board roles, agreements on what constitutes standard versus non-standard changes and policies and procedures for how emergency changes are to be handled.
- Personnel must be aware of how to access and use customer Change Control Profile information.

Partner must maintain a documented process for managing software and hardware releases.

- Process must include identification of Configuration Items affected by the release, how multiple releases may be consolidated into a single release (if appropriate) and creation and approval of plan, build, release and rollback documents.
- Process must define how releases are developed, tested, accepted and installed in a production environment.
- Software and hardware must be kept in repositories, e.g., Definitive Software Library (DSL) and Definitive Hardware Store (DHS).
- Results of the release process must be updated in the CMDB.
- Audits must be conducted to determine whether releases have followed Release Management processes. A documented closed loop corrective action process must be in place and must be initiated when discrepancies are found; records of such actions must be maintained.

Partner must maintain tools for managing changes and releases. These tools may include either commercial off-the-shelf software or custom developed tools and/or scripts that automate portions of the process.

- Methods for using Change Management and Release Management tools to verify installation and deployment must be defined.
- Documented instructions or other information describing how to use the tools must be maintained.
- Users must demonstrate knowledge and awareness of the tools and their capabilities.

Master Security

Same as Master UC

Managed Services

Same as Master UC

On-Site Response/Troubleshooting

Gold (CSSP/Collaborative Services only)

Partners with a Cisco Collaborative Services, Shared Support Program, Reseller Support or SIS agreement are required to provide a description for on-site response, including:

- Geographic coverage
- Best service-level agreement (SLA)
- Dispatch system for on-site service, if separate from call tracking system
- Any subcontractors

For all Cisco products sold with support, the partner must provide four hour on-site response (or better) with service and spare(s) if required, from the time of receiving notification that on-site troubleshooting is required.

Some activities related to On-Site Troubleshooting may be outsourced; see [Outsourcing Policy](#).

Does not apply to Cisco Branded Resale or Packaged Services partners.

Silver

Same as Gold, except:

- Partner must be able to provide on-site troubleshooting within 24 hours (or better) with service and spare(s) if required, from the time of receiving notification that on-site troubleshooting is required.

Master UC

Same as Gold, plus:
<ul style="list-style-type: none"> ▪ Partner must maintain a documented process for on-site troubleshooting, including how on-site troubleshooting is requested, dispatched, tracked and closed. ▪ All activities must be accomplished with internal infrastructure; may not be outsourced.
Master Security
Same as Master UC
Managed Services
Same as Gold

Remote Troubleshooting Access
Gold
N/A
Silver
N/A
Master UC
N/A
Master Security
N/A
Managed Services
Partner must demonstrate remote access to the customer network by either in-band or out-of-band management, or by a combination of both. Partner must be able to demonstrate the ability to support either chosen connectivity option (in-band or out-of-band).

Core Requirements: Service Delivery

Service Level Management
Gold (CSSP/Collaborative Services only)
Partners with a Cisco Collaborative Services, Shared Support Program, Reseller Support or SIS agreement must provide Service Level Agreements (SLA) to customers. Does not apply to Cisco Branded Resale or Packaged Services partners.
Silver
Same as Gold
Master UC
Partner must maintain a documented process for offering and providing managed services to its customers. <ul style="list-style-type: none">Service Catalog must include Service Level Agreement (SLA), Operational Level Agreement (OLA) and Underpinning Contract (UC) specifics and must be owned by the Product Management function.Process must include ownership, alignment and, if necessary, re-negotiation of SLAs, OLAs and UCs with customers, partners and vendors that are tied to all managed service offerings. Partner must maintain a documented process for monitoring and reporting of service level performance metrics. <ul style="list-style-type: none">A recurring internal management review (weekly or monthly) must be conducted to review metrics related to the ability of the organization to deliver the managed services. Review must include data directly related to specific SLAs, OLAs and UCs under contract for customers, partners and vendors tied to all managed services offered.A recurring service review must be conducted to provide service level metrics to end-customers and/or partners to illustrate the value of managed services. This may be accomplished by posting selected reports to a customer portal for customer self-service, emailing reports directly to end-customers, coordinating conference calls with end-customers or a combination of these methods. Partner must provide evidence of actions taken to achieve SLA, OLA and UC commitments and to continually improve the quality of service provided. <ul style="list-style-type: none">Internal management reviews must produce actionable continual improvement activities; actions must be communicated to affected managers.Actions must be followed up to determine whether the desired results are achieved; where results are not achieved, additional action(s) must be determined.Service Level Management personnel must be responsible for communication and final issue resolution (if applicable) with the customer, partner and/or vendor. Partner must maintain a portal or similar tool to provide customers with service level metrics and information. <ul style="list-style-type: none">Portal must be accessible to customers 24x7.Reports must provide real-time and trended data, including data related to open incidents, closed incidents, faults, performance, inventory and service level performance.Portal must be able to respond to customer inquiries tied to metrics or other customer-specific data provided.
Master Security
Same as Master UC
Managed Services
Partner must demonstrate the ability to measure and report network performance as it relates to individual customers and services offered. This provides the foundation for effective monitoring of SLAs. Partner must demonstrate an effective managed spares program to maintain network performance

in order to meet stated SLA requirements, including Mean Time to Repair (MTTR).

Security Management
If partner maintains current registration to ISO 27001, the requirements for Security Management do not apply. Certification must be valid for at least one year from the date of Cisco's on-site audit.
Gold
N/A
Silver
N/A
Master UC
Partner must document and maintain policies to provide direction and support for management of information security within all service activities. <ul style="list-style-type: none">Security policies must be approved by management and communicated to all employees and relevant external parties.Security policies must be periodically reviewed for continuing suitability, adequacy and effectiveness.
Master Security
N/A
Managed Services
Partner must have a security management system that meets the following requirements; <ul style="list-style-type: none">Customer monitoring network must be physically isolated from the partner's corporate infrastructure.Partner must deploy and maintain border security, including access control lists for any border routers.Partner must demonstrate adequate intrusion detection system in place on any relevant subnets that may affect the service.Partner must demonstrate the existence of a Firewall solution to protect appropriate parts of the network.Partner must demonstrate that there are redundant databases for monitoring activities.Partner must demonstrate that procedures are in place to react to potential or detected threats to the integrity of the service. This must include procedures for reacting to security incidents, and periodic vulnerability scans to assess overall security performance.Partner must demonstrate adequate security safeguards for their operations facilities, including providing for controlled access to corporate office buildings.Partner must demonstrate that periodic system wide internal security audits are performed. Records of security audits must be maintained. A closed-loop corrective action process must be initiated for any nonconformities found during security audits.Partner must demonstrate the ability to rapidly deploy relevant security patches to systems when required.

Service Continuity/Disaster Recovery
Gold
N/A
Silver
N/A
Master UC
N/A
Master Security
N/A
Managed Services
Partner must demonstrate the availability of a redundant NOC facility or backup operations capable of seamlessly taking over in the event of a failure in the primary NOC. Partner must demonstrate design and implementation capabilities for implementing redundant servers for critical applications within the NOC.

Redundancy of operations must be available to ensure continuance of support during outages.

Partner must provide all the tools necessary for remote access and dial-in out of band management to remote sites for troubleshooting. This includes remote access to the fault call tracking system.

Point of Sale (POS) Data Reporting

Gold

N/A

Silver

N/A

Master UC

N/A

Master Security

N/A

Managed Services

Partner must report POS data on a monthly basis per the requirements outlined at <http://www.cisco.com/go/mscp>

For recertification, the auditor will randomly select an end-customer from a previously submitted POS report and request the SLA for that customer to ensure the CPE ordered matches the approved bill of materials and the customer's order.

Partner must provide documentation for 3 managed service transactions that match their POS report submitted to Cisco.

Metrics

Gold

Partner must complete customer call back within one hour of receiving customer notification of an incident

Silver

Same as Gold

Master UC

Measurable objectives must be established, documented, tracked and reviewed. Actions must be taken to continually improve performance to objectives, including closed loop corrective actions when targets are not met; records of actions taken must be maintained.

Partner must track and maintain evidence of meeting the following targets:

- Mean Time to Notify (MTTN): 15 minutes -- Measured from initial system detection of a fault to customer notification
- Mean Time to Repair (MTTR): 4 hours -- Measured from the time a support engineer is working on the problem to when it has been restored to its original condition or an adequate workaround has been put in place
- On-Site Troubleshooting Response Time: 4 hours -- Measured from the time on-site troubleshooting is determined as required to when support personnel arrive at customer site

The above metrics must be tracked for the entire population of tickets (not on a sampling of data), and must be available to stakeholders on a monthly or more frequent basis.

Partner must also establish targets and maintain metrics, including but not limited to:

- Incident volume (number of tickets per managed device)
- Customer satisfaction survey response, including a breakdown of the customer's satisfaction level with Incident Management and Change Management.
- Volume of completed scheduled changes; number of missed change deadlines
- Number of On-site Troubleshooting incidents per customer

▪ Security incident volume
Master Security
Same as Master UC, except:
▪ Mean Time to Notify (MTTN): 60 minutes
▪ No requirement for security incident volume (does not apply)
Managed Services
Based on service offering and SLA

Audit Process and Methodology

Audit Scheduling

As a general guideline, an on-site audit will not be scheduled until the partner has submitted a complete online application and the Cisco Partner Program Manager has verified that pre-audit requirements have been met.

A representative from a Cisco third-party audit agency will schedule the on-site audit and will request additional documentation or information prior to or during the audit.

Typically, the on-site audit will take place within 30 working days of Cisco's validation of the partner's pre-qualification requirements.

Role of the Partner

Prior to the audit, the partner is expected to review all of the program requirements, submit a complete online application with the requested pre-audit documents and provide any additionally required documents on the day of the audit.

During the audit, the partner will present a 15-minute general partner overview of the company covering:

- A business model, service and support model, and organizational overview
- If applicable, the business model overview should include provision of any partner added value services, built around Cisco products, such as managed network services, installation support services, and basic and advanced consulting services
- Partner should discuss the business and support relationship with Cisco. Suggested participants for this period of the audit would be the person responsible for managing the support relationship with Cisco, and the main contact for Cisco certifications and specializations.

Role of the Auditor

Cisco uses an independent third-party audit agency to conduct audits. The auditor manages the on-site audit process. The auditor will review supplied documentation prior to the audit, verify whether the partner complies with all of the program requirements, and compile the audit report describing the extent of compliance with each requirement. The auditor will then submit the report and supporting documents to the Cisco Partner Program Manager who will determine whether or not the partner meets these requirements. All information or documentation provided to the auditor is considered "confidential information" as defined in an NDA signed by Cisco's third-party auditors, and will be treated accordingly by both Cisco and the auditor.

Role of the Cisco Channel Account Manager (CAM)

Prior to the audit, it is the CAM's responsibility to ensure the partner fully understands the program requirements and to assist the partner in completing the online application. During the audit it is the responsibility of the CAM to address any business issues.

The CAM is also responsible for ensuring that a Cisco System Engineer (SE) is available for the Demo portion of the audit.

Role of the Cisco System Engineer (SE)

Responsibilities of the Cisco SE include:

- Assisting the Cisco CAM and the partner in preparing for the audit
- Reviewing the Customer Reference Documentation (for Master Specialization) before it is uploaded to CSApp.
- Interfacing with the Cisco Partner Program Manager, the Cisco partner support representative and others as appropriate.

- Co-managing the demonstration portion of the audit with the auditor.

Role of the Cisco Partner Program Manager (PM)

The Cisco Partner Program Manager (PM) is responsible for maintaining program integrity, and as such, the decision to award or revoke program certification or specialization rests with the PM. All grace periods described within the policy document are at the discretion of the PM.

Audit Findings and Follow-Up

At the audit closing session, the auditor will present a brief synopsis of the partner's audit opportunities for improvement and, in particular, will highlight any open action items. For open action items, the partner will be given an opportunity to provide written evidence of closure to the auditor within five business days after completion of the audit.

If unable to close out open action items within five business days, the partner should provide a corrective action plan to the Cisco Partner Program Manager. The action plan must be fully implemented within an agreed upon time period, not to exceed the stated get-well period. At the end of the agreed time period, a visit by the auditor, Cisco partner support representative, or local Cisco SE may be required in order to verify closure of an action item. The final decision to award certification or specialization will not be made until the corrective action plan is satisfactorily completed.

During and after the audit, neither the auditor nor the Cisco CAM can make commitments regarding the qualification decision. The Partner Program Manager will review the audit report and communicate results back to the partner within 20 business days. Results will be emailed back to the primary contact within the partner organization.

It is possible that the findings of the audit are such that qualification or re-qualification for the program cannot be achieved within the stated get well period. In this case, the Partner Program Manager may deny qualification.

If a partner fails to deliver an action plan within the agreed time frame, the partner may also be denied qualification for the program.

Appendix 1: Sample Audit Agendas

Audit Agenda: Gold/Silver Certification for Cisco Collaborative Services Program, Shared Support Program, Reseller Support and SIS

Audit Agenda Item	Estimated duration
Introductions and review of audit goals and methodology	15 minutes
Partner overview presentation	15 minutes
Cisco relationship	15 minutes
Review of Previous Action Items and Opportunities for Improvement, if applicable	15 minutes
Validation of support lab equipment/NFR equipment, including connectivity capabilities and tools	15 minutes
Customer Satisfaction/Loyalty	45 minutes
Pre-Sales/Plan, Design and Implement: <ul style="list-style-type: none"> ▪ Demonstration ▪ Project Management (including Post-Project Review/Lessons Learned) ▪ Design ▪ Quality Assurance ▪ Hiring and Training 	2.5 hours
Service Support: <ul style="list-style-type: none"> • Incident Management, including review of call tracking system and Cisco cases • Problem Management • On-site Response/Troubleshooting 	1.5 hours
Service Delivery: <ul style="list-style-type: none"> • Service Level Management • Security Management • Metrics 	1 hour
Review of audit findings with auditor (if applicable)	15 minutes

Audit Agenda: Gold/Silver Certification for Cisco Branded Resale and Packaged Services Program

Audit Agenda Item	Estimated duration
Introductions and review of audit goals and methodology	15 minutes
Partner overview presentation	15 minutes
Cisco relationship	15 minutes
Review of Previous Action Items and Opportunities for Improvement, if applicable	15 minutes
Revenue from Services	15 minutes
Pre-Sales/Plan, Design and Implement: <ul style="list-style-type: none"> ▪ Demonstration ▪ Project Management (including Post-Project Review/Lessons Learned) ▪ Design ▪ Quality Assurance ▪ Hiring and Training 	2.5 hours
Customer Satisfaction/Loyalty	45 minutes
Service Attach Rate	15 minutes
Service Support: <ul style="list-style-type: none"> • Incident Management 	1 hour
Service Delivery: <ul style="list-style-type: none"> • Security Management • Metrics 	1 hour
Review of audit findings with auditor (if applicable)	15 minutes

Audit Agenda: Master Unified Communications Specialization

Audit Agenda Item	Estimated duration
Introductions and review of audit goals and methodology	15 minutes
Partner overview presentation	15 minutes
Cisco relationship	15 minutes
Review of Previous Action Items and Opportunities for Improvement, if applicable	15 minutes
Validation of support lab equipment/NFR equipment, including connectivity capabilities and tools	15 minutes
Pre-Sales/Plan, Design and Implement: <ul style="list-style-type: none"> ▪ Demonstration ▪ Capacity Planning ▪ Design ▪ Hiring and Training 	2.5 hours
Service Support: <ul style="list-style-type: none"> ▪ Incident Management, including review of call tracking system and Cisco cases ▪ Problem Management ▪ Configuration Management ▪ Change Management and Release Management ▪ On-site Response/Troubleshooting 	2 hours
Service Delivery: <ul style="list-style-type: none"> ▪ Service Level Management ▪ Security Management ▪ Metrics 	1 hour
Review of audit findings with auditor (if applicable)	15 minutes

Audit Agenda: Master Security Specialization

Audit Agenda Item	Estimated duration
Introductions and review of audit goals and methodology	15 minutes
Partner overview presentation	15 minutes
Cisco relationship	15 minutes
Review of Previous Action Items and Opportunities for Improvement, if applicable	15 minutes
Validation of support lab equipment/NFR equipment, including connectivity capabilities and tools	15 minutes
Review of Vulnerability Assessment documentation	15 minutes
Pre-Sales/Plan, Design and Implement: <ul style="list-style-type: none"> ▪ Demonstration ▪ Capacity Planning ▪ Design ▪ Hiring and Training 	2.5 hours
Service Support: <ul style="list-style-type: none"> ▪ Incident Management, including review of call tracking system and Cisco cases ▪ Problem Management ▪ Configuration Management ▪ Change Management and Release Management ▪ On-site Response/Troubleshooting 	2 hours
Service Delivery: <ul style="list-style-type: none"> ▪ Service Level Management ▪ Metrics 	1 hour
Review of audit findings with auditor (if applicable)	15 minutes

Audit Agenda: Managed Services Certification

Audit Agenda Item	Estimated duration
Introductions and review of audit goals and methodology	15 minutes
Partner overview presentation	15 minutes
Cisco relationship	15 minutes
Review of Previous Action Items and Opportunities for Improvement, if applicable	15 minutes
NOC Tour/overview of services offered	30 minutes
Validation of support lab equipment/NFR equipment, including connectivity capabilities and tools	15 minutes
Pre-Sales/Plan, Design and Implement: <ul style="list-style-type: none"> ▪ Project Management (including Post-Project Review/Lessons Learned) ▪ Capacity Planning ▪ Design ▪ Quality Assurance ▪ Hiring and Training 	1.5 hours
Service Support: <ul style="list-style-type: none"> ▪ Incident Management, including review of call tracking system and Cisco cases ▪ Problem Management ▪ Configuration Management ▪ Change Management and Release Management ▪ On-site Response/Troubleshooting ▪ Remote Troubleshooting Access 	2 hours
Service Delivery: <ul style="list-style-type: none"> ▪ Service Level Management ▪ Security Management ▪ Service Continuity/Disaster Recovery ▪ POS Data Reporting ▪ Metrics 	1.5 hours
Review of audit findings with auditor (if applicable)	15 minutes

Appendix 2: Program Policies

This table provides an overview of policies only. See linked requirements for details.

Policy	Purpose	Gold	Silver	Master UC	Master Security	Managed Services (MSCP)
Annual Re-Certification/ Specialization Qualification	Policy regarding annual recertification and re-qualification for specializations.	✓	✓	✓	✓	✓
On-site Audit Waiver	Policy to waive the on-site audit requirement for partners demonstrating outstanding performance within the program.	✓	✓	✓	✓	✓
Get-Well Plans	Policy regarding providing an extended time period to ensure compliance with an outstanding requirement for recertification.	✓	✓	✓	✓	✓
Certification Downgrade	Policy regarding partner downgrade for noncompliance to program requirements.	✓	✓	✓	✓	✓
Mergers, Acquisitions and Affiliate Policy	Policy related to certification (and specialization) of a business entity formed by a merger or acquisition or where the resources and staff fulfilling the certification or specialization requirements are controlled or employed by more than one legal entity.	✓	✓	✓	✓	✓
CCIE/CCVP/ CCSP Hiring and Terminating	Policy regarding loss of or hiring of a CCIE, CCVP or CCSP from another Cisco certified or specialized partner.	✓	✓	✓	✓	N/A
CCIE Sharing	Policy regarding sharing of CCIEs required for certification and/or specialization.	✓	✓	✓	✓	N/A
CCIE Contracting	Policy regarding contracting out required CCIEs, including to Cisco Learning Solution Partners (CLSP).	✓	✓	✓	✓	N/A

Policy	Purpose	Gold	Silver	Master UC	Master Security	Managed Services (MSCP)
<u>Competitor Policy</u>	Policy regarding direct competitors to Cisco not being eligible for certification or specialization.	✓	✓	✓	✓	✓
<u>Outsourcing</u>	Policy for outsourcing part of partner's support service (as required for certification and/or specialization) to a third party. This policy covers call center operation, technical support and on-site service.	✓	✓	✓	✓	✓
<u>Consolidated Support Centers (CSC)</u>	Policy that allows a partner that operates in more than one country to consolidate support operations in one or more regional centers.	✓	✓	✓	✓	✓
<u>Language Requirements</u>	Policy regarding language requirements for audit documents	✓	✓	✓	✓	✓
<u>Discounts and Rebates</u>	Policy regarding discounts and rebates granted for program participation	N/A	N/A	N/A	N/A	✓
<u>Multiple Master Specializations</u>	Policy regarding attaining Master Specialization in more than one technology, i.e., Master UC and Security	N/A	N/A	✓	✓	N/A

Direct competitors of Cisco Systems will not be granted Specialized or Certified Partner status pursuant to the World Wide Channel Partner Program. Direct competitors may participate as registered partners. Any entity that is owned or controlled by a competitor may not participate as Specialized or Certified Partners. Ownership or control is defined as 51% or more.

Detailed Program Policies

Annual Re-Certification/Specialization Qualification
Gold
<p>Certification is valid for 12 months. Partners are expected to remain in compliance with the program requirements throughout the certification period. Partner compliance is validated through an annual recertification audit.</p> <ul style="list-style-type: none"> ▪ Certified partners must submit an on-line application for recertification by their certification anniversary date each year. ▪ Partners that have not submitted a complete application within 30 days of their certification anniversary date may be de-certified. ▪ In order to maintain certification, the recertification audit must be conducted no later than 60 days after the partner's certification anniversary date. ▪ If a partner's recertification is delayed for any reason, including a corrective action plan to address a deficiency, the partner's certification anniversary date will not be adjusted. The partner will still be due for recertification on their next anniversary date.
Silver
Same as Gold
Master UC
Same as Gold
Master Security
Same as Gold
Managed Services
Same as Gold

On-Site Audit Waiver
Gold
<p>In order to qualify, partners must have demonstrated exemplary performance during their prior year's audit, resulting in no audit action items and get-well plans. Partners must also have remained in compliance with the overall certification program, including requirements for personnel and customer satisfaction, consistently during the 12 months preceding their current anniversary date, with no get-well plans assigned by the Program Manager.</p> <p>Partners must also meet all criteria outlined in Section II.1 of the Certification and Specialization Terms and Conditions, plus relevant attach rate and service revenue metrics. Any changes to the program requirements, partner's support agreement, merger/acquisition or business operations may disqualify partners from an on-site audit waiver.</p> <p>Eligibility for the audit waiver is based upon the discretion of the Cisco Channel Certification Manager. Partners awarded an audit for a given recertification anniversary date must participate in an on-site audit for recertification on their following anniversary. Partners will not be awarded audit waivers two consecutive years.</p> <p>All partners qualifying under the current Channel Partner Program requirements for the first time will not be eligible for the on-site audit to be waived, unless they have been recently audited for Master UC, Master Security, or Managed Services.</p>
Silver
Same as Gold
Master UC
Same as Gold
Master Security
Same as Gold

Managed Services
Same as Gold

Get-Well Plans

Gold

During the course of a get-well plan, the partner will maintain the current certification level, provided that all other certification or specialization requirements are met. Failure to meet the get-well plan requirements may result in loss of certification or specialization and corresponding discount. Eligibility for get-well plan is based upon the discretion of the Cisco Channel Certification Manager. Consecutive get-well plans (two get-well plans in one certification year) are not allowed.

Silver

Same as Gold

Master UC

Same as Gold

Master Security

Same as Gold

Managed Services

Same as Gold

Certification Downgrade

Gold

Cisco may decertify or downgrade a partner if the partner fails to comply with Gold or Silver requirements during the certification term due to, but not limited to, the following:

- Failure to maintain current ICPA
- Failure to meet certified individual requirements
- Failure to meet specialization requirements
- Failure to meet customer service requirements
- Failure to meet the service attach rate requirement, if applicable
- Failure to submit the renewal application within 30 days of anniversary date

Silver

Same as Gold

Master UC

Same as Gold

Master Security

Same as Gold

Managed Services

Same as Gold. plus

- In addition to any of its other remedies, Cisco reserves the right to terminate a partner from participation in the Managed Services Channel Program for the following reasons: (a) submission of false, misleading, or incomplete MSCP information; (b) other fraud or abuse of this or other Cisco marketing or sales programs; (c) the distribution of Cisco Products purchased from any source other than Cisco or an authorized Cisco Distribution Partner, or Global Logistics Partner purchasing product in the MSCP program and deploying product in non-managed environments, intentionally purchasing product under the Managed Service identifier to obtain higher discounts (for example, buying CPE for use in a Cisco Powered Managed Service and using the product to terminate a Cisco Strategic Managed Service or Cisco Legacy Managed Service).

Mergers, Acquisitions and Affiliate Policy

Gold

The new, combined entity must inform Cisco of the integration of the entities by providing the Program Manager with a plan for integration of processes, systems, labs, escalations, etc., as well as timelines for this integration.

Where the resources and staff relevant to the program are controlled or employed by different

companies within the same corporate group, Cisco will grant certification or specialization only if the applicant can demonstrate that those staff and resources operate as an integrated business unit with respect to the support services supplied to the partner's customers. For that reason, certification (and specialization) is granted for a single company within a country/country group. Cisco requires that the resources and staff relevant to the applicant's certification (and specialization) work as an integrated business unit to fulfill the customer's pre-sales and post-sales support needs.

This integration must conform to the requirements as laid out below.

To be considered toward certification or specialization program qualification, certified individuals must be *full-time* or *full-time equivalent* employees of the company based within the country for which certification (and specialization) is applied and identified as such in Cisco's training database.

The relevant resources and staff must act operationally as an integrated business unit.

There must be:

- Common support and management structures
- Common escalation procedures
- A shared intranet, with visibility to customer status across the affiliates
- Call-tracking systems that intercommunicate
- A centralized approach allowing post-sales engineers to access information about all installations and support all customers, even when planned, designed, or implemented by another affiliate

The staff must be full-time or full-time equivalent employees of the affiliate or applicant and working within the country for which certification is applied for.

A fully owned subsidiary, or the parent company of a certified partner can benefit from the same discount of the certified partner. The non certified business division will not be able to use the branding of the certified division.

Mergers

Regardless of when companies merge, Cisco certification will recognize the new entity as of the date the new legal contract is signed with Cisco. Until the new legal contract is signed, the merging entities will maintain their separate certification (and specialization) achieved.

An on-site audit will be required within 90 days of the merger in order to verify that the combined company meets all requirements for that certification (and specialization). The requirement for an on-site audit is to determine the level of integration and potential disruption in the pre-sales or post-sales functions of the two businesses.

The new, combined entity must inform Cisco on the integration of the entities by providing the Program Manager with a plan for integration of processes, systems, labs, escalations, etc as well as timelines for this integration. For companies that will remain separate legal entities, please see the affiliate policy below.

Affiliates

Each affiliate applicant must show:

- The affiliate is controlled, directly or indirectly, by the applicant
- Both the applicant and the affiliate are controlled, directly or indirectly, by the ultimate parent company
- The affiliate controls, directly or indirectly, the applicant

Control for these purposes may be assumed where there is, directly or indirectly, 51 percent share ownership or where local accounting rules allow the applicant and the affiliate to file consolidated

statutory accounts as part of a corporate group.
Silver
Same as Gold
Master UC
Same as Gold
Master Security
Same as Gold
Managed Services
Same as Gold, plus partners that meet the definition of affiliates that want to transact with Cisco in the Managed Services Channel Program must, at a minimum, have achieved Cisco Premier status independent of the Parent (affiliate) company, and the Parent company must be responsible for the POS requirements of their affiliates transacting in MSCP.

CCIE/CCVP/CCSP Hiring and Terminating
Gold
Losing Partner
If the loss of a CCIE, CCVP, or CCSP takes a certified partner below the number of individuals required for certification or a specialization, partner is to notify Cisco of its noncompliance within 30 days.
Upon receipt of such notice, partner may qualify for an extension of up to six months to replace the CCIE, CCVP, or CCSP in order to avoid de-certification or losing the specialization that requires a CCIE, CCVP, or CCSP. A partner that voluntarily terminates the employment of a CCIE may not qualify for the time extension. During the extension period, the partner will retain its certification or relevant specialization as long as all other certification or specialization requirements are met.
If a partner does not notify Cisco of its noncompliance with the CCIE, CCVP, or CCSP requirement within 30 days and Cisco identifies the deficiency, the partner may be given an extension of up to 60 days to replace the CCIE, CCVP, or CCSP in order to avoid de-certification or losing the specialization that requires a CCIE, CCVP, or CCSP. This extension period will begin upon Cisco's notification to the partner of noncompliance.
Gaining Partner
If a partner hires a CCIE, CCVP, or CCSP away from another Cisco certified or specialized partner, Cisco will not count this individual toward certification or specialization for the hiring partner for a period of 12 months from the termination date of the previous partner. This rule does not apply if a Cisco certified or specialized partner terminated the CCIE, CCVP, or CCSP or is willing to release their CCIE badge to be used. In this case, Cisco will require documentation from the partner that terminated the CCIE, CCVP, or CCSP or releases their CCIE, CCVP, or CCSP. If the CCIE, CCVP, or CCSP worked for more than one certified or specialized partner within the past 12 months, termination or release documentation will be required from each previous company.
Silver
Same as Gold
Master UC
Same as Gold
Master Security
Same as Gold
Managed Services
N/A

CCIE Sharing
Gold
A partner using the Consolidated Service Center model (see CSC policy) may meet the CCIE requirement in the following manner:
<ul style="list-style-type: none"> Half of the required CCIEs must be located in the designated CSC. These engineers must be

<p>distinct from those nominated for in-country certification for the CSC country or any other countries. The remainder of the required number of CCIEs must be located in the country applying for certification.</p> <ul style="list-style-type: none"> ▪ If a partner has multiple CSCs, CCIEs can only be allocated from the designated CSC that will provide remote support for the country applying for certification. ▪ If a remote country is not using a CSC, all CCIES required for certification must be in country.
Silver
Same as Gold
Master UC
Same as Gold
Master Security
Same as Gold
Managed Services
N/A

CCIE Contracting (including to CLSPs)
Gold
<p>CCIEs required for certification must be legally employed by the applying partner in the country where the partner is seeking certification. A maximum of 50 percent of the required number of CCIEs can be hired under contract provided that the following criteria are met:</p> <ul style="list-style-type: none"> ▪ CCIE must have exclusive, full-time contract with partner in country seeking certification and must dedicate 100 percent of his or her time to that partner's business ▪ Contract must be good for at least 12 months from the audit date
Silver
Same as Gold
Master UC
Same as Gold
Master Security
Same as Gold
Managed Services
N/A

Competitor Policy
Gold
<p>No direct Cisco competitor can be Cisco certified or specialized. In the event a current certified partner becomes a competitor through a merger and acquisition process, the partner will receive a 30 days de-certification notification.</p>
Silver
Same as Gold
Master UC
Same as Gold
Master Security
Same as Gold
Managed Services
Same as Gold

Outsourcing
Gold
<p>Call Center Operation</p> <p>The partner may outsource initial call-taking activities to a third party as long as the following requirements are met:</p> <ul style="list-style-type: none"> ▪ The partner must demonstrate how the skills and capabilities of the outsourced party are evaluated in determining suitability to provide such services, including the mechanism employed to monitor ongoing performance.

- The outsourced activities must be formalized in a contract between the partner and the outsourced company. This contract must be made available to the audit team for review during the audit and must include a SLA consistent with the support requirements for the partner's level of certification.
- The outsourced party must receive phone calls in the local language through the partner's published service telephone number for the country.
- The outsourced party must have appropriate access to the partner's call-tracking system to allow for immediate logging of customer calls.
- The outsourced party must ensure callback by a partner engineer within one hour.
- The outsourced party must be able to contact partner engineers or management and transfer customer phone calls to the partner as appropriate.
- Subsequent call tracking and management, troubleshooting, case updates, escalation and alerts, and case closure are the full responsibility of the partner.
- No technical support is to be outsourced as part of the Call Center.

After-Hours Call Center Support

After-hours call center operation can be outsourced to a third party, such as a paging service, if the following criteria are met:

- The partner must demonstrate how the skills and capabilities of the outsourced party are evaluated in determining suitability to provide such services, including the mechanism employed to monitor ongoing performance.
- The outsourced activities must be formalized in a contract between the partner and the outsourced company. This contract must be made available to the audit team for review during the audit and must include a SLA consistent with the support requirements for the partner's level of certification.
- The third party must have procedures to guarantee that customers will receive technical support as stipulated in their service contract. These procedures must consist of an escalation process where, if the designated on-call engineer does not respond within a specified timeframe, a second attempt is made. If there is still no response, a manager is notified.
- Procedures must be documented on how the partner will be notified, during normal business hours, of all calls received during the previous after-hours or holiday period.
- No technical support is to be outsourced as part of the Call Center.

Technical Support Operation

Technical support operation must remain in-house with the partner and cannot be outsourced to a third party.

On-site Hardware Replacement Services

The partner may outsource on-site hardware replacement provided that the following requirements are met:

- The partner must demonstrate how the skills and capabilities of the outsourced party are evaluated in determining suitability to provide such services, including the mechanism employed to monitor ongoing performance.
- The outsourced activities must be formalized in a contract between the partner and the outsourced company. This contract must be made available for review during the audit.
- Details regarding the training and skill level of the engineers of the outsourced party to support Cisco products must be provided.

Silver

Same as Gold

Master UC

Partner may not outsource activities as described for Gold certification; must be accomplished with internal infrastructure.

Master Security

Same as Master UC

Managed Services

Same as Gold, except:

- Technical support for specific edge technologies may be outsourced to partners with specific domain knowledge necessary to provide a fully managed solution. Any third party must have all appropriate Cisco certifications for those technologies. Partners must own a NOC and be outsourcing one element of their MNS business, not their entire MNS offering.

Consolidated Support Centers (CSC)

Gold

A partner that operates in more than one country may elect to consolidate support operations in one or more regional centers. The Consolidated Support Center (CSC) may be utilized to take, handle, resolve or escalate customer support cases, in conjunction with the partner's local support organization.

The CSC must meet the following criteria as validated by an annual audit:

- CSC must operate on a 24x7 schedule, either as a single entity or through a "follow-the-sun" coverage model
- CSC must follow operations and service delivery methodologies based upon an accepted industry standard such as the Information Technology Infrastructure Library (ITIL) framework.
- CSC must employ a consistent process for handling and passing cases between the local and central operations.
- CSC and all countries utilizing it must share the same IT infrastructure and tools
- Participating countries must have visibility through tools to real-time information on the status of cases
- Partner can have more than one CSC providing support to customers in a given country, but must identify all centers providing support, scope of responsibility and documented process for providing seamless support.

The CSC(s) must provide support specified for certification level of the remote country, including:

- Telephone support with local phone number and support of national language(s)
- Call-back and on-site response
- Single, integrated call tracking system with transparent escalation process (system must meet all program requirements)
- All resources providing technical support, in the local support organization and in the CSC, must have full access to the call tracking system

At the time of the audit the following requirements will be validated:

- Partner must outline a lab strategy, sparing strategy and relationship to specializations in remote country
- Partner must demonstrate a single, integrated call tracking system
- Partner must demonstrate case escalations between country seeking certification and CSC
- Partner must demonstrate that CSC staff and local staff have full access to call tracking system
- Partner must demonstrate central lab's remote access and access across the different countries
- Partner must provide international escalation procedure: demonstrated by example of two cases per country

Lab Equipment (for Cisco Collaborative Services, Shared Support, SIS and Reseller Agreements)

Equipment necessary to satisfy the demonstration and post-sales lab requirements for certification and specialization can be located in the CSC if the following criteria are met:

- Engineers in the remote country must have full access to equipment located in the CSC (on a 24-hour basis for Gold certified countries). Partner will be required to demonstrate this during the on-site audit.
- If a remote country is not using a designated CSC, all required equipment must be located in-country.

- If a partner utilizes a centralized lab (in a CSC) for achieving certification and/or specialization in remote countries, the CSC lab will be audited on an annual basis.

Audit Requirements: Remote Country Using CSC

If a country operation seeking certification is using a CSC in another country, the following audit requirements apply (in addition to the standard audit itinerary):

- Partner must provide adequate documentation of the support processes between the CSC and country seeking certification, including but not limited to, passing of cases between the two organizations.
- Partner must demonstrate that the CSC CCIEs designated to support the remote country and the management of both the CSC and support organization of the remote country are incorporated in the escalation process. This should be demonstrated in the 10 sample cases.
- Partner must demonstrate that support personnel in the CSC and country seeking certification have full access to the call tracking system in order to enter and update cases.
- Partner must provide documented process outlining seamless escalation process to CSC.
- Partner must provide evidence of execution of CSC recommendations at end customer installation.

Audit Requirements: CSC

A separate audit of the CSC will be conducted to ensure that support between the countries and central operation is performed in accordance with SLAs, and that policies and procedures are understood and correctly executed on both. Cisco will exercise commercially reasonable efforts to attempt to schedule a CSC audit at a time contiguous with other program audits to reduce overhead and interference.

Suggested participants:

- Partner's Cisco Alliance Manager/Director and a Technical Manager responsible for all service and support of Cisco technology
- Cisco account manager and Cisco SE responsible for partner relationship across geographic region, or local SE in country where CSC is located
- The partner theater support or local technical lead, able to demonstrate the tools and case handling (usually a CCIE)

Prerequisites (to be collected prior to the audit):

- Case handling and escalation process documentation, in English
- Description of integrated call tracking system, in English
- Auditor will select two cases (not older than 12 months) per supported country
- Lab equipment use policy

Itinerary:

- Introductions and audit goals (auditor)
- Overview of audit methodology (auditor)
- Partner support strategy overview presentation, including regional and/or technology coverage, organization structure, SLAs and metrics
- Call handling process from end customer to CSC to Cisco (reviewing of call tracking system, including two cases per remote country using CSC)
- Review of audit findings (if applicable)

During the CSC audit, the partner must:

- Provide an overview of qualified engineers
- Outline lab equipment strategy and sparing strategy, including relationship to specializations in remote countries
- Demonstrate a single, integrated call tracking system, including tracking of elapsed time from case receipt to closure (all requirements for tracking and escalation should be satisfied)
- Demonstrate that the CSC CCIEs designated to support the remote country and the management of both the CSC and support organization of the remote country are incorporated

in the escalation process (this should be demonstrated in the two sample cases per remote country using the CSC)

- Demonstrate that support personnel in the CSC and country seeking certification have full access to the call-tracking system in order to enter and update cases
- Demonstrate the central lab's remote access capabilities and access across the different countries
- Provide international escalation procedure: demonstrated by example of two cases per country
- Provide the ratio assigned to in-country engineers versus remote counties supported
- Demonstrate that the lab is equipped to support the various remote country specializations.
- Have, or have access to the Service Level Agreements (SLA) of customers in the remote country(s) of support.
- Demonstrate solid connectivity in accessing the lab and call tracking systems remotely particularly in the event of poor network infrastructure locations.
- Demonstrate the CSC has technical personnel on duty to support customers in all languages of the supported remote countries. (A duty roster for the local CCIEs must be presented to the auditor for review.)
- Demonstrate local management visibility of high priority cases. (Two sample cases must be provided to the auditor.)
- Present a documented review process that validates that escalation is triggered in accordance with the escalation procedures and/or other business rules meeting the specific country requirements.

Silver

Same as Gold

Master UC

Same as Gold

Master Security

Same as Gold

Managed Services

Same as Gold, except:

- Partners with current MSCP qualification who want to use Consolidated Support model do not require a separate CSC audit.

Language Requirements

Gold

Partner may submit documents in a language other than English.

If the partner submits documents in a language other than English, Cisco will attempt to qualify the documents using an auditor familiar with the partner's language.

If an auditor cannot qualify the documents, Cisco will attempt to have them qualified by a Cisco employee familiar with the partner's language. This responsibility will rest with the theatre in which the partner is applying for Master Specialization.

If neither the auditor nor a Cisco employee can qualify the documents, the partner will be asked to translate them into English.

Silver

Same as Gold

Master UC

Same as Gold

Master Security

Same as Gold

Managed Services

Same as Gold

Discounts and Rebates

Gold
N/A
Silver
N/A
Master UC
N/A
Master Security
N/A
Managed Services
<p>Discount Structure</p> <p>The available discount at which a partner may purchase Managed Service CPE products is dependent upon the level to which the Managed Service has been certified below. Discounts are applicable only when buying Direct from Cisco. Purchase price when buying from distributor or global logistic partner are to be negotiated directly with distributor or global logistic partner.</p> <ul style="list-style-type: none"> ▪ Cisco Powered Managed Services: Discount 47% off GPL + 10% rebate of net amount ▪ Cisco Strategic Managed Services: 47% ▪ Cisco Legacy Managed Services: 42% <p>Irrespective of the Managed Service, discounts will be available only for eligible Managed Service CPE. Products purchased for a partner's internal use, core infrastructure or resale without the provision of a Managed Service, are not eligible under the MSCP.</p> <p>Discounts awarded under the three discount levels cannot be combined.</p> <p>Discounts, Rebates and Claiming</p> <p>A rebate of 10% of the net purchase price of the Managed Service CPE will be paid to the partner for CPE purchases that match the agreed upon product lists for the partner's Managed Services that have been designated as Cisco Powered Managed Services. This rebate is in addition to Cisco Powered Managed Services discount for eligible CPE products and subject to the following conditions:</p> <ul style="list-style-type: none"> ▪ Rebate will be paid to partner centrally on achievement of criteria ▪ Rebate and qualification to be calculated and paid on CPE sales is only associated with Cisco Powered Managed Services. <p>On an individual Cisco Powered Managed Service basis, claims will be validated and if the requirements are met, Cisco will calculate the eligible rebate for the CPE deployed at end user sites during the claim period. Cisco will then confirm to the partner the value of the rebate that they are entitled to claim. If the partner is on credit hold with Cisco finance, the rebate will be withheld until the account is made current.</p> <p>Eligible Products</p> <p>Rebates and/or discounts are awarded for CPE purchases that match the agreed upon CPE lists for each Managed Service. No other SKUs or product families are eligible for discount or rebate. Rebates will only be paid, subject to all other program conditions, on products that have serial numbers and that are not included as components of a larger assembly at zero cost. For example, an interface card may be a component of a complete product, or an individual item to be sold separately. When the interface card is included in the price of the complete product, a rebate will only be paid on the complete product item that includes the other components (providing the complete product item serial number is quoted).</p> <p>Combination with other Programs</p> <p>MSCP rebates and/or discounts cannot be claimed in conjunction with any of the following:</p> <ul style="list-style-type: none"> ▪ Solution Incentive Program (SIP) ▪ Opportunity Incentive Program (OIP) ▪ Value Incentive Program (VIP)

- Cisco EUP promotions
- Infrastructure discounts

MSCP rebates and discounts do apply when combined with CTMP and TMP trade-ins pursuant to the CTMP and TMP terms and conditions.

Data Accuracy

Rebates and/or discounts will only be paid if accurate and complete Point of Sale ("POS") information is provided. It is the responsibility of the partner to provide POS information consistent with the POS template (see MSCP POS Template; <http://www.cisco.com/go/mscp>) no later than the second week of each month for the prior month's transactions in order to qualify for the discounts and/or rebates set forth in this program. POS is to be supplied for all Managed Services transactions that are purchased under the program. Cisco will not honor discounts or pay any quarterly rebates unless POS data is in compliance and up to date. Failure to deliver accurate POS data for a 3 month period will cause a partner to be suspended from purchasing CPE under this program.

Cisco reserves the right to audit all purchase orders, discounts and rebates claimed or made under the MSCP. Cisco reserves the right to validate the end user details and the status of the Managed Service deployed.

If irregularities are found such as incorrect/non-existent end user detail, incorrect MSID or late submission of deployment reports, then Cisco reserves the right to withhold discounts and rebate payments, and/or to terminate partner participation in the MSCP at Cisco's discretion.

Rebate Eligibility

SKUs or product families eligible for the rebate are tied to pre-established BOMs by Managed Service type as provided by each pilot participant.

Rebates will be paid only on the applicable Managed Service transactions (as identified by a unique pre-established reusable deal ID per transaction).

Product that is procured from a distributor may only be purchased from an authorized distributor.

Partners are responsible for keeping their own sales information. Cisco will provide partner access to program results via the MSCP tool. If partner believes there are any discrepancies between Cisco published bookings and their own records they are responsible for identifying such potential discrepancies to Cisco. Any bookings discrepancies must be reported immediately. Deadline for any bookings discrepancy cases is one month from final bookings date.

Sales that are eligible for the rebate under the MSCP are not eligible for any other Cisco rebate program unless otherwise stated by Cisco.

Cisco reserves the right to modify or cancel the program at its discretion without prior notice to channel partners.

Cisco reserves the right to refuse this offer to deals that do not comply with the intent of this program

Rebate is based on meeting full payout criteria.

Net bookings are used to qualify partner for MSCP revenue requirement. Actual payment is based on specific MSCP period net bookings that ship in time periods as defined above. Net Bookings = MSCP period bookings less MSCP period de-bookings. Bookings are recognized when order is placed with Cisco. Authorized Distributor orders may not be received by Cisco on the same business day an order is placed with a Cisco Authorized Distributor. Authorized Distributor

bookings are typically received by Cisco in one business day; partners buying through distributors must purchase at least one business day prior to the deadline (see above) to apply toward period bookings. Cisco does not recognize distributor point-of-sale (POS) until product ships and invoices, regardless of when product is booked with an Authorized Distributor.

Specific to Authorized Distributor bookings, the timing or transaction date will be tied to the "Claim Date" vs. the actual raw "POS date" when the goods are actually shipped. The "Claim Date" is tied to the event when Cisco actually reimburses the applicable Distributor for claims submitted against the Managed Services Channel Program (MSCP).

If the partner has an accounts receivable statement that is overdue by 15 days or more, the MSCP rebate will be withheld until the account is made current. Cisco reserves the right to add or remove Managed Services from the eligible list of services at the beginning and end of each Cisco fiscal quarter.

In addition to any of its other remedies, Cisco reserves the right to terminate a partner from participation in this program for the following reasons: (a) submission of false, misleading, or incomplete program information, including claims for sales made under the program; (b) other fraud or abuse of this or other Cisco marketing or sales programs; and (c) the distribution of products purchased from any source other than Cisco or an authorized Cisco distributor.

Rebate payments will be made within region or theatre where net bookings/shipments originated. Enrolled partners should provide the appropriate bank routing information within each of the applicable regions and/or theatres.

POS Close-Out Policy

In the event that an enrolled partner is delinquent in providing monthly POS reports for a total of 90 days, any outstanding rebates due to the applicable partner will be put on hold. In addition, enrollment privileges in the current program will be revoked. The delinquency period is measured from the time POS data is due to Cisco (five working days following the calendar month-end). The applicable enrolled partner then has an additional 90 days to recover and provide up to date POS reporting information. In the event that such data is provided over this additional 90 day period, outstanding rebates will be paid in full and the partner will automatically be eligible for privileges contained within the current and prior program periods.

No special payments will be made if and when a partner recovers and qualifies for a payment. In such cases, the timing of payment will coincide with the standard quarterly cycle as provided to all enrolled partners. If after a total of 180 days the applicable partner still does not provide the required POS data, any outstanding rebates will be terminated and closed out. In addition, enrollment privileges will be revoked until the partner has provided all the required up to date POS reporting information. In the event that POS information is finally provided, the partner will be eligible for the current program period.

As noted, rebate payment periods are measured in three month or quarterly increments.

Multiple Master Specializations

Gold

N/A

Silver

N/A

Master UC

Pre-Audit Requirements

- Advanced Specialization: Partners must hold an Advanced Specialization in all technologies for which they desire Master Specialization.
- CCIE: Partners must have a technology-specific CCIE certification in all technologies for which they desire Master Specialization. A person holding multiple CCIE certifications may only be

designated to fill the requirement of one Master Specialization.

- Project Manager: Partners must have a technology-specific project manager in all technologies for which they desire Master Specialization. Each must be a unique full-time regular employee *residing in the country of the partner seeking certification* and in good standing with Cisco.
- Industry-specific Security certifications: The person designated to fill this requirement must be a dedicated member of the security practice and a unique full-time regular employee *residing in the country of the partner seeking specialization* and in good standing with Cisco.
- Customer Reference Accounts: Reference accounts may be shared across Master Specializations. That is, a customer for whom the partner has designed and deployed Cisco solutions that meet the requirements of the Master Security Specialization AND the Master Unified Communications Specialization may use that customer as a reference account for BOTH master specializations.

Demos

Partners may combine demos for as many technologies as they feel comfortable.

Applicability of Industry Standards/Certifications

If the partner is applying ISO 20000, ISO 27001, SAS70 or other certification as an exemption (as specified in the Requirements section of this document), this certification may be used as an alternative to an on-site audit of the applicable requirements for as many technology practices for which the certification is valid. Certification must be valid for at least one year from the date of Cisco's on-site audit.

Master Security

Same as Master UC

Managed Services

N/A