Cisco Channel Program Audit and Policies Document

Version 6.1

May 31, 2015

Version	Date	Document Updated By	Summary of Modifications
6.0	21-Nov-2014	WWPO Certification Team	www.cisco.com/go/audit/
6.1	31-May-2015	WWPO Certification Team	www.cisco.com/go/audit/

Resale: Gold (G), Silver (S); Master Specialization: Collaboration (Collab), Security (Sec); Cloud Builder (CB); Cloud & Managed Services: Master (M), Advanced (A), Express (E)

Resale: Gold (G), Silver (S); Master Specialization: Collaboration (Collab), Security (Sec); Cloud Builder (CB); Cloud & Managed Services: Master (M), Advanced (A), Express (E)

Introduction

The Cisco Channel Partner Program

As markets transition to meet the demands of a new world economy, the network continues its rapid expansion – to become the platform for a new era of any-device, any-content, and any-time communications.

What's driving the transition?

- Globalization, which demands an IT infrastructure that enables people to work and serve new markets anywhere and everywhere, at any time.
- Collaboration or the ability to work across borders to innovate and transform the enterprise.
- Virtualization of technology resources, so that customers can get more from their resources while still keeping capital costs down.
- Hybrid IT, new cloud architectures and services, offering you and your customers more flexibility and choice.

The challenge for Cisco and our partners is to recognize and seize opportunities in this time of transition. The industry-leading Cisco Channel Partner Program helps partners capture the momentum of markets in transition. This means aligning with change and finding new ways to accelerate growth, differentiation, profitability, and customer satisfaction. Customer satisfaction continues to be among the highest priorities of Cisco and a cornerstone of the Cisco Channel Partner Program. 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 provides partners with the latest Cisco technologies and training to build their capabilities. And the program rewards partners with incentives, branding, and other benefits for the value they bring to our joint customers.

To meet newly established market demands, our channel programs must constantly evolve. Nevertheless, the mission of the Cisco Channel Partner Program remains the same: to enable partners to drive profitable growth, both for themselves and for Cisco. To meet customer needs and help our partners capture this growth opportunity, Cisco provides a framework for partners to build the sales and technical skills, and best business practices, necessary to deliver solutions and services based on Cisco technologies.

How to use this Document

This document provides a detailed list of audit requirements specific to each program: Resale: Gold (G), Silver (S); Master Specialization: Collaboration (Collab), Security (S) Cloud Builder (CB); and Cloud and Managed Services: Master (M), Advanced (A), and Express – NOC (E).

The requirements in this document are nominally based on the Information Technology Infrastructure Library (ITIL) Version 3 framework, and are aligned with the Cisco Lifecycle Services model. Processes within each lifecycle may occur across several phases; for example, Change Management is part of Service Transition, but is also a key process during Service Operation. Partners will be expected to demonstrate the effectiveness and efficiency of all processes (for example, operational efficiency, metrics for Customer Satisfaction [CSAT], etc.).

1 Audit Process and Methodology

1.1 Audit Scheduling

An audit will be scheduled once the partner has submitted a complete new or renewal online application and the Cisco Certification Program Manager has verified that pre-audit requirements have been met.

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

Generally, the audit will take place within 30 days of Cisco's validation of the partner's prequalification requirements. This timeframe is dependent upon auditor availability, location of the audit, or combination of multiple certification audits.

Cisco personnel authorized to attend a partner's audit will be noted on the audit confirmation. Employees or contractors who do not have prior approval from the Cisco Certification Program Manager will not be permitted to participate in the audit, regardless of their role.

Annual recertification
Certified partners must submit an online application for recertification by their certification anniversary date each year. Partners that have not submitted a complete application, including all required documentation, before the 30th day past their anniversary date (anniversary date + 30 days) will be decertified.

In order to maintain certification, the recertification audit must be conducted no later than 60 days after the partner's certification anniversary date.

New audit cycle
Partners who demonstrate outstanding performance within the program may be eligible to renew without an audit for up to 3 years.

Renew Annually
3 year cycle with potential for in-cycle reviews and validations
What will trigger action during the 3 year cycle?

- Addition of specializations or services
- Significant program changes
- Major compliance issues or previous audit performance

Partners who outsource their NOC operations will be audited annually (no waiver) to ensure continued program requirement compliance. See Appendix 5: CMSP Policies for details.

Focused audit
Focused audits are offered to eligible partners who have demonstrated consistent compliance and solid audit history. The focused audit is designed to include more specific capabilities of a partner's business. It will capitalize on the partner's previous audit history (e.g. action items and opportunities for improvement) while tailoring the current re-certification audit to a partner's business and technical capability, with focus on strengthening processes and continual improvement.
NOTE: Does not apply to the demonstration requirements for any Master specializations.

Outsourcing NOC operations
Partners may outsource some elements or the entire NOC operations to a NOC services provider as described in Appendix 6: Outsourcing NOC Operations.

The requirements for outsourcing NOC operations, which will be reviewed in their entirety at the time of audit, include:

- Partner and NOC services provider responsibilities
- Summary of program requirements that can be outsourced for partner to meet published CMSP requirements together with NOC services provider

Readiness Review
A Readiness Review is now available for partners prior to the audit.

The Readiness Review is available for Cisco Partners to engage with an auditor and review their Cisco Channel Program audit preparedness. NSF, a third party auditing firm, offers this service as an optional partner-paid opportunity for evaluation of the partner's systems as compared to the Audit Document controls. The auditor who conducts the Readiness Review will not be the same auditor that will conduct the audit. Participation in the Readiness Review does not guarantee any specific outcome for the audit, however, it will provide a view of any potential gaps in the readiness for the audit. The link to request a Readiness Review can be found at www.cisco.com/go/audit/.

1.2 Role of Audit Participants

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 be prepared to provide any additional required documents on the day of the audit.

During the audit, the partner must present a 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 phase 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 onsite audit process. During the audit, the auditor will verify whether the partner complies with the spirit and intent of all program requirements and compiles an audit report describing the extent of compliance with each requirement. The auditor will then submit the report and supporting documents to the Cisco Certification Program Manager who will determine whether or not the partner meets the program requirements. All information or documentation provided to the auditor is considered "confidential information" as defined in a nondisclosure agreement (NDA) signed by Cisco's third-party auditors, and will be treated accordingly by both Cisco and the auditor.

Role of the Cisco Partner Account Manager (PAM)
Prior to the audit, it is the PAM's responsibility to ensure the partner fully understands the program requirements and to assist the partner in completing the online application. During the audit, the PAM must be present and fully engaged throughout the duration, and it is the responsibility of the PAM to address any business issues during the audit whether onsite or attending remotely. This requirement is to ensure that partners have Cisco's support during the 3rd party audit.
If an audit is onsite, the PAM should either attend in person or make arrangements to ensure Cisco has a representative onsite to support the partner.

If an audit is being conducted remotely via WebEx or TelePresence, the PAM should make arrangements to attend the audit remotely, only if there is no option to attend in person.

The PAM is also responsible for ensuring that the appropriate subject matter experts are available (i.e., sales experts or engineers who normally perform customer demonstrations, relevant product managers for managed services, and operational staff).

Role of the Cisco Systems Engineer (SE)
Responsibilities of the Cisco SE include:
- Assisting the Cisco PAM and the partner in preparing for the audit.
- Approving the customer reference documentation (for Master specializations and Cisco Powered services) and then uploading it into the CSApp tool.
- Interfacing with the Cisco Certification Program Manager, the Cisco partner support representative and other stakeholders as appropriate.
- Co-managing the demonstration portion of the audit with the auditor.
- Identifying Cisco SMEs to participate in the evaluation of the Master demonstration.
- Working with SMEs to understand the program and applicability of technology requirements.

The SE assisting the auditor to evaluate the Master demo cannot be the SE assigned to the account or the SME preparing the partner for audit.

Role of the Cisco Subject Matter Expert (SME) for Master specializations and Cisco Powered services
A Cisco Subject Matter Expert (SME) is a highly skilled technical resource with specific knowledge in the subject Cisco technology to be audited (e.g., Unified Communications specialist for Master Collaboration specialization). This SME (CCIE, Product Sales Specialist, SE III, or Consulting Systems Engineer [CSE]) should work with the PAM to understand the program audit requirements and assist the partner in preparing for the technical portion of the audit, including demonstration. The SME should also aid the auditor during the onsite audit by offering perspective and context to the partner's responses and to assist the auditor in interpreting specific technical details to determine if the program requirements have been satisfied. It is recommended that the Cisco SME and auditor have a pre-audit meeting to discuss the scoring methodology that will be utilized to evaluate the audit (5-7 days prior to the audit).

Role of the Cisco Certification Program Manager (PM)
The Cisco Certification 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 get-well policies described within this document are at the discretion of the PM.

1.3 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 5 business days, the partner should provide a corrective action plan to the Cisco Certification Program Manager. The action plan must be fully implemented within an agreed upon time period, not to exceed the stated get-well period. At this time, the application status will be placed into Audit-Hold. 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 PAM can make commitments regarding the qualification decision. The Certification 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 requalification for the program cannot be achieved within the stated get-well period. In this case, the Certification Program Manager may deny qualification. If a partner fails to deliver an action plan within the agreed timeframe, the partner may also be denied qualification for the program.

1.4 Important Timelines

These timeline rules apply to all auditable applications:

- A partner is given an anniversary date when they are approved for the first time.
- A partner is required to fill out a recertification application each year.
- The status for that certification changes from "Approved" to "Re-cert" mode, 90 days prior to the anniversary date.
- Certification renewal reminder notices are sent 90 days, 60 days, and 30 days prior to a partner's certification anniversary date.
- Specialization notices are sent 90 days and 30 days prior to the specialization anniversary date.
- Specializations (non-auditable) which are not renewed by ten days post anniversary date will be automatically deleted from the system.
- A partner can submit their certification and/or Master specialization recertification application anytime during that renewal period but no later than 30 days after the anniversary date.
- If a partner does not submit a recertification application including all required documentation within 30 days from the anniversary date, the status is removed entirely.
- The audit must occur within 60 days of the partner's anniversary date; Cisco reserves the right to assign auditors based on availability.
- Audit cancellations by a partner must be communicated to Cisco no less than 15 business days prior to the audit otherwise. Audit will proceed as scheduled; the final decision is at the discretion of Certification Program Manager; audit cancellation fees will apply.
    - Greater than15 calendar days – 25% of audit cost
    - 15-11 calendar days – 50% of audit cost
    - Less than 10 calendar days – 100% of audit cost
    - All processes related to cancellation fees will be managed directly by the 3rd party auditing firm
- New program applications left unresolved for 90 days are deleted.
- Auditor sends audit summary to partner, PAM, and Certification Program Manager within 24 hours of audit.
- Partner has 5 business days to close any open action items with the auditor.
- Certification Program Manager has 20 business days from the receipt of the audit report to review the document and make a final decision, or to request more information from the partner during that time.
- An audit is valid for 180 days; this period may be extended if the Certification Program Manager initiates a get-well plan to address audit action items.
- If a new partner fails an audit, they will be required to wait 180 days from the previous audit date to re-submit an application.
- Certification is valid for 1 year (partner must remain in compliance throughout the year).
- No waiver of rights under the Cisco Channel Partner Program Audit and Policies by either party shall constitute a subsequent waiver of such right or any other right under the Cisco Channel Partner Program Audit and Policies.

1.5 Refusal to Certify

Cisco reserves the right, at its sole discretion, to deny certification to a Channel Partner applicant regardless of whether the applicant satisfies the substantive criteria set forth in the Cisco Channel Program Audit and Policies.

Pre-Qualification Requirements Overview

Requirement	Resale	
2.1 Resale Program Pre-Qualification	**G**	**S**
2.1.1 Personnel	•	•
2.1.2 Specializations	•	•
2.1.3 Agreements/Contracts	•	•
2.1.4 CSAT	•	•
2.1.5 Service Attach Rate	•	•
2.1.6 Revenue from Services	•	•
2.1.7 Hybrid IT Prerequisites	•	•

Requirement	Master Specialization		
2.2 Master Specialization Pre-Qualification	**Collab**	**Sec**	**CB**
2.2.1 Specializations	•	•	•
2.2.2 Personnel	•	•	•
2.2.3 Agreements/Contracts	•	•	•
2.2.4 Network Operations Center (NOC)	•	•	•
2.2.5 Training Requirements	•	•	•
2.2.6 Customer References	•	•	•
2.2.7 Demonstration	•	•	•
2.2.8 Third Party Credentials	N/A	N/A	•
2.2.9 Integrated Infrastructure	N/A	N/A	•
2.2.10 Proof of Value (POV)	N/A	•	N/A
2.2.11 Practice Areas	N/A	•	N/A

Requirement	Cloud & Managed Services		
2.3 CMSP Pre-Qualification	**M**	**A**	**E**
2.3.1 Personnel	•	•	•
2.3.2 Agreements/Contracts	•	•	•
2.3.3 Specializations	•	•	•
2.3.4 ATP Program	•	•	•
2.3.5 Network Operations Center (NOC)	•	•	•
2.3.6 Customer References	•	•	•
2.3.7 Service Offerings	•	•	•
2.3.8 SLA	•	•	•
2.3.9 Data Center	•	•	•

Resale: Gold (G), Silver (S); Master Specialization: Collaboration (Collab), Security (Sec); Cloud Builder (CB); Cloud & Managed Services: Master (M), Advanced (A), Express (E)

Pre-Qualification Requirements

2.1 Resale Program

NOTE: As of 1 April 2015, Cisco is no longer accepting new or recertifying Silver certification applications.

2.1.1 Personnel Applies to: G, S (See Table)

Gold: Partner must have a minimum of 12 unique certified full-time employees, including minimum 4 CCIEs*, one Business Value Practitioner; no more than 4 Cisco Sales Experts (CSEs) / Selling Business Outcomes (SBOs) can be counted toward the total. Individuals may also be allocated to specialization roles within program allowances if qualified to fill them; see requirements.
*50 percent of the CCIE requirement may be met with Cisco Certified Design Experts (CCDEs)

Silver: Partner must have a minimum of 6 unique certified full-time employees, including minimum 2 CCIEs*; no more than 2 Cisco Sales Experts (CSEs) / Selling Business Outcomes (SBOs) can be counted toward the total. Individuals may also be allocated to specialization roles within program allowances if qualified to fill them; see requirements.
*50 percent of the CCIE requirement may be met with Cisco Certified Design Experts (CCDEs)

NOTE: All Cisco certified personnel requirements must be satisfied by a unique full-time, regular certified employee residing in the country where certification/ specialization is sought and in good standing with Cisco. During the audit, the partner must provide evidence of full time employment for each individual playing a role in certifications and specializations. Certified individuals may associate themselves to a Cisco Learning Partner utilizing the Cisco Partner Self Service (PSS) tool for up to two weeks to ensure that their Certified Cisco Systems Instructor (CCSI) accreditation remains valid. Written confirmation from the partner's HR department must be uploaded within CSApp in the "Administrative Tasks" hyperlink. The documentation should be on the partner's company letterhead detailing the time period that they will be associated to the Learning Partner. The certified individual may only disassociate from the Channel Partner a maximum of four (4) times within a twelve month period to deliver training for a Learning Partner. Failure to comply with this policy will put the CCSI and the Channel Partner out of compliance and at risk for disqualification.

The only exception to this is for CCIEs/CCDEs. Partners may employ full-time contracted employees (not to exceed 50 percent of the required number of CCIEs/CCDEs) to fulfill the CCIE/CCDE 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) / Selling Business Outcomes (SBOs) requirement, the extra personnel must pass the sales expert exam or Selling Business Outcomes exam (available early 2015, required after Aug 1 2015).

2.1.2 Specializations Applies to: G, S (See Table)

Gold: Partner must hold four Advanced Architecture specializations: Advanced Enterprise Networks Architecture (required), Advanced Security Architecture (required), and two of the following: Advanced Collaboration Architecture, Advanced Data Center Architecture, Advanced Service Provider Architecture.

Silver:

- **Option 1:** Partner must hold any two of the following Advanced Architecture specializations: Enterprise Networks Architecture, Security Architecture, Collaboration Architecture, Data Center Architecture, Service Provider Architecture.

- **Option 2:** Partner must hold one Architecture: Advanced Enterprise Networks Architecture, Advanced Security Architecture, Advanced Collaboration Architecture, Advanced Data Center Architecture, Advanced Service Provider Architecture
  and one Advanced Technology specialization: Advanced Unified Fabric Technology, Advanced Unified Computing Technology

2.1.3 Agreements/Contracts Applies to: G, S (See Table)

Direct partners must have a valid resale support agreement with Cisco, including a Cisco Branded Services or a Partner Branded Services agreement. The support agreement must be accompanied by a valid Cisco product purchasing agreement, e.g., Systems Integrator or Indirect Channel Partner Agreement (ICPA).

In the Europe and Emerging Market regions (except Latin America), 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.

Partners who transition from one type of support contract or agreement to another during the certification term should contact their Channel Certification Program Manager to understand the impact on certification requirements. For direct partners, lack of a valid support agreement may result in immediate decertification. This also applies to indirect partners in the Europe and Emerging Market regions (except Latin America). For partners that sell both partner branded services and Cisco branded services, the partner branded services performance metrics will be used for certification purposes.

2.1.4 CSAT

Current CSAT Requirements which remain in effect through July 2015 (FY15) Applies to: G, S (See Table)

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

- Partner must use the Cisco Partner Access online (PAL) customer satisfaction tool on a regular basis to send surveys to current customers (those engaged within the past 12-24 months) and assess and act upon customer satisfaction results. See PAL tool for details.
- 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 ("partner sourced") and/or Cisco high-touch sales representatives ("Cisco sourced").
- Evidence of results analysis and reinforcement of best practices for customer satisfaction must be captured by the partner, including evidence that a closed loop process is being used 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 Silver or Gold certification, the following CSAT requirements apply:

- Minimum of 30 responses for Gold, 20 responses for Silver from Cisco sourced and partner sourced surveys in each country or country group where the partner is seeking certification; measurement will take place at the first measurement period (January or July) that occurs after a full six months of 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 will be measured on 30 valid responses at the first measurement period after a full six months of certification achievement.
- Partner must participate in the Low Score Follow Up process in PAL.
- Premier partners moving to either Silver or Gold certification must have a minimum of (30 for Gold, 20 for Silver) valid responses and meet the theater customer satisfaction target at the first measurement period that occurs after a full six months of certification achievement.
- If a partner falls out of compliance with the program requirements and is decertified within six months of submitting a new certification application, they will be treated as a recertifying partner and will be responsible for meeting the CSAT requirements.

For Silver or Gold re-certification, the following CSAT requirements apply:

- To ensure a reasonable and statistically significant measurement, a minimum of (30 for Gold, 20 for Silver) total valid responses is required from Cisco sourced and partner sourced surveys in each country or country group where the partner is seeking recertification; measurement will take place at the first measurement period (January or July) that occurs after a full six months of certification.
- Measurement is based on results from the prior 12-month period from the measurements dates: end of Cisco fiscal Q2 (January) and end of Cisco fiscal Q4 (July).
- Failure to meet the (30 for Gold, 20 for Silver) valid responses will be considered lack of participation and is grounds for decertification. 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.

CSAT abuse (including but not limited to sending surveys to non-customers) is considered a serious offense and will result in decertification.

New CSAT Requirements effective Aug 2015 (FY16) Applies to: G, S (See Table)

Partners must actively participate in the Cisco partner customer satisfaction survey process:

- January (Q2) measurement: Partner must use the Cisco Partner Access online (PAL) customer satisfaction tool to provide valid contact /email addresses for current customers (those engaged within the past 12-24 months) to receive a customer satisfaction survey.
- July (Q4) measurement: Partner must enter Follow-Up activities in the PAL tool for all low scores (1 or 2) received for the current fiscal year.
- Evidence of results analysis and reinforcement of best practices for customer satisfaction must be captured by the partner, including evidence that a closed loop process is being used for addressing customer issues raised in customer satisfaction surveys. Analysis must include review of the overall satisfaction Excel spreadsheet.

For new Silver or Gold certification, the following CSAT requirements apply:

- Participation in CSAT activities starting at the first measurement after a full six months of attaining Gold or Silver 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.
- Provide a minimum of (30 for Gold, 20 for Silver) valid customer contact/email addresses for the January (Q2) measurement. Partners will no longer be responsible for survey responses (all contact/email addresses must be entered by the Q2 measurement date).
- Participation in Low Score Follow Up process in PAL with activities to be completed by the July (Q4) measurement. Partner must enter Follow-Up activities in the PAL tool for all low scores (1 or 2) received for the current fiscal year.
- Premier or Silver Partners moving to Gold certification must provide a minimum of 30 valid customer contact/email addresses at the first January measurement period that occurs after a full six months of attaining Gold certification.
- If a partner falls out of compliance with the program requirements and is decertified, if they attain Certification again within six months, they will be treated as a recertifying partner and will be responsible for meeting the CSAT requirements at the next measurement period.

For Silver or Gold re-certification, the following CSAT requirements apply:

- Provide a minimum of (30 for Gold, 20 for Silver) valid customer contact/email addresses for the January (Q2) measurement. Partners will no longer be responsible for survey responses (all contact/email addresses must be entered by the Q2 measurement date).
- Participation in Low Score Follow Up process in PAL with activities to be completed by the July (Q4) measurement. Partner must enter Follow-Up activities in the PAL tool for all low scores (1 or 2) received for the current fiscal year.
- Failure to meet CSAT requirements will be considered lack of participation and is grounds for decertification. 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.

CSAT abuse (including but not limited to providing non-customer contact/email addresses) is considered a serious offense and will result in decertification.
Please Note: The PAL tool will not open on 01-AUG for the FY16 survey. More details to be announced on the CSAT website.

2.1.5 Service Attach Rate Applies to: G, S (See Table)

Applies to both Cisco branded services and partner branded 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. The service attach rate is calculated as follows:

$$\text{Attach Rate \%} = \frac{\text{Total \$ value of service sold (attached) in the measurement period*}}{\text{Total \$ value opportunity of service sales in the measurement}} \times 100$$

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 in the PMC tool (click on Scorecard tab).

The following requirements apply to the service attach rate:

- RMAs and spares are not included in this measurement.
- Direct and indirect service attach rate performance data can be found using the PMC tool within the metrics area (click on Scorecard tab).

2.1.6 Revenue from Services Applies to: G, S (See Table)

Applies to both Cisco branded services and partner branded services.

Partners must generate at least 15 percent of revenue from services during the prior two Cisco quarters. For example:

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

The revenue from services rate is calculated as follows:

$$\text{Revenue from Services \%} = \frac{\text{Total revenue of service sold (Managed, Professional Service, and SMARTnet}}{\text{Total product revenue of the networking division}} \times 100 = 15\%$$

Revenue from services must meet the following requirements:

- The percentage of revenue from all services (includes all vendors, does not have to be 100% Cisco specific) 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.

2.1.7 Hybrid IT Prerequisites Applies to: G, P (See Table)

The following prerequisites apply for Hybrid IT pertaining to provider contracts, service level agreements (SLA) and service marketing descriptions:

Cisco Cloud Services require a provider contract, an SLA and a service marketing description:

- If selling a Cisco Cloud Service and no provider contract is required, a partner must be able to provide documentation outlining the end to end lifecycle of the service to include who (either the service provider or the services reseller) owns the end customer support.
- If a partner is selling a Cisco Cloud Service and there is no end customer SLA held by the Services Reseller, documentation must be provided as to who holds the end customer SLA and provides end customer support.
    - A template is provided at www.cisco.com/go/audit to be completed as contract/SLA documentation for Cisco Cloud resell. This document should be uploaded with the Hybrid IT documentation in the SLA slot for Cisco Cloud services.
- A Service Marketing description document

Cisco Powered Cloud and Cisco Powered Managed Services require a provider contract, an SLA and a service marketing description:

A Services Reseller Partner must have a provider contract and an SLA with the Services Provider if selling a Cisco Powered Cloud Service or Cisco Powered Managed Service. For additional information, please refer to the Cisco Powered Managed and/or Cloud Reseller Policy.

If the Services Reseller does not hold the SLA with the end customer because the Services Provider holds the SLA, this should be clearly defined in the agreement between the Services Reseller and the Services Provider.

- A template is provided at www.cisco.com/go/audit to be completed as contract/SLA documentation for Cisco Cloud resell. This document should be uploaded with the Hybrid IT documentation in the SLA slot for Cisco Powered Cloud or Cisco Powered Managed services.
- A Service Marketing description document

If the Services Provider is a CMSP Partner and the Services Reseller is a certified location of the CMSP Partner, a contract is not required; however, documentation to support the internal process must be provided to include full end customer support such as: ownership and management of the SLA, point of contact, change management protocol and escalations.

Cisco Based Partner Created Services require an SLA and a service marketing description plus additional documentation:

- If selling a partner's own Cisco Based Partner Created Service no provider contract should be required; however, a partner must be able to provide documentation outlining the end to end lifecycle of the service to include the end customer support process. Templates have been provided at www.cisco.com/go/audit to consolidate the required documentation and upload into the CSApp application.
- Partner must provide an end customer SLA. A signed SLA is preferred; however a generic SLA will be accepted.
- Partner must provide a marketing document that includes the service description, which may be any collateral used to market, explain and sell the service to the end customer.
- Providers:
  - A provider can be an external relationship with a services provider OR
  - A provider can be an internal relationship if the partner is an approved CSMP partner.
    - (e.g. of an internal relationship: a CMSP partner may have been audited in Germany where the NOC or Data Center resides and may have a Gold or Premier Certified location in India that will be reselling their CMSP Cisco Powered Services. The Germany location would be the provider)

Cisco Based Partner Created Service Required Documentation

Cisco Based Validation
The documentation (listed below) should be uploaded into the CSApp application to provide an overview of the Cisco Based service. Templates have been provided at www.cisco.com/go/audit. Once uploaded, this particular Hybrid IT will show requirements as met. Please note that the Cisco Based service will be validated by a 3rd party auditing firm. The auditing firm will determine if the service meets the intent of Cisco Based. You may be contacted to provide additional information if necessary.

- Network Topology (for the particular Cisco Based Service only)
- List of tools (tools used for monitoring and managing) Service
- ITIL Certified Individual
- Service Marketing descriptions
- Service Level Agreement (SLA)
- Service Process Documents for 1 Plan, 1 Build, 2 Manage Cisco Based Validation (see table below)

Plan (Choose 1)	Build (Choose 1)	Manage (Choose 2)
Design Document	Disaster Recovery Plan and Testing	Service Desk Reports including KPIs
Lab topology and reservation process	Change Management Process	Escalation Process
Project Management Process	Service Level Measurement and Reporting	Examples of a Case – end to end to include change request; RMA/TAC; Call Back; Auto Escalated incident; proactive and reactive management
Customer Training	Capacity Management	Incident Management
Demand Management	Release and Deployment Management	Problem Management
	NW Readiness Assessment Example	Remote Troubleshooting Access

2.2 Master Specializations

2.2.1 Specializations

Applies to: Collab, Sec, CB (See Table)

Master Collaboration: Partner must have the Advanced Collaboration Architecture specialization.
Master Security: Partner must have the Advanced Security Architecture specialization.
Master Cloud Builder: Partner must have the Advanced Data Center Architecture specialization.

2.2.2 Personnel Applies to: Collab, Sec, CB (See Table)

Master Collaboration: Partner must have personnel to satisfy the roles for Collaboration Architecture, plus:

- 1 CCIE Voice (or CCIE Collaboration)
- 1 PMP/Prince II (specific to UC)

Master Security: Partner must have personnel to satisfy the roles for Advanced Security Architecture specialization, plus:

- 1 CCIE Security*
- 1 CCNP Security*
- 1 Fire Jumper – see Appendix 7
- 1 PMP/Prince II

*must be unique individuals

Master Cloud Builder: Partner must have personnel to satisfy the roles for the Advanced Data Center Architecture specialization, plus the appropriate personnel to maintain third party credentials as noted in 2.2.8 below.

All Cisco certified personnel requirements must be satisfied by a unique certified, full-time, regular employee residing in the country where certification/specialization is sought and in good standing with Cisco. During the audit, partner must provide evidence of full time employment for each individual playing a role in certifications and specializations.

2.2.3 Agreements/Contracts Applies to: Collab, Sec, CB (See Table)

Partner must have a purchasing agreement with Cisco, e.g., Systems Integrator or Indirect Channel Partner Agreement (ICPA).

2.2.4 Network Operations Center (NOC) Applies to: Collab, CB (See Table)

Master specialization evaluates a partner's capabilities based on IT service management standards and ITIL service desk functionality. Partners must provide objective evidence of their ability to meet the requirements; compliance does not require the physical presence of a network operations center (NOC).

If the auditor is unable to physically visit the NOC at the time of the audit, partner must ensure that the auditor is aware of this restriction prior to the audit. In the event that an auditor visit is not possible, partner must provide:

- Live video or feed into the NOC
- Access to all tools
- Quick state of the union presentation for the NOC and its capabilities

Additional information that will be reviewed:

- Job descriptions (e.g., what skills are required to work in the NOC?)
- List of NOC tools
- Evidence of 24x7 capability
- Live onsite visit (if possible)

2.2.5 Training Requirements Applies to: Collab, Sec, CB (See Table)

Master Collaboration: There are no incremental training requirements beyond the training requirements in the Advanced Collaboration Architecture specialization.

Master Security: There are no incremental training requirements beyond the training requirements in the Advanced Security Architecture Specialization.

Master Cloud Builder: Partner must complete the Virtual Workspace (VXI) Foundation training. Partner must meet Virtual Workspace (VXI) Foundation training requirements by:

1) Uploading the appropriate Citrix or VMware desktop virtualization credentials using the CSApp document upload process.
2) Uploading a completed and signed Training Verification template into CSApp as proof of completion of the online training modules.
3) Allocating Cisco prerequisites AM, SE, and FE job roles using the role allocation functionality in CSApp.

2.2.6 Customer References Applies to: Collab, Sec, CB (See Table)

Master Collaboration: Prior to the audit being scheduled, partner must submit documentation for 5 direct reference accounts (3 reference accounts for Master specialization renewal) demonstrating complex deployments including third party integration. Each submission must contain the Master Security and Collaboration Customer Reference Checklist.

Partner should work with the Cisco Systems Engineer (SE) to collect and submit the required documents into the CSApp tool. The SE must verify the customer reference documentation prior to uploading into CSApp. Partner may use the same customer reference account for requalification only if there is a new sale within that account that meets the current criteria.

Master Security: Same as Master Collaboration, except:
- Partner may use same customers for proof of value (POV) and customer reference accounts.
- Partner must submit documentation for 3 partner executed POVs.
- Each submission must contain the Master Security Customer Reference Checklist.

Master Cloud Builder: Prior to the audit being scheduled, partner must submit documentation for 3-7 direct reference accounts demonstrating complex deployments including third party integration. Each submission must contain the Master Cloud Builder Customer Reference Checklist.

Partner should work with the Cisco Systems Engineer (SE) to collect and either:
1) sign the document for the partner contact to upload into CSApp, or
2) submit these documents into the CSApp tool.

The SE must verify the customer reference documentation prior to uploading into CSApp. Partner may use the same customer reference account for requalification only if there is a new sale within that account that meets the current criteria.

2.2.7 Demonstration Applies to: Collab, Sec, CB (See Table)

Collaboration: Based on a provided customer scenario, OR a real customer deal that would meet demonstration objectives, partner must demonstrate and present solutions that solve customer technical, business and financial requirements. See Master Collaboration Solution Customer Scenario and Demo Guideline.

Security: Based on a provided customer scenario, OR a real customer deal that would meet demonstration objectives, partner must demonstrate and present solutions that solve customer technical, business and financial requirements. Demonstration is limited to 3 hours. See Master Security Solution Customer Scenario and Demo Guideline.

Cloud Builder: Based on a provided customer scenario, OR a real customer deal that would meet demonstration objectives, partner must demonstrate and present solutions that solve customer technical, business and financial requirements. Demonstration is limited to 6 hours. See Master Cloud Builder Solution Customer Scenario and Demo Guideline.

2.2.8 Third party Credentials Applies to: CB (See Table)

Master Cloud Builder: Using CSApp's document upload procedure, partner must upload documented proof of active certifications in one or more of the following:

Virtualization:
- VMware — Enterprise or Premier Certification
- Redhat — Premier or SI Certification
- Citrix — Gold or Platinum Certification
- Microsoft – Silver or Gold Certification

Storage:
- EMC – Velocity Partner with Consolidate or Advanced Consolidate
- NetApp – Gold or Platinum or Star
- Hitachi Data Systems – Gold or Platinum

2.2.9 Integrated infrastructure (Computer, Storage, and Network Components) Applies to: CB (See Table)

Master Cloud Builder: Customer solutions must be based on Cisco's integrated infrastructure stacks: Vblock, FlexPod, ExpressPod, and/or VIA-HDS. Validation will be part of customer reference requirements, as well as demonstration requirements where partners will showcase their knowledge of the infrastructure stacks, how to build, order, and install – including third party integration within the overall solution.

Prior to scheduling the audit, partner must indicate which of the following options (minimum 1, maximum 4) they wish to have audited and consequently recognized following approval: Vblock, FlexPod, ExpressPod, and/or VIA-HDS.

The integrated infrastructure selection must also correspond to the appropriate third-party credentials for storage and virtualization/hypervisor.

2.2.10 Proof of Value (POV) Applies to: Sec (See Table)

Master Security: Partner or Cisco SE must upload Proof of Value (POV) Assessment documentation (examples of POV Best Practices may be found at https://communities.cisco.com/docs/DOC-55882).

These customers may be from among the 5 deployment customer reference accounts or they may be different customers.

2.2.11 Practice Areas Applies to: Sec (See Table)

Master Security: Partner must validate proficiency in three (3) practice areas from among the six (6) available areas. See Appendix 7.

2.3 Cloud and Managed Services Program (CMSP)

2.3.1 Personnel Applies to: M, A, E (See Table)

Master: Partner must have the following personnel:

- Minimum 1 individual with Information Technology Infrastructure Library (ITIL) v2 or v3 Foundation certificate
- Minimum 1 CCIE (of any technology specialty)
- NOC personnel to ensure that NOC service is available 24x7x365
- Personnel and any required specializations for Cisco Powered service(s) offered

Advanced: Partner must have the following personnel:

- Minimum 1 individual with Information Technology Infrastructure Library (ITIL) v2 or v3 Foundation certificate
- Minimum 1 CCxP (CCDP, CCNP, CCIP, CCNP Security, CCNP Voice, CCNP Wireless, CCNP Data Center); may be superseded by higher level certification (e.g. - a CCIE may supersede a CCxP)
- NOC personnel to ensure that NOC service is available 24x7x365
- Personnel and any required specializations for Cisco Powered service(s) offered

Express: Partner must have the following personnel:

- Minimum 1 individual with Information Technology Infrastructure Library (ITIL) v2 or v3 Foundation certificate
- Minimum 1 CCNA (of any technology specialty); may be superseded by higher level certification
- NOC personnel to ensure that NOC service is available 24x7x365
- Personnel and any required specializations for Cisco Powered service(s) offered

All Cisco certified personnel requirements must be satisfied by a unique full-time, regular employee. During the audit, partner must provide evidence of full time employment for each certified individual.

The CMSP certified personnel requirements are at the company level and must be met in order to be considered for Master, Advanced, or Express. Individual Cisco Powered services may have their own additional requirements. If the individual satisfying the company level requirement has, or exceeds, the Cisco Powered service requirement, this person will fulfill both requirements.

For CMSP Advanced level, if the partner plans to offer only Cisco Powered Business Video or Cisco Powered TelePresence-as-a-Service (TPaaS), partner has the option to have either a CCxP or an individual who has passed the required exams (refer to current version of the Cloud and Managed Services Program Audit and Policies Document; see section 2.3.1 for list of exams).

2.3.2 Agreements/Contracts Applies to: M, A, E (See Table)

Partner must have a purchasing agreement with Cisco, e.g., Systems Integrator or Indirect Channel Partner Agreement (ICPA) in the countries where they wish to transact. This includes the requirement for the partner to register each partner location at www.cisco.com/go/partnerregistration.

During the application process, partners will be required to “click to accept” the CMSP Terms and Conditions (see Appendix 5). Partners enrolled in CMSP must abide by the terms of their service support agreements (e.g., for Cisco branded services or partner branded services) and must maintain at least the minimum service requirements to remain in the services program.

If partner has outsourced NOC operations, partner must have an executed, documented contract and signed SLA with penalties with a NOC services provider detailing end-to-end accountability and process for management support. Partner must also upload a NOC integrated process plan during the application process. (See Appendix 6; requirements will be reviewed in their entirety at the time of the audit.)

2.3.3 Specializations Applies to: M, A, E (See Table)

Specializations are required as referenced in Cisco Powered services. See Cisco Powered Cloud and Managed Services Portfolio Requirements; product restrictions vary by Cisco theater. Contact your Cisco Partner Account Manager (PAM) for more information on restricted products.

2.3.4 ATP Program Applies to: M, A, E (See Table)

Authorized Technology Partner (ATP) program certification is required for any restricted products (e.g., UCCE ATP is required for UCC Enterprise products and TelePresence ATP is required for TelePresence products). Product restrictions vary by Cisco theater. Contact your Cisco Partner Account Manager (PAM) for more information on restricted products. Partners are responsible for applying and acquiring the appropriate Cisco specialization and/or ATP to access restricted products for resale, or Cloud and Managed Services.

2.3.5 Network Operations Center (NOC) Applies to: M, A, E (See Table)

Partner may own and operate a physical or virtual network operations center (NOC) through which Cisco Powered services are offered, or may outsource NOC operations to a NOC services provider. (Partner may or may not own NOC assets.)

Partner must have policies, processes, and provide NOC(s) functions to ensure a globally consistent customer experience for Cisco Powered services.

Partner must select a location for the audit during the application process at which they are able to show how NOC requirements are being met. If NOC location is at a different site, partner must show auditor evidence of remote access to the NOC. This may be the partner location with access to NOC or a service provider's NOC.

Together, partner and NOC services provider must meet NOC requirements and must have personnel to ensure that NOC service is available 24x7x365. The auditor will review job descriptions (e.g. what skills are required to work in the NOC), a list of NOC tools, evidence of 24x7 capability and visit onsite (if possible)

Providing the auditor with a list of tools that are used in the NOC is a best practice. See Appendix 6; requirements will be reviewed in their entirety at the time of the audit).

2.3.6 Customer References Applies to: M, A, E (See Table)

Partner must submit two customer references for each Cisco Powered service offered by completing the Cloud and Managed Services Partner Customer Reference Validation customer reference template. Evidence will be validated during the audit.

Partners applying for new Cisco Powered cloud services are required to provide customer references at the next recertification, rather than at the initial audit.

2.3.7 Service Offerings Applies to: M, A, E (See Table)

Master: Partner must have at least 2 Cisco Powered service offerings.

Partner must upload the following documents for each Cisco Powered service:

- Marketing description
- Completed customer reference template with 2 customers listed
- Service level agreement (SLA)

Partner must provide point of sale (PoS) information of sold Cisco Powered cloud services for cloud compensation.

Advanced: Partner must have at least 1 Cisco Powered service offering.

Partner must upload the following documents for each Cisco Powered service:

- Marketing description
- Completed customer reference template with two customers listed
- Service level agreement (SLA)

Partner must provide point of sale (PoS) information of sold Cisco Powered cloud services for cloud compensation.

Express: Partner must have 2 Cisco-based cloud or managed service offerings.

A Cisco-based managed service is:

- an offer where the key features of the service are provided by Cisco device(s), or a network-based service is built on Cisco infrastructure, AND

- the service includes monitoring and management of Cisco equipment owned or leased by the customer (Cisco end points or customer premises equipment).

A Cisco-based cloud service is a cloud-based service built on Cisco reference architecture; see examples at the Cisco Design Zone.

2.3.8 Customer Service Level Agreement (SLA) Applies to: M, A, E (See Table)

Partner must upload a currently active, signed service level agreement (SLA) for each Cisco Powered service.

The uploaded SLA should:
- be signed by a customer,
- include terms of more than 1 year, and
- describe service obligations.

If an active SLA is not available, a generic SLA is acceptable.

2.3.9 Data Center (DC) Applies to: M, A, E (See Table)

Partner must own or lease the products that are required to build a multi-tenant cloud infrastructure for a Cisco-based data center to offer Cisco Powered cloud services, except TelePresence-as-a-Service (TPaaS). The physical location of the data center may be owned by the partner, rented, or leased.

Program Requirements Overview

Requirement	Resale		Master Specialization			Cloud & Managed Services		
	G	S	Collab	Sec	CB	M	A	E
Cisco Lifecycle Services: Plan								
3 Pre-Sales Requirements								
3.1 Support Lab								
3.1.1 General Requirements	•	•	•	•	•	•	•	•
3.2 Demonstration and Demand Generation								
3.2.1 Solution Demonstration	•	•	•	•	•	•	•	•
3.2.2 Demand Generation	N/A	N/A	N/A	N/A	•	N/A	N/A	N/A
3.3 Project Management								
3.3.1 Personnel	•	•	•	•	•	•	•	•
3.3.2 Project Plan	•	•	•	•	•	•	•	•
3.3.3 Project Objectives	•	•	•	•	•	•	•	•
3.3.4 Project Charter	•	•	•	•	•	•	•	•
3.3.5 Resource Management	•	•	•	•	•	•	•	•
3.3.6 Customer Requirements	•	•	•	•	•	•	•	•
3.3.7 Project Start Meeting	•	•	•	•	•	•	•	•
3.3.8 Risk Management	•	•	•	•	•	•	•	•
3.3.9 Project Milestones	•	•	•	•	•	•	•	•
3.3.10 Customer Communication Plan	•	•	•	•	•	•	•	•
3.3.11 Project Implementation	•	•	•	•	•	•	•	•
3.3.12 Project Review and Evaluation	•	•	•	•	•	•	•	•
3.4 Design								
3.4.1 Network Design Process	•	•	•	•	•	•	•	•
3.4.2 Design Documents	•	•	•	•	•	•	•	•
3.5 Hiring and Internal Training								
3.5.1 Training Plans	•	•	•	•	•	•	•	•
3.5.2 Training Records	•	•	•	•	•	•	•	•
3.5.3 List of Required Personnel	•	•	•	•	•	N/A	N/A	N/A
3.6 Post-Implementation Customer Training								
3.6.1 Customer Training Process	•	•	•	•	•	•	•	•
4 Service Strategy Requirements								
4.1 IT Financial Management								
4.1.1 Budgeting and Financial Planning Processes	N/A	N/A	•	N/A	•	•	•	•
4.2 Service Portfolio Management								
4.2.1 Portfolio Management Process	N/A	N/A	•	N/A	•	•	•	•
4.3 Demand Management								
4.3.1 Demand Management Process	N/A	N/A	•	N/A	•	•	•	•
Cisco Lifecycle Services: Build								
5 Service Design Requirements								
5.1 Service Catalog Management								
5.1.1 Information about Services Offered	N/A	N/A	•	N/A	•	•	•	•
5.1.2 Professional Services	N/A	N/A	N/A	N/A	•	N/A	N/A	N/A
5.1.3 Service Catalog Maintenance	N/A	N/A	•	N/A	•	•	•	•
5.1.4 Service Catalog Updates	N/A	N/A	•	N/A	•	•	•	•
5.2 Service Level Management								
5.2.1 SLAs/SLOs	•	•	•	N/A	•	•	•	•

Requirement	Resale		Master Specialization			Cloud & Managed Services		
5.2.2 Service Level Measurement and Reporting	●	●	●	N/A	●	●	●	●
5.2.3 Parts Replacement	●	●	●	N/A	●	●	●	●
5.3 Capacity Management								
5.3.1 Business Capacity	N/A	N/A	●	N/A	●	●	●	●
5.3.2 Service Capacity	N/A	N/A	●	N/A	●	●	●	●
5.3.3 Resource Capacity	N/A	N/A	●	N/A	●	●	●	●
5.3.4 Capacity Improvements	N/A	N/A	●	N/A	●	●	●	●
5.4 Availability Management								
5.4.1 Availability Measurement	N/A	N/A	N/A	N/A	N/A	●	●	●
5.4.2 Availability Reporting	N/A	N/A	N/A	N/A	N/A	●	●	●
5.4.3 Availability Review and Planning	N/A	N/A	N/A	N/A	N/A	●	●	●
5.4.4 Availability Improvements	N/A	N/A	N/A	N/A	N/A	●	●	●
5.5 IT Service Continuity/Disaster Recovery								
5.5.1 IT Infrastructure Monitoring	N/A	N/A	●	N/A	●	●	●	●
5.5.2 IT Infrastructure Problem Resolution	N/A	N/A	●	N/A	●	●	●	●
5.5.3 Service Continuity/Disaster Recovery Planning	N/A	N/A	●	N/A	●	●	●	●
5.5.4 Disaster Recovery Plan Testing	N/A	N/A	●	N/A	●	●	●	●
5.6 Information Security Management **If partner maintains current registration to ISO 27001, the requirements for Information Security Management will be waived.**								
5.6.1 Security Policies and Procedures	●	●	●	●	●	●	●	●
5.6.2 Physical Security	●	●	●	●	●	●	●	●
5.6.3 Network Security	●	●	●	●	●	●	●	●
5.6.4 Server Security	●	●	●	●	●	●	●	●
5.6.5 Logical Data Security	●	●	●	●	●	●	●	●
5.7 Hybrid IT								
5.7.1 Provider Management	●	●	N/A	N/A	N/A	N/A	N/A	N/A
5.7.2 End Customer Relationship	●	●	N/A	N/A	N/A	N/A	N/A	N/A
5.7.3 Hybrid IT Resell Methodology Review	●	●	N/A	N/A	N/A	N/A	N/A	N/A
5.8 Third Party Contracting (referenced by ITIL as Supplier Management)								
5.8.1 Third Party Contracted Activities and Services	●	●	N/A	N/A	N/A	●	●	●
5.8.2 Subcontractor Management	●	●	N/A	N/A	N/A	●	●	●
5.8.3 Subcontractor Contracts	●	●	N/A	N/A	N/A	●	●	●
5.8.4 Subcontractor Communication	●	●	N/A	N/A	N/A	●	●	●
5.8.5 Periodic Subcontractor Reviews	●	●	N/A	N/A	N/A	●	●	●
6 Service Transition Requirements								
6.1 Transition Planning and Support								
6.1.1 Risk Management	N/A	N/A	N/A	N/A	N/A	●	●	●
6.1.2 Redundant Management Connection	N/A	N/A	N/A	N/A	N/A	●	●	●
6.2 Change Management								
6.2.1 Change Management Process	●	●	●	N/A	●	●	●	●
6.2.2 Change Rollback	N/A	N/A	●	N/A	●	●	●	●
6.2.3 Requests for Changes	N/A	N/A	●	N/A	●	●	●	●
6.2.4 Change Definitions	N/A	N/A	●	N/A	●	●	●	●
6.2.5 Standard Change Turnaround Time	N/A	N/A	N/A	N/A	N/A	●	●	●
6.2.6 Customer-Specific Change Control	N/A	N/A	●	N/A	●	●	●	●
6.2.7 Change Manager and Change Advisory Board	N/A	N/A	●	N/A	●	●	●	●
6.2.8 Change Management Tools	N/A	N/A	●	N/A	●	●	●	●
6.3 Release and Deployment Management								
6.3.1 Release and Deployment Process	N/A	N/A	●	N/A	●	●	●	●

Requirement	Resale		Master Specialization			Cloud & Managed Services		
6.3.2 Phased Release	N/A	N/A	•	N/A	•	•	•	•
6.3.3 Configuration Item (CI) Identification	N/A	N/A	•	N/A	•	•	•	•
6.3.4 Software and Hardware Repositories	N/A	N/A	•	N/A	•	•	•	•
6.3.5 Release Management Audits	N/A	N/A	•	N/A	•	•	•	•
6.4 Service Asset and Configuration Management								
6.4.1 Data Collection Process	N/A	N/A	N/A	N/A	N/A	•	•	•
6.4.2 Configuration Control Processes and Tools	N/A	N/A	N/A	N/A	N/A	•	•	•
6.4.3 Configuration Change Plans	N/A	N/A	N/A	N/A	N/A	•	•	•
6.5 Service Validation and Testing								
6.5.1 Service Validation and Testing Process	N/A	N/A	N/A	N/A	N/A	•	•	•
6.6 Service Evaluation								
6.6.1 Service Evaluation Process	N/A	N/A	N/A	N/A	N/A	•	•	•
6.7 Service Knowledge Management								
6.7.1 Information Availability and Accessibility	N/A	N/A	•	N/A	•	•	•	•
Cisco Lifecycle Services: Manage								
7 Service Operation Requirements								
7.1 Service Desk Function (Call/Contact Center)								
7.1.1 Customer Service Availability	•	•	•	N/A	•	•	•	•
7.1.2 Local Language Answering	•	•	•	N/A	•	•	•	•
7.1.3 One-Hour Callback	•	•	•	N/A	•	•	•	•
7.1.4 Call Logging	•	•	•	N/A	•	•	•	•
7.1.5 Incident Severity Level	•	•	•	N/A	•	•	•	•
7.1.6 Escalation Process	•	•	•	N/A	•	•	•	•
7.1.7 After-Hours Support	•	N/A	•	N/A	•	•	•	•
7.1.8 Service Desk Duty Manager	•	•	•	N/A	•	•	•	•
7.1.9 Computer-Based Call Tracking System	•	•	•	N/A	•	•	•	•
7.2 Request Fulfillment								
7.2.1 Service Request Process	•	•	•	N/A	•	•	•	•
7.2.2 Automated Service Request Tool	N/A	N/A	N/A	N/A	N/A	•	•	•
7.3 Event Management								
7.3.1 Event Management Process	•	•	•	N/A	•	•	•	•
7.4 Incident Management								
7.4.1 Incident Management Process	•	•	•	N/A	•	•	•	•
7.4.2 Managed Device Monitoring	N/A	N/A	N/A	N/A	N/A	•	•	•
7.4.3 Fault and Performance Data Monitoring	N/A	N/A	N/A	N/A	N/A	•	•	•
7.4.4 Management Platform	N/A	N/A	N/A	N/A	N/A	•	•	•
7.4.5 Event Correlation	N/A	N/A	N/A	N/A	N/A	•	•	•
7.4.6 Incident Detection	N/A	N/A	•	N/A	•	•	•	•
7.4.7 Incident Logging and Querying	N/A	N/A	•	N/A	•	•	•	•
7.4.8 Customer Notification	N/A	N/A	•	N/A	•	•	•	•
7.4.9 Notification Methods	N/A	N/A	•	N/A	•	•	•	•
7.4.10 Incident Prioritization and Categorization	N/A	N/A	•	N/A	•	•	•	•
7.4.11 Stakeholder Updates	N/A	N/A	•	N/A	•	•	•	•
7.4.12 Incident Troubleshooting and Investigation	N/A	N/A	•	N/A	•	•	•	•
7.4.13 Handoff to Problem Management	N/A	N/A	•	N/A	•	•	•	•
7.4.14 Known Error Database	N/A	N/A	•	N/A	•	•	•	•
7.4.15 Incident Closure Authorities	N/A	N/A	•	N/A	•	•	•	•
7.4.16 Incident Closure Summary	N/A	N/A	•	N/A	•	•	•	•

Requirement	Resale		Master Specialization			Cloud & Managed Services		
7.5 Problem Management								
7.5.1 Problem Management Process	●	●	●	N/A	●	●	●	●
7.5.2 Root Cause Analysis	●	●	●	N/A	●	●	●	●
7.5.3 Closed Loop Corrective Action	●	●	●	N/A	●	●	●	●
7.5.4 Proactive Problem Management	N/A	N/A	●	N/A	●	●	●	N/A
7.6 Access Management								
7.6.1 Access Management Process	N/A	N/A	●	N/A	N/A	●	●	●
7.7 Onsite Response/Troubleshooting								
7.7.1 Onsite Response/Troubleshooting Description	●	●	●	N/A	●	●	●	●
7.8 Remote Troubleshooting Access								
7.8.1 Remote Access	N/A	N/A	N/A	N/A	N/A	●	●	●
8 Continual Service Improvement Requirements								
8.1 Service Improvement								
8.1.1 Continual Improvement Activities	●	●	●	N/A	●	●	●	●
8.1.2 Continual Improvement Methodology	●	●	●	N/A	●	●	●	●
8.2 Service Measurement								
8.2.1 Service Objectives	●	●	●	N/A	●	●	●	●
8.2.2 Mean Time to Notify (MTTN)	N/A	N/A	●	N/A	●	●	●	●
8.2.3 Mean Time to Restore Service (MTRS)	N/A	N/A	●	N/A	●	●	●	●
8.2.4 Onsite Troubleshooting Response Time	●	●	●	N/A	●	●	●	●
8.2.5 Customer Perception and Feedback	●	●	●	N/A	●	●	●	●
8.3 Service Reporting								
8.3.1 Service Reports	N/A	N/A	●	N/A	●	●	●	●
8.3.2 Cloud or Managed Service Contracts	N/A	N/A	N/A	N/A	N/A	●	●	●

Cisco Lifecycle Services: Plan

3 Pre-Sales Requirements

3.1 Support Lab

3.1.1 General Requirements Applies to: G, S, Collab, Sec, CB, M, A, E (See Table)

Partner must have a support lab for proof of concept, post-sales support, and training, in the country seeking certification.

Support lab must meet the following requirements:

- 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, and the 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.

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.

NOTE 1: This requirement does not apply to Gold and Silver partners who have a Cisco Branded Services (CBS) contract (i.e.: those who only sell Cisco SMARTnet and do not operate in a co-branded or shared support model) or partners with an approved CoE. However, Gold and Silver "CBS or SMARTnet only" partners applying for Master specializations or CMSP must meet all requirements outlined in this section, regardless of their service support agreement type, due to the intent and capabilities represented by these designations.

NOTE 2: Master Cloud Builder lab can be anywhere, so long as the lab setup can support the business and be readily accessed remotely.

NOTE 3: CMSP partners offering cloud services may use a virtualized lab to demonstrate this requirement.

3.2 Demonstration and Demand Generation

3.2.1 Solution Demonstration Applies to: G, S, Collab, Sec, CB, M, A, E (See Table)

Partner must deliver a demonstration of a solution or a managed or cloud service based on Cisco equipment. A role-play scenario will be employed to carry out the demonstration, where the auditor plays the role of the potential customer and the partner is the organization demonstrating the solution.

The demonstration will take into account the following:

- Partner's knowledge of the customer business requirements and customer needs
- Partner's knowledge of the Cisco technology and/or solution
- Use of the Cisco equipment
- Quality of the presentation material used
- Presentation skills observed during the demonstration
- Overall impression created

The auditor will assess the demonstration and provide an appraisal against each skill using a scoring matrix, and will rate each skill as "Attention Required, Satisfactory, Good or Outstanding." A score of "Attention Required" in one or more area will result in an action item.

Where considered appropriate the auditor will recommend action to be taken should an issue not meet the normally accepted standards. Reasons will be given for each action item.

In addition to the above the auditor will also check for the following:

- The demonstration facility and the quality of the equipment used

- The demonstration equipment or virtualized cloud solution being present at time of audit
- Establishing that the partner has demonstration equipment or virtualized cloud solution available that is sufficient for the partner to demonstrate effectively Cisco solutions
- The process to reserve demonstration rooms for that specific technology
- The process of assigning of pre-sales technical staff to customer demonstrations

NOTE 1: Gold and Silver partners must not demonstrate the same solution for two successive audit years. A demonstration may not be required for recertification audits, as determined and documented by the Certification Program Manager.

NOTE 2: Master specialized partners must complete a demonstration using either the pre-defined customer scenario or one of their own to develop a demonstration that incorporates the criteria defined in the Demonstration Checklist. Master Security Specialized Partners may utilize dCloud as a demo option. However, dCloud is not currently available for use in satisfying the Master Cloud Builder demonstration requirements because it does not support all Integrated Infrastructure vendors or options. Also, dCloud is not available for use in satisfying the Master Collaboration demonstration requirements at this time because it does not support all Collaboration technology configurations. Cisco will continue to evaluate its suitability for future use as additional functionality becomes available for these two technologies. Master demonstration will be evaluated and scored as described in the Master Collaboration, Master Security, or Master Cloud Builder Demonstration Checklist.

NOTE 3: CMSP partners must review Cisco Powered Cloud and Managed Services Portfolio Requirements for demonstration requirements, and must be prepared to demonstrate:
- *The business value of the cloud or managed service based on Cisco technology*
- *Technical knowledge of the Cisco solutions being sold*

If the laboratory equipment or virtualized cloud solution is based at a different location, there must be adequate access to that lab equipment in order to perform a credible demonstration

3.2.2 Demand Generation Applies to: CB (See Table)

Master Cloud Builder Specialized partners must have a process to create demand for their offers.

This must include process to conduct customer workshops; run demand generation campaigns, and other marketing activities to showcase the cloud professional services offered by the partner. During the audit, partner must explain what the customer workshops entail, and detail any demand generation campaigns current or previous, outlining goals of the campaign.

3.3 Project Management

NOTE: Requirements for project management (3.3.1-3.3.12) do not apply for CMSP partners who offer one or a combination of the following services only: Cisco Powered IaaS, Cisco Powered DaaS, Cisco Powered DRaaS, Cisco Powered Cloud Cell Architecture for SAP HANA, Cisco Powered FnSaaS, or Cisco Powered HSS.

3.3.1 Personnel Applies to: G, S, Collab, Sec, CB, M, A, E (See Table)

Project Manager must be PMP or Prince certified, or must have two years project management experience.

Partner must provide evidence of Project Manager qualification, either by individual certification or by sample projects and/or project management education hours or credits. NOTE: PMP or Prince certification is required for Master Collaboration and Master Security specializations.

If the Business Value Practitioner has been certified for at least 3 months at the time of the audit, the auditor will review status of one business case and any architectural roadmaps that are in place. The goal is to see how the role is being implemented into the business, not just the project management, but the overall strategic business.

3.3.2 Project Plans Applies to: G, S, Collab, Sec, CB, M, A, E (See Table)

Partner must provide 2-3 customer-specific project plans based on a consistent template for deploying a solution that includes Cisco advanced technologies in a customer environment completed within 24 months.

The provided project plans must include evidence of the requirements listed in 3.3.3-3.3.12.

3.3.3 Project Objectives Applies to: G, S, Collab, Sec, CB, M, A, E (See Table)

Project objectives must reference how the Cisco solution addresses a customer need, problem, or request.

Partner must explain how project objectives are defined and documented, e.g., in a project plan or other document.

Master Cloud Builder Specialized partners must provide evidence of at least 1 project plan for a complete private cloud solution that covers implementation and setup of cloud management.

3.3.4 Project Charter Applies to: G, S, Collab, Sec, CB, M, A, E (See Table)

A project charter is a statement of the scope, objectives, and participants in a project. It provides a preliminary delineation of roles and responsibilities, outlines the project objectives, identifies the main stakeholders, and defines the authority of the project manager. It serves as a reference of authority for the future of the project.

Partner must develop a project charter, including governance with key stakeholders. Partner must describe how the project charter is included in the project plan.

3.3.5 Resource Management Applies to: G, S, Collab, Sec, CB, M, A, E (See Table)

Resource management includes:

- Allocating qualified resources and their skill levels
- Monitoring and management of resource utilization

Partner must provide evidence of resource management; evidence may be in Gantt charts and/or cross-reference to credentials for the individuals assigned to the project.

3.3.6 Customer Requirements Applies to: G, S, Collab, Sec, CB, M, A, E (See Table)

Customer requirements must be clearly documented, including detailed specifications, e.g., request for proposal (RFP), request for quotation (RFQ), or request for information (RFI). Project plans must address operational requirements and technical specifications.

Partner must explain how customer requirements are detailed in project plans.

3.3.7 Project Start Meeting Applies to: G, S, Collab, Sec, CB, M, A, E (See Table)

The project start meeting is the first meeting with the project team and the client. This meeting introduces the members of the project team and the client and provides the opportunity to discuss the role of each team member.

An internal and external meeting must be conducted at the beginning of the project; records of this meeting must be maintained.

3.3.8 Risk Management Applies to: G, S, Collab, Sec, CB, M, A, E (See Table)

Project management must include identification and mitigation of project risks, as well as identification of actions to be taken throughout the project.

Partner must describe how action items are tracked, e.g., in an action item list or log/register to track action ownership, assigned date, due date, and closure.

3.3.9 Project Milestones Applies to: G, S, Collab, Sec, CB, M, A, E (See Table)

Milestones mark the end of a stage or completion of a significant deliverable. Milestones allow project management to more accurately determine whether or not the project is on schedule.

Partner must explain how milestones are tracked (e.g., in a project plan).

3.3.10 Customer Communication Plan Applies to: G, S, Collab, Sec, CB, M, A, E (See Table)

The customer communication plan is a methodology for notifying customer of any changes during the project.

Partner must explain how customer communication plans are developed.

3.3.11 Project Implementation Applies to: G, S, Collab, Sec, CB, M, A, E (See Table)

Partner must provide evidence of project implementation activities.

Records of implementation may include evidence of implementation standards by which partner installs, cables, labels, and powers equipment during implementation (not customer-specific).

3.3.12 Project Review and Evaluation Applies to: G, S, Collab, Sec, CB, M, A, E (See Table)

Partner must have processes for project review and evaluation.

Examples of project review processes include:

- Peer review of deliverables as needed
- Deliverable/milestone signoff with customer
- Posting of all project content to a designated repository
- Project closure, including user acceptance testing (UAT), and customer training process
- Post-project review and lessons learned
- Review of customer satisfaction/feedback
- Review of project profitability

Partner must describe how project review and evaluation is completed.

3.4 Design

NOTE: Requirements for Design (3.4.1-3.4.2) do not apply for CMSP partners who offer one or a combination of the following services only: Cisco Powered IaaS, Cisco Powered DaaS, Cisco Powered DRaaS, Cisco Powered Cloud Cell Architecture for SAP HANA, Cisco Powered FnSaaS, or Cisco Powered HSS.

3.4.1 Network Design Process Applies to: G, S, Collab, Sec, CB, M, A, E (See Table)

Partner must have a process for building a network design for a customer describing how requirements are specified, how design activities are planned, and how designs are reviewed to ensure that requirements are met.

Partner must describe how network design is accomplished, e.g., in a documented procedure/flowchart, or a detailed explanation of the design process.

NOTE: CMSP partners offering cloud service(s) must demonstrate how virtualized environment is provisioned and accomplished.

3.4.2 Design Documents Applies to: G, S, Collab, Sec, CB, M, A, E (See Table)

Partner must maintain documented evidence of design activities, including customer-specific examples of network designs from projects completed in the previous 12-24 months.

Design documents must include:

- Review and verification of customer requirements including existing/new application requirements
- Review all sizing requirements and design assumptions
- Network Readiness Assessment Plan: Partner's methodology to assess the existing network architecture
- Proposed system design
- Physical or virtualized design specifications
- Details of the management and measurement systems
- Network security policies and procedures: partner's methodology used to assess the customer's security policies and procedures; documented report of customer's existing network security, and gap identification

3.5 Hiring and Internal Training

3.5.1 Training Plans Applies to: G, S, Collab, Sec, CB, M, A, E (See Table)

Partner must provide evidence of documented training plans for internal personnel, including:

- 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

3.5.2 Training Records Applies to: G, S, Collab, Sec, CB, M, A, E (See Table)

Partner must provide evidence of internal training records, e.g., Human Resources records, training certificates, etc.

3.5.3 List of Required Personnel Applies to: G, S, Collab, Sec, CB (See Table)

Partner must maintain a current listing of required personnel; records must be maintained of all individuals fulfilling the required roles, including any certification and specialization roles where appropriate.

3.6 Post-Implementation Customer Training

3.6.1 Customer Training Process Applies to: G, S, Collab, Sec, CB, M, A, E (See Table)

Partner must have processes for providing customer training for new technology, and must explain or show how customer training is developed and made available to customers. Records of customer training activities must be provided.

NOTE: CMSP partners offering cloud service(s) may demonstrate customer training on how customers are able to utilize their portal to provision services; e.g., by showing how customers request incremental computer and/or memory resources.

4 Service Strategy Requirements

4.1 IT Financial Management

4.1.1 Budgeting and Financial Planning Processes Applies to: Collab, CB, M, A, E (See Table)

Partner must have processes for budgeting and financial planning. Financial management processes may include methods for budgeting, accounting, charging and billing activities related to the services provided.

Partner must provide evidence that financial management processes are in place.

4.2 Service Portfolio Management

4.2.1 Portfolio Management Process Applies to: Collab, CB, M, A, E (See Table)

The service portfolio is the complete set of services, including services in the pipeline (proposed or in development), active services (in the service catalog), and retired services. The range of services offered must be managed in order to ensure that business value is provided; that is, new services must be evaluated, existing services modified, and older services retired as appropriate.

Partner must have processes for managing the entire set of services that are offered.

Business plans or other similar planning records may be provided as evidence of service portfolio management.

4.3 Demand Management

4.3.1 Demand Management Process Applies to: Collab, CB, M, A, E (See Table)

Partner must have processes for managing demand for services.

Partner must understand and influence customer demand and provide capacity to meet those demands. This may include analysis of business activity patterns, server demand and user profiles, or differential charging to encourage customers to use specific services at less busy times.

Business plans, marketing plans or other similar planning records may be provided as evidence of demand management.

Master Cloud Builder Specialized partners must show connection between their demand generation activities, and their ability to scale to the capacity or demand created. This plan must include scalability of qualified personnel for the creation of customer designs, qualified personnel capable of installing/implementing the integrated infrastructure, as well as ability to meet customer timeframes; which includes lead times on equipment, and allocation of resources appropriately.

Cisco Lifecycle Services: Build

5 Service Design Requirements

5.1 Service Catalog Management

5.1.1 Information About Services Offered Applies to: Collab, CB, M, A, E (See Table)

Partner must provide information about services offered.

Detailed information about the services offered must be created and maintained; information must be accessible, e.g., in a published datasheet or presentation.

NOTE: Not exempt from gap audit for Master specialization partners. During a gap audit, partner must still show the relevant information pertaining to the technology being audited. For example, partner must show cloud-specific professional services for Master Cloud Builder requirements, and collaboration-specific services for Master Collaboration requirements.

5.1.2 Professional Services Applies to: CB (See Table)
Partner must describe which professional services are offered.

Professional services offer high margins to Master Cloud Builder Specialized partners; thereby maximizing their profitability and creating unique differentiation in this space.

During the audit, Master Cloud Builder Specialized partner must show auditor documentation outlining the specific professional services offered. Common professional services in this market include: readiness assessments, design services, application consultation, and others.

Managed services or post-sales support services are not eligible to fulfill this requirement.

5.1.3 Service Catalog Maintenance Applies to: Collab, CB, M, A, E (See Table)
Partner must maintain a service catalog.

For each service offered, the following information must be available: Service activities, deliverables, service level agreements (SLAs) or service level objectives (SLOs) and customer responsibilities.

During a gap-audit, partners must still show the relevant information pertaining to the technology being audited. For example, partner must show cloud-specific professional services for Cloud Builder requirements, and Collaboration-specific services for Collaboration requirement.

5.1.4 Service Catalog Updates Applies to: Collab, CB, M, A, E (See Table)
Partner must have a process for updating the service catalog.

The process for updating service information must include ownership, alignment and, if necessary, re-negotiation of SLAs, with customers, partners, and vendors that are tied to all managed service offerings.

Evidence of service catalog updates must be provided.

NOTE: Not exempt from gap audit for Master specialization partners. During a gap audit, partner must still show the relevant information pertaining to the technology being audited. For example, partner must show cloud-specific professional services for Master Cloud Builder requirements, and collaboration-specific services for Master Collaboration requirements.

5.2 Service Level Management

5.2.1 SLAs/SLOs Applies to: G, S, Collab, CB, M, A, E (See Table)
Partner must provide service level agreements (SLAs) or service level objectives (SLOs) to customers.

Service level agreements (SLAs) are agreement between the partner and customer specifying the responsibilities of the partner and define service level targets. SLAs are typically included in a service contract, but may also be a standalone document.

Service level objectives (SLOs) outline the objectives agreed upon by the partner and customer specifying the responsibilities of the partner. SLOs may or may not include penalties for missed targets, but do outline the responsibility and recourse for customers.

Partner must provide evidence of actual customer SLAs or SLOs for the services offered.

NOTE 1: This requirement does not apply to Gold and Silver partners who have a Cisco Branded Services (CBS) contract (i.e.: those who only sell Cisco SMARTnet and do not operate in a co-branded or shared support model) or partners with an approved CoE. However, Gold and Silver "CBS or SMARTnet only" partners applying for Master specializations or CMSP must meet all requirements outlined in this section, regardless of their service support agreement type, due to the intent and capabilities represented by these designations.

NOTE 2: Master Cloud Builder Specialized partners must show post-implementation agreements with customer showing post-deployment responsibilities for software and hardware upgrades, and ongoing maintenance. Alternately, Master Cloud Builder partners must show handoff process and contractual agreements if customer is assuming responsibility for the infrastructure and third-party applications post-implementation.

5.2.2 Service Level Measurement and Reporting Applies to: G, S, Collab, CB, M, A, E (See Table)

Partner must have a process for measuring and reporting of service level performance metrics.

A recurring review (recommended weekly or monthly) must be conducted to review metrics related to the ability of the organization to deliver the services. Review must include data directly related to specific SLAs, SOWs or Project Agreements under contract for customers, partners, and vendors tied to all services offered.

Partner must explain or show how service level metrics are measured or reviewed; records of reviews must be provided.

NOTE 1: This requirement does not apply to Gold and Silver partners who have a Cisco Branded Services (CBS) contract (i.e.: those who only sell Cisco SMARTnet and do not operate in a co-branded or shared support model) or partners with an approved CoE. However, Gold and Silver "CBS or SMARTnet only" partners applying for Master specializations or CMSP must meet all requirements outlined in this section, regardless of their service support agreement type, due to the intent and capabilities represented by these designations.

NOTE 2: If Master Cloud Builder Specialized partner shows proof of customer transfer (and is not responsible for changes or upgrades post-implementation as indicated in 5.2.1), this requirement is not applicable.

NOTE 3: CMSP partners offering cloud service(s) must explain or show how capacity planning and change management processes are employed for their cloud-based services.

5.2.3 Parts Replacement Applies to: G, S, Collab, CB, M, A, E (See Table)

Partner must provide evidence of a parts replacement/spares program (e.g., spares inventory, spares process, records), or a support contract with Cisco (e.g., SMARTnet).

NOTE 1: If Master Cloud Builder Specialized partner shows proof of customer transfer (and is not responsible for changes or upgrades post-implementation indicated in 5.2.1), this requirement is not applicable.

NOTE 2: Not required for CMSP partners offering one or a combination of the following services only: Cisco Powered IaaS, Cisco Powered DaaS, Cisco Powered DRaaS, Cisco Powered Cloud Cell Architecture for SAP HANA, Cisco Powered FnSaaS, Cisco Powered HSS or Cisco Powered TPaaS (when the TPaaS partner is not supplying the Customer Premises Equipment-CPE).

NOTE 3: Gold, Silver, and Master specialization partners may subcontract this requirement; requirements for Third Party Contracting apply (see 5.8).

5.3 Capacity Management

5.3.1 Business Capacity Applies to: Collab, CB, M, A, E (See Table)

Capacity management is the discipline that ensures IT infrastructure is provided at the right time in the right volume at the right price, and ensuring that IT is used in the most efficient manner. Business capacity management includes capacity planning, assessments and projections for current and future business needs.

Partner must explain or show how business capacity is measured and monitored in order to forecast capacity needs based on business events, including describing or demonstrating how capacity review, planning, analysis, and change management is conducted.

5.3.2 Service Capacity Applies to: Collab, CB, M, A, E (See Table)

Service capacity management ensures that capacity levels support established service level targets.

Partner must explain or show how service capacity is monitored, including describing or demonstrating how capacity management, review, planning, and analysis are conducted.

5.3.3 Resource Capacity Applies to: Collab, CB, M, A, E (See Table)

Resource capacity management ensures that capacity levels are provided for at the individual IT device level (i.e., Cisco devices). For some components, capacity may refer to size or volume, such as bandwidth or memory utilization.

Partner must explain or show how resource capacity is measured and monitored at the device level, including describing or demonstrating how capacity review, planning, and analysis are conducted.

5.3.4 Capacity Improvements Applies to: Collab, CB, M, A, E (See Table)
The primary goal of capacity management is to proactively ensure that IT capacity meets current and future business requirements in a cost-effective manner.

Partner must show how internal recommendations for improvement of performance and capacity are developed, reviewed, and executed on an ongoing basis (e.g., in a stewardship report).

NOTE: If Master Cloud Builder Specialized partner shows proof of customer transfer (and is not responsible for changes or upgrades post-implementation as indicated in 5.2.1), this requirement is not applicable.

5.4 Availability Management

5.4.1 Availability Measurement Applies to: M, A, E (See Table)
Availability indicates the ability of a managed service or component to perform to its agreed function when required. Availability is typically calculated as a percentage.

Partner must explain or show how the availability of all managed components and sub-systems is measured.

5.4.2 Availability Reporting Applies to: M, A, E (See Table)
Partner must report on the availability of managed components and sub-systems; reports must be made available to customers.

Partner must provide sample service or application performance reports (e.g., uptime reports, unscheduled and scheduled outage reports) as well as evidence that reports have been provided to customers.

5.4.3 Availability Review and Planning Applies to: M, A, E (See Table)
Partner must provide evidence of availability review and planning, and must explain how trend analysis is used to identify any potential availability issues, e.g., in a recurring review meeting.

5.4.4 Availability Improvements Applies to: M, A, E (See Table)
Partner must provide recommendations for availability improvements to the customer, e.g., in a stewardship report. Partner must describe how recommendations for improvement will be provided to the customer, and must provide sample recommendation reports if available.

5.5 IT Service Continuity/Disaster Recovery

NOTE: If Master Cloud Builder Specialized partner shows proof of customer transfer (and is not responsible for changes or upgrades post-implementation as indicated in 5.2.1), these requirements (5.5.1-5.5.4) are not applicable.

5.5.1 IT Infrastructure Monitoring Applies to: Collab, CB, M, A, E (See Table)
Monitoring of internal systems (e.g., of the OSS/NOC management system and platforms) is done to ensure that the partner's infrastructure does not compromise services provided to customers.

Partner must describe or show how the availability, capacity, and performance of the IT infrastructure are monitored.

5.5.2 IT infrastructure Problem Resolution Applies to: Collab, CB, M, A, E (See Table)
Partner must have a documented process for responding to issues that arise from the monitoring of internal systems.

Partner must explain or show how internal IT issues are resolved when an incident is found with internal systems that may present a risk to IT services; this may include the use of incident, , change, and release management procedures.

5.5.3 Service Continuity/Disaster Recovery Planning Applies to: Collab, CB, M, A, E (See Table)
Partner must have a documented service continuity/disaster recovery plan defining the steps required to recover one or more IT services or to recover from NOC outages, in order to support customer SLAs in the event of a disaster or outage.

Service continuity may be accomplished by having redundant, linked NOCs, via distributed service desk operators that have secondary access to service desk tools in the event of a failure, or by a contracted relationship with another provider to support service continuance.

5.5.4 Disaster Recovery Plan Testing Applies to: Collab, CB, M, A, E (See Table)
Partner must test the service continuity/disaster recovery plan at least annually. Periodic testing of the service continuity/disaster recovery plan ensures that it remains feasible and current.

Records of testing to be provided as evidence, e.g., in a lab environment simulating an actual outage or disruption in service.

If partner is provided with an audit waiver during the year, they will be required to upload evidence of periodic testing at the time of re-certification. This documentation will also be reviewed by the auditor at the time of audit.

5.6 Information Security Management

If partner maintains current registration to ISO 27001, the requirements for Information Security Management will be waived.

5.6.1 Security Policies and Procedures Applies to: G, S, Collab, Sec, CB, M, A, E (See Table)

Partner must have documented security policies and procedures in place to protect the internal environment from threats that may compromise the ability to provide services to the customer.

Security policies and procedures must be

- approved by management,
- communicated to all employees and relevant outside parties, and
- periodically reviewed and tested for suitability, adequacy, and effectiveness

5.6.2 Physical Security Applies to: G, S, Collab, Sec, CB, M, A, E (See Table)

Partner must have methods and procedures for maintaining physical security, and must describe or show how physical security is maintained.

Physical security may include 24x7 video monitoring, badge access, security guards, and physical access controls.

5.6.3 Network Security Applies to: G, S, Collab, Sec, CB, M, A, E (See Table)

Partner must have methods and procedures for maintaining network security, and must describe or show how network security is maintained.

Network security includes firewalls, intrusion detection, web proxy, access control lists, VPN routing and forwarding, access control server, and security event monitoring system.

5.6.4 Server Security Applies to: G, S, Collab, Sec, CB, M, A, E (See Table)

Partner must have methods and procedures for maintaining server security, and must describe or show how server security is maintained.

Server security may include server hardening, anti-virus, host intrusion prevention, and patch management.

5.6.5 Logical Data Security Applies to: G, S, Collab, Sec, CB, M, A, E (See Table)

Partner must have methods and procedures for maintaining logical data security, and must describe or show how network security is maintained.

Data security includes digital certificates, strong passwords, file access controls, endpoint security, and online privacy.

NOTE: the requirements for Information Security Management will be waived for partners who maintain a current registration to ISO 27001. The ISO 27001 must be completed for the country that is being audited and include the ISO 27001 Security element as part of the ISO certification.

5.7 Hybrid IT

5.7.1 Provider Management

Applies to: G (See Table)

Partner must have a documented contract with the services provider.

If selling a Cisco Cloud Service and there is no provider contract, partner services reseller must provide documentation or describe which activities are the responsibility of the provider and which are the responsibility of the reseller. Contracts or process documentation must include service level agreements (SLAs) and ownership of SLA; records of contract approval or documentation updates must be maintained.

Clearly defined processes are to include an escalation process that identifies roles and responsibilities and points of contact.

Partner must have defined criteria for evaluation and selection of services providers. Provider selection criteria may be defined in a checklist or other document. Providers must be periodically re-evaluated to ensure that requirements, including SLAs (if applicable), are being met.

- Records of provider evaluations and re-evaluations must be provided as evidence.
- Partner must have a documented process for notifying services *providers when requirements, including SLAs (if applicable), are not met; corrective action to resolve the problem must be tracked and records maintained.
- Periodic business reviews are recommended with services providers in order to ensure that both parties are satisfied.

**NOTE: Provider - a provider may be Cisco, a CMSP partner with Cisco Powered Service offerings or a partner selling their own Cisco Based Power Service. The provider documentation will be dependent upon which services provider that the partner utilizes to meet the Hybrid IT requirements. All provider documentation should outline the service responsibilities, including escalation process, between the entities.*

5.7.2 End Customer Relationship

Applies to: G, S (See Table)

Partner must have a documented contract or SLA with the end customer. Service level agreements (SLAs) and other records of contract approval must be maintained.

Partner must have a documented process for managing the lifecycle of the end customer relationship. This must include a description of how end customers are notified when requirements, including SLAs, are not met, and how corrective actions are tracked and records maintained. Periodic reviews with end users must include documented assessments to evaluate the relationship and provide recommendations for improvements to include additional service options and availability. Quarterly business reviews are recommended with end customers in order to ensure that both parties are satisfied.

If the services reseller does not hold an SLA with the end customer because the services provider hold the end customer contract/SLA, documentation must be provided that clearly outlines the SLA ownership and responsibilities.

5.7.3 Hybrid IT Resell Methodology Review

Applies to: G, S (See Table)

Partner must provide an end-to-end sales cycle documentation overview or a demonstration that represents how they resell a service to an end customer. Partner may describe the process or provide a marketing plan as evidence or demonstrate by selling the service to the auditor.

The Hybrid IT resale within the certification program is about the recurring income model and the business outcome discussions partners have with end customers.

Recommended elements to include in documentation:

- What is your process to engage with the end customer periodically to offer a resale service or to an additional resale service(s)?
- What is your process for renewal? Is it annual? Is it automatic or do you proactively reach out to the end customer?
- Do you offer additional service benefits to further sell service adoption?
- Do you measure and review satisfaction and include the review discussions with end customer?
- Do you engage the service provider to partner in the discussions with the end customer?

5.8 Third Party Contracting (referenced by ITIL as Supplier Management)

5.8.1 Third Party Contracted Activities and Services

Applies to: G, S (See Table)

Partner must define which, if any, activities or services needed to meet program requirements are subcontracted to a third party. Subcontracting of requirements does not absolve the partner of the responsibility to ensure that all applicable requirements are met.

The following requirements may be subcontracted:

- **5.2.3 Parts Replacement**: Requirements for parts replacement may be subcontracted by Gold, Silver, and Master Specialization partners only
- **7.1.1-7.1.9 Service Desk Function (Call/Contact Center):** Requirements for Service Desk functions may be subcontracted by any partner, assuming that the following minimum requirements are also met:
- The subcontracted party must receive phone calls in the local language through the partner's published servicer telephone number for the country.

- The subcontracted party must have appropriate access to the partner's computer-based call tracking system to allow for immediate logging of customer calls.
- The subcontracted party must be able to contact partner engineers or management and transfer customer phone calls to the partner as appropriate.
- Follow up on logged cases must remain the responsibility of the partner, including subsequent call tracking and management, troubleshooting, case updates, escalation and alerts, and case closure.
- The subcontracted party must have procedures to guarantee that customers will receive technical support as stipulated in their service contract; procedures must include requirements for escalation of problems.
- The subcontracted party must have methods for notification of the partner, during normal business hours, of all calls received during the previous after-hours or holiday period.
- Subcontracted party engineers must be qualified for on-site hardware replacement services, as applicable. Partner must provide details regarding the training and skill level of the engineers subcontracted to support Cisco products. *(NOTE: Not required for CMSP partners offering one or a combination of the following services only: Cisco Powered IaaS, Cisco Powered DaaS, Cisco Powered DRaaS, Cisco Powered Cloud Cell Architecture for SAP HANA, Cisco Powered FnSaaS, Cisco Powered HSS or Cisco Powered TPaaS (when the TPaaS partner is not supplying the Customer Premises Equipment-CPE).*

NOTE: For Resale (Gold/Silver) partner branded services, technical support operation must remain in-house with the partner and cannot be subcontracted to a third party. Technical support refers to Level 2 or higher support activity; see Appendix 1 for detailed description of support levels.

5.8.2 Subcontractor Management Applies to: G, S, M, A, E (See Table)
Partner must have defined criteria for evaluation and selection of suppliers/subcontractors. Supplier selection criteria may be defined in a checklist or other document. Subcontractors must be periodically re-evaluated to ensure that requirements, including SLAs, are being met.

Partner must describe or show how suppliers/subcontractors are evaluated and selected, and re-evaluated. Records of supplier/subcontractor evaluations and re-evaluations must be provided as evidence.

5.8.3 Subcontractor Contract Applies to: G, S, M, A, E (See Table)
Partner must have a documented contract with the supplier/contracted company.

Contracts must include SLAs; records of contract approval must be maintained.

5.8.4 Subcontractor Communication Applies to: G, S, M, A, E (See Table)
Partner must have a documented process for notifying suppliers/subcontractors when requirements, including SLAs, are not met; subcontractor corrective action to resolve the problem must be tracked and records maintained.

5.8.5 Periodic Subcontractor Reviews Applies to: G, S, M, A, E (See Table)
Partner must conduct periodic reviews with the supplier/subcontractor to evaluate the relationship. Quarterly business reviews are recommended in order to ensure that both parties are satisfied.

Partner must provide evidence of periodic supplier reviews, and must explain or show how any issues resulting from these reviews are resolved.

6 Service Transition Requirements

6.1 Transition Planning and Support

6.1.1 Risk Management Applies to: M, A, E (See Table)
Service transition refers to the introduction of new services, changes to existing services, change of supplier, decommission or discontinuation of services or service components, or the implementation of fundamental changes to the service. Risk identification and mitigation is essential to ensuring a successful transition of services in the operational business environment.

Partner must identify, manage, and control risks in order to prevent failure and disruption during transition activities. Partner must provide evidence that risks are identified and controls are established as necessary, during the planning stage. Evidence may be in the form of a risk management matrix or other list of identified risks.

6.1.2 Redundant Management Connection Applies to: M, A, E (See Table)

A redundant management connection between the partner and the customer site provides failover monitoring in case the primary management connection terminates.

Partner must provide evidence that a redundant management connection is available as an option to customers, e.g., in a sample statement of work.

NOTE: Not required for CMSP partners offering one or a combination of the following services only: Cisco Powered IaaS, Cisco Powered DaaS, Cisco Powered DRaaS, Cisco Powered Cloud Cell Architecture for SAP HANA, Cisco Powered FnSaaS, or Cisco Powered HSS.

6.2 Change Management

6.2.1 Change Management Process Applies to: G, S, Collab, CB, M, A, E (See Table)

Change management is the process responsible for controlling the lifecycle of all changes, from change request through implementation and review.

Partner must have a documented process for managing changes, and must describe how changes are made, including how change requests are recorded, evaluated, authorized, prioritized, planned, coordinated and implemented, documented, and closed. Records of changes must be shown as evidence of the process.

6.2.2 Change Rollback Applies to: Collab, CB, M, A, E (See Table)

A change rollback is executed when a change fails, in order to reset the environment to the last known good state or configuration. Rollback plans must be in place prior to execution of a change.

Partner must have a process for rolling back changes when necessary, and must describe how rollback is accomplished by providing examples of rolled back changes, if available.

6.2.3 Requests for Changes Applies to: Collab, CB, M, A, E (See Table)

A request for change (RFC) is a formal proposal for a change to be made, and may be recorded on paper or electronically.

RFCs must include details of the proposed change, including 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. Information must be sufficient to maintain traceability for all changes related to additions, modifications, or deletions of any software or hardware, including version and release control.

Partner must provide examples of in-process and completed RFCs.

6.2.4 Change Definitions Applies to: Collab, CB, M, A, E (See Table)

Partner must have clear definitions for standard and non-standard changes. Definitions must be documented, e.g., in change management procedures.

6.2.5 Standard Change Turnaround Time Applies to: M, A, E (See Table)

Partner must offer 24-hour turnaround for standard changes.

Partner must describe the process for capturing and completing standard change requests, and for addressing standard changes within 24 hours of request from the customer.

6.2.6 Customer-Specific Change Control Applies to: Collab, CB, M, A, E (See Table)

If a customer requests that a specific change management process be followed, there must be a process for ensuring that the customer's process is recorded and available when needed. Users must be aware of how to access and use customer-specific change control processes.

Unique customer requirements may 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.

Partner must explain how customer-specific change processes are handled; examples of unique requirements must be shown.

6.2.7 Change Manager and Change Advisory Board Applies to: Collab, CB, M, A, E (See Table)
Partner must have evidence of change ownership, including a single owner (Change Manager) and a cross-functional group (Change Advisory Board) for reviewing and managing changes, and for analysis and assessment of routine activities before they are treated as standard changes.

Partner must provide a responsibility matrix, job descriptions, or other identification of responsibility for change management.

6.2.8 Change Management Tools Applies to: Collab, CB, M, A, E (See Table)
Partner must provide evidence that tools (e.g., ticketing system) are used to manage changes; may be off-the-shelf or custom developed tools and/or scripts that automate portions of the process.

Instructions must be available describing how to use change management tools; users must demonstrate knowledge and awareness of how to use the tools.

6.3 Release and Deployment Management

6.3.1 Change Management Process Applies to: Collab, CB, M, A, E (See Table)
Release and deployment management is the process for planning, scheduling and controlling the movement of releases (hardware, software, or documentation) to test and production environments to a customer.

Partner must have a documented process for managing software and hardware release and deployment; procedure(s) must include planning, preparation, build and test, service testing/pilots, transfer, and deployment.

6.3.2 Phased Release Applies to: Collab, CB, M, A, E (See Table)
Partner must define how releases are developed, tested, accepted and installed in a production environment.

Partner must provide evidence of a phased release process, from development through installation, e.g., in a documented procedure.

6.3.3 Configuration Item (CI) Identification Applies to: Collab, CB, M, A, E (See Table)
Partner must identify configuration items (CI) 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.

Partner must explain or show how CIs are identified during the release process, and must provide records of completed releases including release documentation.

6.3.4 Software and Hardware Repositories Applies to: Collab, CB, M, A, E (See Table)
Partner must keep software and hardware documentation in repositories, e.g., Definitive Software Library (DSL) and Definitive Hardware Store (DHS), in order to control revisions and to prevent unauthorized movement of releases.

Partner must show how software and hardware repositories are used.

6.3.5 Release Management Audits Applies to: Collab, CB, M, A, E (See Table)
Partner must conduct audits to determine whether releases have followed the release management process.

Partner must explain how audits are conducted to ensure that releases are completed according to applicable procedures. Records of audits must be provided, including evidence that corrective actions are initiated when discrepancies are found.

6.4 Service Asset and Configuration Management

6.4.1 Data Collection Process Applies to: M, A, E (See Table)
Partner must have a data collection process for capturing and managing critical information and data (service assets and configuration information).

The data collection process must include all necessary network details and managed component details that are required for activating managed services.

Partner must explain or show how the data collection and management process works; this includes describing how asset and configuration information is identified, recorded, stored, and revised/updated when necessary. This may include providing a documented process or demonstration of a tool.

6.4.2 Configuration Control Processes and Tools Applies to: M, A, E (See Table)
Partner must have processes and tools that provide for effective control of configurations for managed devices.

For Cisco Series router/switches under management, partner must perform a back-up process that includes demonstrating that they have the correct read/write access privileges, a process to access and store configurations, and a process to restore a service by uploading a stored configuration. Configurations must be stored in an active database or file server.

For Cisco Collaboration applications under management, partner must provide leading best practice recommendations to customer in support of customer backup of Cisco UC servers. This includes providing scheduling recommendations for performing backups. Partner must have a process or tool to monitor the availability of the backup service executable (.exe) on Cisco UC servers under management. Partner must have the correct read/write access privileges and process to restore a service by uploading a configuration backup.

6.4.3 Configuration Change Plans Applies to: M, A, E (See Table)
Partner must have documented configuration change plans.

Configuration changes must be managed to ensure that configuration item data remains current; no CI should be added, modified, replaced, or removed without appropriate documentation of the change.

Partner must provide evidence that CI stakeholders are assigned, with defined roles for updating of CI information.

6.5 Service Validation and Testing

6.5.1 Service Validation and Testing Process Applies to: M, A, E (See Table)
Service validation and testing ensures that deployed services meet customer expectations, and verifies that IT operations are able to support the new service.

Partner must have a documented process for validation and testing activities, including acceptance testing procedures or other QA processes. Records of testing activities and customer signoff must be provided.

6.6 Service Evaluation

6.6.1 Service Evaluation Process Applies to: M, A, E (See Table)
Service evaluation considers whether the performance of the service is acceptable, and whether it is providing the expected value to the customer.

Partner must have a process for ensuring that the performance and value of the service remains acceptable to the customer. Evidence of service evaluation activities, e.g., records of periodic customer meetings, must be provided.

6.7 Service Knowledge Management

6.7.1 Information Availability and Accessibility Applies to: Collab, Sec, CB, M, A, E (See Table)
Knowledge management includes processes and tools for gathering, storing, and providing access to information related to service operations.

Partner must provide evidence that relevant service information is available and accessible, e.g., in databases or tools. This may include known error databases, knowledge bases, etc. Partner must explain or show how information is gathered, stored, and accessed.

Cisco Lifecycle Services: Manage

7 Service Operation Requirements

7.1 Service Desk Function (Call/Contact Center)

NOTE 1: Requirements for service desk (7.1.1-7.1.9) do not apply to Gold and Silver partners who have a Cisco Branded Services (CBS) contract (i.e.: those who only sell Cisco SMARTnet and do not operate in a co-branded or shared support model) or partners with an approved CoE. However, Gold and Silver "CBS or SMARTnet only" partners applying for Master specializations or CMSP must meet all requirements outlined in this section, regardless of their service support agreement type, due to the intent and capabilities represented by these designations.

NOTE 2: Gold/Silver Requirements for service desk (7.1.1-7.1.9) may be subcontracted; requirements for third party contracting apply (see 5.8).

7.1.1 Customer Service Availability Applies to: G, S, Collab, CB, M, A, E (See Table)
Partner must provide evidence that customer service is available 24x7, over internet-based systems, phone, fax, pager, or email.

NOTE: For Silver partners only, availability requirement is reduced to 8x5.

7.1.2 Local Language Answering Applies to: G, S, Collab, CB, M, A, E (See Table)
Partner must have a published customer service number that is in-country; this should preferably be a toll free number, and must be answered in the local language.

7.1.3 One-Hour Callback Applies to: G, S, Collab, CB, M, A, E (See Table)
Partner must provide one-hour callback in the local language, from a technical resource.

7.1.4 Call Logging Applies to: G, S, Collab, CB, M, A, E (See Table)
Partner must provide evidence that all calls are immediately logged upon initial communication with the customer.

7.1.5 Incident Severity Level Applies to: G, S, Collab, CB, M, A, E (See Table)
Partner must provide evidence that problem severity/priority is established by the customer and recorded as part of the call handling process.

7.1.6 Escalation Process Applies to: G, S, Collab, CB, M, A, E (See Table)
Partner must have a documented and robust escalation process through the partner management structure and, when necessary, to Cisco, and must explain or show how escalations are handled.

Documented escalation procedure(s) must address the following:
- Definition of customer calls by priority/severity
- 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)

NOTE: Although a call center is not required for Gold and Silver partners using Cisco branded services, CBS partners are still required to have an escalation process (e.g. Technical Assistance Center).

7.1.7 After-Hours Support Applies to: G, Collab, CB, M, A, E (See Table)
Partner must provide after-hours support and must explain how it is provided.

If 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. Partner must also provide evidence that support engineers have write access to the call-tracking system to log after-hours calls.

7.1.8 Service Desk Duty Manager Applies to: G, S, Collab, CB, M, A, E (See Table)
Partner must provide evidence of a duty manager or equivalent staff position for the Service Desk.

7.1.9 Computer-Based Call Tracking System Applies to: G, S, Collab, CB, M, A, E (See Table)
Partner must have a computer-based call tracking (e.g., ticketing or incident management) system available; system may be off-the-shelf or custom-built.

Partner must have a process for creating a ticket for each call as required, and must explain or show how tickets are created and entered into the system.

Computer-based call tracking system must have the following capabilities:
- Automatic allocation of the case number to ensure sequential and orderly tracking of case history and associated case information
- Fields to track caller information (name, company, phone number, e-mail ID, pager, contract ID, etc.)

- A field for a brief case description/headline defining the salient points related to the case
- Date- and time-stamped case notes; case notes must include call information, RMA shipments, and on-site activities
- The ability to capture, trend, and track all support activities, including problem definitions and engineering updates to the case, whether corrective or informational
- Generation of meaningful metrics to monitor case quality
- Recording of date and exact time (with a non-modifiable timestamp) when case is opened and closed
- Automatic escalation alerts, generated based on current priority and length of time case has been open; escalation alerts may be e-mail, SMS messages, or pager alerts to parties identified in partner's escalation procedures. Alerts must be generated in accordance with partner's documented escalation procedures and must be functioning for Priority 1 and 2 type cases as a minimum requirement
- Non-modifiable entries of case updates
- Non-modifiable time stamps for significant events (e.g., change of priority, change of status, change of owner)
- Recording of Cisco TAC case ID number when cases are escalated to Cisco TAC; may be a separate field in the system or recorded in case notes
- Access for partner engineers while at customer premises, to allow for creation of new tickets and updating of open tickets
- Access for support engineers to immediately log after-hour calls

Partner must explain or demonstrate each of the above system capability requirements.

NOTE: Silver partners may have manually initiated escalation alerts; alerts must be recorded as defined by partner's escalation process, and must be accompanied by an e-mail, SMS message, pager message, or telephone call to the parties identified in partner's escalation procedures.

7.2 Request Fulfillment

7.2.1 Service Request Process Applies to: G, S, Collab, CB, M, A, E (See Table)

Service requests are typically low risk, low cost and are small changes, e.g., a request to change a password or to install software, or a request for information. A separate process for request management prevents minor requests from congesting the incident or problem management processes.

Partner must have a documented process for responding to service requests, and must explain or show how requests are recorded, resolved, and closed. Requests may or may not be handled by the formal request for change (RFC) process.

7.2.2 Automated Service Request Tool Applies to: M, A, E (See Table)

Partner must have an automated service request tool; this may include a web interface where users can select and input details of the service request from a pre-defined menu.

Partner must explain or show how automated service request tool is used.

7.3 Event Management

7.3.1 Event Management Process Applies to: G, S, Collab, CB, M, A, E (See Table)

Events will either be informational (and should be logged), warning (alert should be sent), or exceptions (e.g., when something behaves out of normal patterns, which could trigger an incident).

Partner must have a documented process for ensuring that all events are documented once they are detected and filtered; partner must explain or show how events are handled through the appropriate process (e.g., management of events within a tool).

NOTE: This requirement does not apply to Gold and Silver partners who have a Cisco Branded Services (CBS) contract (i.e.: those who only sell Cisco SMARTnet and do not operate in a co-branded or shared support model) or partners with an approved CoE. However, Gold and Silver "CBS or SMARTnet only" partners applying for Master specializations or CMSP must meet all requirements outlined in this section, regardless of their service support agreement type, due to the intent and capabilities represented by these designations.

7.4 Incident Management

7.4.1 Incident Management Process Applies to: G, S, Collab, CB, M, A, E (See Table)

Incident management is the process responsible for managing the lifecycle of all incidents that can stem from repeated or severe events. The primary objective is to restore IT service as quickly as possible.

Partner must have a documented process for incident management, and must explain or show how incidents are identified, logged, categorized, prioritized, investigated and diagnosed, resolved, and closed.

NOTE: This requirement does not apply to Gold and Silver partners who have a Cisco Branded Services (CBS) contract (i.e.: those who only sell Cisco SMARTnet and do not operate in a co-branded or shared support model) or partners with an approved CoE. However, Gold and Silver "CBS or SMARTnet only" partners applying for Master specializations or CMSP must meet all requirements outlined in this section, regardless of their service support agreement type, due to the intent and capabilities represented by these designations.

7.4.2 Managed Device Monitoring Applies to: M, A, E (See Table)

All key components of the managed service must be monitored in order to detect failures or potential failures, and to resolve incidents before IT services are impacted.

Partner must monitor managed devices for environmental, availability, and performance information, and must explain or show how managed devices are monitored in order to detect incidents.

7.4.3 Fault and Performance Data Monitoring Applies to: M, A, E (See Table)

Partner must have a documented process for monitoring, tracking, and acting upon fault and performance data.

Partner must provide evidence of a monitoring process that includes:

- Polling interval for core monitoring data within a range of less than 5 minutes
- A customer portal or similar tool to allow customer real-time access to incident information
- Availability and storage of fault and performance data; data must be stored and accessible online for a period of not less than 12 months

7.4.4 Management Platform Applies to: M, A, E (See Table)

Partner must have a management platform capable of retrieving and acting upon environmental, availability, and performance information for managed devices.

Partner must provide evidence that the management platform is highly available, includes environmental and performance information, and feeds into the partner's ticketing system. Documented instructions must be available for using the tool.

Environmental monitoring may include monitoring of the equipment and/or data center, lab, and surroundings of the installed equipment and may include temperature monitoring, humidity monitoring, dust or particle monitoring, water leak detection, and/or equipment energy consumption.

Users must demonstrate knowledge and awareness of the tools and their capabilities.

7.4.5 Event Correlation Applies to: M, A, E (See Table)

Event correlation cross-references and correlates events to help determine the root-cause and accelerate root cause analysis.

Partner must have a management platform that has event correlation business rules, and must explain or show how the management platform provides the ability to correlate events from all devices under management.

7.4.6 Incident Detection Applies to: Collab, CB, M, A, E (See Table)

Partner must provide evidence that incidents are automatically detected within 5 minutes of occurrence.

7.4.7 Incident Logging and Querying Applies to: Collab, CB, M, A, E (See Table)

Partner must provide evidence that incidents are logged and accessible for queries, and must explain or show how records can be queried for a period of up to 90 days, e.g., in a ticketing system or database.

7.4.8 Customer Notification Applies to: Collab, CB, M, A, E (See Table)

Partner must have a process for notifying customers of detected incidents, and must provide evidence of customer notification, including records of contact made, e.g., in a customer file.

7.4.9 Notification Methods Applies to: Collab, CB, M, A, E (See Table)

Partner must provide notification to customers within 15 minutes. Customers must be able to select their preferred notification method by choosing at least two methods, including email and phone.

Partner must provide evidence of customer notification by their preferred method within 15 minutes of incident detection.

7.4.10 Incident Prioritization and Categorization Applies to: Collab, CB, M, A, E (See Table)
Categorization/prioritization of incidents is typically based on the impact on IT services and the business.

Partner must explain or show how tickets are categorized and prioritized, and must provide the documented guidelines used.

7.4.11 Stakeholder Updates Applies to: Collab, CB, M, A, E (See Table)
Frequency and criteria for stakeholder status updates must be based on severity, business impact, and/or SLA.

Methods must be in place for stakeholders to provide input on existing and open incidents, and for Incident Management personnel to review and respond to stakeholder input at a defined frequency.

Partner must have a documented process for communicating ticket updates to stakeholders, and must explain or show how stakeholders are updated on the status of tickets, and how stakeholder input is obtained and responded to.

7.4.12 Incident Troubleshooting and Investigation Applies to: Collab, CB, M, A, E (See Table)
Incident management procedure(s) must include instructions for resolution of known errors (e.g., previously resolved errors) and investigation of unknown errors.

Partner must have established methods for investigation and troubleshooting of incidents, and must explain how incidents are investigated and resolution is determined; examples of closed incidents must be provided.

7.4.13 Handoff to Problem Management Applies to: Collab, CB, M, A, E (See Table)
Incident management procedure(s) must include a link to problem management procedures for handoff of errors that are unknown or cannot be resolved.

Partner must provide evidence that unknown errors are handed off to or resolved with the help of problem management procedures.

7.4.14 Known Error Database Applies to: Collab, CB, M, A, E (See Table)
Partner must maintain a searchable database of known errors; database must be widely used within incident and problem management. Articles in the known error database must be assigned to a subject matter expert (SME).

Partner must provide evidence of a known error database; database may be off-the-shelf or custom-designed (e.g., using Excel or other similar tool). Users must demonstrate knowledge and awareness of the database and its capabilities.

7.4.15 Incident Closure Authorities Applies to: Collab, CB, M, A, E (See Table)
Partner must clearly identify, document, and communicate authorities for incident closure, e.g., in an authority matrix.

Partner must provide evidence that such authorities are communicated and adhered to, e.g., by providing records of closed incidents.

7.4.16 Incident Closure Summary Applies to: Collab, CB, M, A, E (See Table)
Partner must document a summary of the incident at the time of closure; summary must include details of incident resolution, as well as categorization of the incident based on pre-defined categories.

Partner must provide examples of incident summaries, e.g., in the ticketing system.

7.5 Problem Management

7.5.1 Problem Management Process Applies to: G, S, Collab, CB, M, A, E (See Table)
Problem management includes incidents for which there is no known solution (handed off from Incident Management), or is proactively identified from ticket, availability, or performance trending (e.g., multiple incidents on the same device within a time period).

Partner must have a documented process for problem management, and must explain how problems are detected, logged, categorized, prioritized, investigated and diagnosed, resolved, and closed. Partner must provide examples showing a link from incident management, including proactively identified problems from repeated similar incidents, and a link to change management for initiating changes that result from problem investigation.

NOTE: This requirement does not apply to Gold and Silver partners who have a Cisco Branded Services (CBS) contract (i.e.: those who only sell Cisco SMARTnet and do not operate in a co-branded or shared support model) or partners with an approved CoE. However, Gold and Silver "CBS or SMARTnet only" partners applying for Master specializations or CMSP must meet all requirements outlined in this section, regardless of their service support agreement type, due to the intent and capabilities represented by these designations.

7.5.2 Root Cause Analysis Applies to: G, S, Collab, CB, M, A, E (See Table)

Root cause analysis is an activity that identifies the underlying or original cause of an incident or problem.

Partner must provide documented evidence of root cause analysis, including identification, validation, documentation of problem root causes, and storage of information for evaluating similar problems (e.g., in a known error database/knowledge base).

NOTE: This requirement does not apply to Gold and Silver partners who have a Cisco Branded Services (CBS) contract (i.e.: those who only sell Cisco SMARTnet and do not operate in a co-branded or shared support model) or partners with an approved CoE. However, Gold and Silver "CBS or SMARTnet only" partners applying for Master specializations or CMSP must meet all requirements outlined in this section, regardless of their service support agreement type, due to the intent and capabilities represented by these designations.

7.5.3 Closed Loop Corrective Action Applies to: G, S, Collab, CB, M, A, E (See Table)

Partner must conduct closed loop corrective action for all problems, and must provide recommendation to stakeholders of appropriate problem remediation steps.

Records of corrective action must be maintained, including problem identification, root cause analysis, remediation steps, and review for effectiveness and closure. Examples of completed corrective actions must be provided.

Partner must provide evidence of the ability to provide real-time reports on open corrective actions, e.g., open tickets in the ticketing system or an RFC.

NOTE: This requirement does not apply to Gold and Silver partners who have a Cisco Branded Services (CBS) contract (i.e.: those who only sell Cisco SMARTnet and do not operate in a co-branded or shared support model) or partners with an approved CoE. However, Gold and Silver "CBS or SMARTnet only" partners applying for Master specializations or CMSP must meet all requirements outlined in this section, regardless of their service support agreement type, due to the intent and capabilities represented by these designations.

7.5.4 Proactive Problem Management Applies to: Collab, CB, M, A (See Table)

Proactive problem management includes review of recurring problems, identification of trends, and preventive action implementation.

Partner must have a documented process for proactive problem management, and must explain or show how problems are proactively identified and resolved. Records must be provided as evidence that problem data is analyzed to identify and remediate recurring problems, e.g., "top ten" reporting, with drill-down to further detail.

7.6 Access Management

7.6.1 Access Management Process Applies to: Collab, M, A, E (See Table)

Access management is the process for granting authorized users the right to use a service, while preventing access to non-authorized users.

Partner must have a documented process for providing access rights for users which should include management of CCO (Cisco User IDs), and:

- Methods for users to request access
- Verification of requests
- Provision of access rights
- Logging and tracking of access, including regular reviews
- Removal or restriction of rights when necessary

7.7 Onsite Response/Troubleshooting

7.7.1 Onsite Response and Troubleshooting Description Applies to: G, S, Collab, CB, M, A, E (See Table)

Partner must have a documented description for onsite response and troubleshooting, including:

- Geographic coverage

- Best service-level agreement (SLA)
- Dispatch system for onsite service, if separate from call tracking system
- Any subcontractors used (if allowed)

Partner must explain or show how onsite response and troubleshooting are provided to customers.

NOTE: This requirement does not apply to Gold and Silver partners who have a Cisco Branded Services (CBS) contract (i.e.: those who only sell Cisco SMARTnet and do not operate in a co-branded or shared support model) or partners with an approved CoE. However, Gold and Silver "CBS or SMARTnet only" partners applying for Master specializations or CMSP must meet all requirements outlined in this section, regardless of their service support agreement type, due to the intent and capabilities represented by these designations.

NOTE 2: Not required for CMSP partners offering one or a combination of the following services only: Cisco Powered IaaS, Cisco Powered DaaS, Cisco Powered DRaaS, Cisco Powered Cloud Cell Architecture for SAP HANA, Cisco Powered FnSaaS, Cisco Powered HSS or Cisco Powered TPaaS (when the TPaaS partner is not supplying the Customer Premises Equipment-CPE).

7.8 Remote Troubleshooting Access

7.8.1 Remote Access Applies to: M, A, E (See Table)

Remote access may be either in-band or out-of-band management, or by a combination of both, including ability to support either chosen connectivity option (in-band, where the control and management data shares the same network as the data being processed or out-of-band, where a separate network is maintained for management access and control data).

Partner must have remote access to the customer network for troubleshooting activities, and must explain or show how remote access is gained to the customer network, including what options are available for connectivity.

NOTE: Not required for CMSP partners offering one or a combination of the following services only: Cisco Powered IaaS, Cisco Powered DaaS, Cisco Powered DRaaS, Cisco Powered Cloud Cell Architecture for SAP HANA, Cisco Powered FnSaaS, or Cisco Powered HSS.

8 Continual Service Improvement Requirements

8.1 Service Improvement

8.1.1 Continual Improvement Activities Applies to: G, S, Collab, CB, M, A, E (See Table)

Partner must take actions to continually improve performance to objectives.

Partner must explain or show how continual improvements are initiated and implemented, and must provide evidence of continual improvement, including records of actions taken to improve performance, particularly when established objectives are not being met.

8.1.2 Continual Improvement Methodology Applies to: G, S, Collab, CB, M, A, E (See Table)

Partner must have a documented methodology for continual improvement, including:

- Defining what should be measured
- Defining what can be measured
- Gathering the data
- Processing the data
- Analyzing the data
- Presenting and using the information
- Implementing corrective action

Partner must provide evidence of the disciplined methodology used, including records of data collection, analysis, and corrective action.

8.2 Service Measurement

8.2.1 Service Objectives Applies to: G, S, Collab, CB, M, A, E (See Table)

Partner must establish measurable objectives for service availability, reliability, and performance.

Service objectives must be established, documented, tracked, and reviewed. Metrics must be relevant to the business and must address service levels, customer satisfaction, business impact, and supplier performance.

Partner must provide evidence that performance is measured and results are reviewed, e.g., in periodic business review meetings.

NOTE: This requirement does not apply to Gold and Silver partners who have a Cisco Branded Services (CBS) contract (i.e.: those who only sell Cisco SMARTnet and do not operate in a co-branded or shared support model) or partners with an approved CoE. However, Gold and Silver "CBS or SMARTnet only" partners applying for Master specializations or CMSP must meet all requirements outlined in this section, regardless of their service support agreement type, due to the intent and capabilities represented by these designations.

8.2.2 Mean Time to Notify (MTTN) Applies to: Collab, CB, M, A, E (See Table)

Mean Time to Notify (MTTN) is measured from initial system detection of a fault to customer notification by email or other prearranged electronic means.

Partner must provide evidence that MTTN performance data is correctly captured and tracked and that the following targets are being met for the applicable program:

Program	MTTN Target (all targets are SLA "best case")
Master Specialization (Collab, Sec, CB)	<20 minutes
CMSP (M, A, E)	See Cisco Powered Cloud and Managed Services Portfolio Requirements

NOTE: Partner may use alternate label for "MTTN", provided that the meaning is the same.

8.2.3 Mean Time to Restore Service (MTRS) Applies to: Collab, CB, M, A, E (See Table)

Mean Time to Restore Service (MTRS) is measured from the point of failure until it the service is fully restored and delivering its normal functionality to customers and end users (e.g., by temporary or permanent fix).

Partner must show how MTRS is outlined and defined in the customer's SLA, and must provide records showing that MTRS data is correctly captured and that targets are being met. Partner must restore services to the previous known working configuration based on the customer's SLA; for example:

Priority Level	MTRS Target
P1	4 hours
P2	24 hours
P3	2 business days
P4	5 business days

NOTE 1: Partner may use alternate label for "MTRS", provided that the meaning is the same.

NOTE 2: CMSP partners must refer to the service-specific targets listed in the Cisco Powered Cloud and Managed Services Portfolio Requirements.

8.2.4 Onsite Troubleshooting Response Time Applies to: G, S, Collab, CB, M, A, E (See Table)

Onsite troubleshooting response time is measured from the time onsite troubleshooting is determined as required to when support personnel arrive at customer site.

Partner must provide evidence that onsite troubleshooting response time data is correctly captured and tracked and that the following targets are being met for the applicable program:

Program	Onsite Troubleshooting Response Time
Resale Program: Gold	4 hours
Resale Program; Silver	24 hours
Master Specialization: (Collab, CB)	4 hours, except • Cloud/Oil/Gas/Energy/Utilities: may vary by customer
CMSP: Master	4 hours

NOTE 1: This requirement does not apply to Gold and Silver partners who have a Cisco Branded Services (CBS) contract (i.e.: those who only sell Cisco SMARTnet and do not operate in a co-branded or shared support model) or partners with an approved CoE. However, Gold and Silver "CBS or SMARTnet only" partners applying for Master specializations or CMSP

must meet all requirements outlined in this section, regardless of their service support agreement type, due to the intent and capabilities represented by these designations.

NOTE 2: Not required for CMSP partners offering one or a combination of the following services only: Cisco Powered IaaS, Cisco Powered DaaS, Cisco Powered DRaaS, Cisco Powered Cloud Cell Architecture for SAP HANA, Cisco Powered FnSaaS, Cisco Powered HSS or Cisco Powered TPaaS (when the TPaaS partner is not supplying the Customer Premises Equipment-CPE).

8.2.5 Customer Perception and Feedback Applies to: G, S, Collab, CB, M, A, E (See Table)
Partner must provide records showing that customer perception is measured and analyzed and appropriate actions are taken to resolve any customer issues.

8.3 Service Reporting

8.3.1 Service Reports Applies to: Collab, CB, M, A, E (See Table)
Partner must report incident, exception, inventory, availability, and performance data internally and to customers.

Reports must include:

- **Incident management reports**: Reports detailing the current work activities to correct incidents on the customer network; metrics on the management of incidents, such as number of incidents, average time to resolve, common causes identified.
- **Exception reports**: Reports generated by customer-specified thresholds or ranges; provides ability for customers to self-select parameters on individual devices and determine thresholds for the raising of exception reports.
- **Device inventory reports**: Reports of devices under management for the customer; provides data that is relevant to the customer regarding inventory of equipment or WAN services used in delivering the service.
- **Service availability reports**: Summary views of service availability; reports on the overall service availability, e.g., by site or equipment.
- **Performance analysis reports**: Historical performance analysis of the service, typically over a number of sample periods (daily, weekly, monthly) and including data to allow the customer to understand how the overall service is performing.

NOTE: CMSP partners must also provide reports specific to the service(s) offered; see Cisco Powered Cloud and Managed Services Portfolio Requirements.

8.3.2 Cloud or Managed Service Contracts Applies to: M, A, E (See Table)
Partner must provide evidence of a cloud or managed service(s) contract for orders placed within the last 12 months (applies to recertification audits only).

Cisco will randomly select a sample size of up to 10% of all transactions for orders placed within the past 12 months. Partner must provide evidence of full compliance with the order eligibility requirements (see Program Policies: Cloud and Managed Services Finance Policies and Procedures).

Appendix 1: Support Levels

Support Level	Level 0 Procedural	Level 1 Basic	Level 2 Advanced	Level 3 Expert
Context	Past terminology usage within Cisco has been to characterize simple processing of a customer call as 'Level 0 Support'. As the granularity of roles within Cisco and its service partner community has expanded, so has the need for definition of support which is more than simple call processing, yet less skill-intensive than Level 1 product troubleshooting.	Level 1 service is generally considered to be technical in nature, and having basic complexity characteristics. This service level requires some independent judgment and analysis beyond a simple script. Some Cisco partner programs expect this level of support to be provided by the partner.	Considered to be the bulk of advanced customer support, requiring certified resources with specialized education. Some Cisco partner programs expect this level of support to be provided by the partner.	Considered to be the highest in complexity, and often requires direct interaction with development engineering resources when product defects are involved.
Service Definition	• Log an end-customer call and assign it to the correct resource or technology team with symptoms, affected hardware, and software version. • Verify support entitlement and service level • Provide initial problem categorization • Answering general questions using pre-scripted text • Provide references directing customers to available tools or documentation on Cisco.com	• Provide general product information (pre-sales and post-sales) • Hardware and software configuration, installation, and feature set upgrade support for mature products • Resolve obvious hardware problems • Resolve known problems through documentation available on Cisco.com or other local resources • Provide basic internetworking troubleshooting expertise • Provide basic support on the standard software protocols and features • Collect captured network traces and diagnostic data • Provide regular problem resolution status reports to the end user • Filter non-technical problems from technical problems • Perform base problem determination and collect relevant technical information	• Resolve the majority of complex configuration problems by troubleshooting and problem simulation (i.e., recreates) • Resolve most software or hardware problems • Determine product defects • Define an action plan for troubleshooting/resolution • Use external analyzing tools when appropriate • Analyze traces and diagnostic data when appropriate • Perform interoperability and compatibility testing for new software and hardware releases prior to being deployed into production network • Perform lab simulation and problem duplication • Perform lab testing before deployment of possible fix • Generate workarounds for hardware and software bugs (where present or alternate functionalities allow it) and troubleshooting bugs that were not diagnosed or resolved during Level 1 Support. • Provide contact with complete steps to reproduce a problem in event of escalation to Level 3 support	• Resolve problems reported to TAC for the first time in which no documentation exists in respect of the problem on Cisco.com or any other format • Resolve problems associated with previously unidentified bugs that have not yet been published on Cisco.com • Generate workarounds for hardware and software bugs and troubleshooting bugs that require a specialized expertise level beyond Level 1 or Level 2 support • Perform issue reproduction with complex lab simulations • Provide or interface with product and/or software development engineering support for resolution of product defects • Identify interoperability issues that may be caused by 3rd party software/hardware

Support Level	Level 0 Procedural	Level 1 Basic	Level 2 Advanced	Level 3 Expert

Service Request Characteristics	• Same day closure
	• Serviceable by non-certified resource
	• Solvable by pre-established documented procedures
	• Examples of Level 0 Service Requests include but are not limited to:
	  • RMA (Returned Material Authorization) not requiring troubleshooting
	  • DOA (Dead on Arrival) hardware
	  • Software download support
	  • Licensing
	  • Password reset
		• Documented and understood problems with stable product lines which can be solved by support engineers with basic network or technology knowledge and troubleshooting skill
		• Examples of Level 1 Service Requests include but are not limited to:
		  • Hardware failure verification on established product lines
		  • Assistance with basic configuration issues
		  • Installation assistance
			• Requires skilled research and technical ability to diagnose and resolve problem
			• Involves a known bug or new bug which is easy to moderate to diagnose
			• Complex production working environments and limited interoperability issues
			• Examples of Level 2 Service Requests include but are not limited to:
			  • Assistance with advanced configuration issues
			  • Troubleshooting performance issues
			  • Resolving interoperability problems
			  • Analysis of protocol traces
				• Requires significant research time
				• Requires complex lab recreation scenario
				• Requires quality interaction with Cisco Development teams
				• Involves new bug of significant complexity
				• Requires depth of understanding of products and interaction between products

Appendix 2: Glossary

access management: The process responsible for allowing users to make use of IT services, data, or other assets.

case management system: A system, typically electronic, for recording, tracking, updating, closing of incidents and subsequent reporting of same.

CCIE Emeritus: A long term Cisco Certified Internetwork Expert (CCIE) who has moved out of the "day to day" technical work but would like to remain involved in the program serving as an ambassador to current and future CCIE's; emeritus status does not constitute a valid CCIE.

Certified Resale partner: A partner that has qualified for Cisco Gold, Silver, Premier, or Select certification under the Cisco Channel Partner Program guidelines.

change: The addition, modification or removal of anything that could have an effect on IT services.

change management: Process of controlling changes to the infrastructure or any aspect of services, in a controlled manner, enabling approved changes with minimum disruption.

Cisco-based cloud service: A cloud-based service built on a Cisco reference architecture; see examples.

Cisco-based managed service: An offer where the key features of the service are provided by Cisco device(s), or a network-based service is built on Cisco infrastructure AND the service includes monitoring and management of Cisco equipment owned or leased by the customer (Cisco end points or Customer Premises Equipment).

Cisco Powered service: A cloud or managed service for which a partner must meet the requirements of the service as specified in the Cisco Powered Services Portfolio: Requirements Document, as reviewed and validated by a third-party audit.

Cisco Powered services designation: Indicates that the cloud or managed service has met the requirements as specified in the Cisco Powered Services Portfolio: Requirements Document, as reviewed and validated by a third-party audit. A partner may hold Cisco Powered services designation for several cloud and/or managed services.

Cloud Builder: A Cloud Builder is a company who assembles all cloud ready infrastructure inclusive of the unified data center components, and third party ecosystem solutions (storage, hypervisor, management, and orchestration solutions).

cloud provider: A Cloud Provider is one who offers virtualized or hosted IT services from the provider's own data center.

cloud service: Management of data, software and/or computing that is provided in a virtualized (or non-virtualized) data center operation that can be offered to an end customer under a subscription or usage-based model from CMSP partner's Data Center.

CMSP services reseller: A company that has met the CMSP Services Reseller requirements and acts as an aggregator, agent, or broker and resells a CMSP Partner's Cloud Service or Managed Service as if they were its own services. This relationship is reflected in a contractual agreement between CMSP Partner and CMSP Services Reseller.

configuration item (CI): Any component that needs to be managed in order to deliver an IT Service. Information about each CI is recorded in a configuration record within CMDB and is maintained throughout its lifecycle by Configuration Management. CIs are under the control of Change Management. CIs typically include hardware, software, buildings, people, and formal documentation such as process documentation and SLAs.

configuration management: The process responsible for maintaining information about Configuration Items required to deliver an IT service, including their relationships. This information is managed throughout the lifecycle of the CI. The primary objective of Configuration Management is to underpin the delivery of IT Services by providing accurate data to all IT Service Management processes when and where it is needed.

configuration management database: A database used to manage configuration records throughout their lifecycle. The CMDB records the attributes of each CI, and relationships with other CIs. A CMDB may also contain other information linked to CIs, for example Incident, Problem or Change records. The CMDB is maintained by Configuration Management and is used by all IT Service Management processes.

corrective action: Action taken to remove the root-cause of a detected problem in order to prevent its recurrence.

country group: The Cisco sales theaters located in Europe, Middle East, Africa, Russia, Asia Pacific, Japan, China, US, Canada and LatAm have defined country groupings to be regarded as a “country” for certification and specialization purposes. This allows partners to pool their resources across countries in order to qualify for certification and specialization. Certification and specialization is granted to partners for each country within a country grouping; see details.

customer premises equipment (CPE): For purposes of the CMSP, means product used by a partner to deliver a cloud or managed service where the product is either: Dedicated to a single end user and located at an end user’s premises; or Customer Specific Equipment (as defined below). The scope of this definition may be expanded at Cisco’s discretion to include certain network products that are not centrally managed, but are connected to a centrally managed product and are essential to the delivery of a Cisco Powered service. Examples of such network products might include routers and switches used to terminate transport circuits, IPT handsets and powered Ethernet LAN cards and switches.

customer specific equipment (CSE): For purposes of the CMSP means product dedicated to a single end user or multiple end users and located in a partner’s hosting center or point-of-presence (PoP). Examples would be managed, hosted, or cloud-based call managers dedicated to a single or multiple enterprises operated from a hosting center.

data center (DC): Physically houses various equipment, such as computers, servers (e.g., web servers, application servers, database servers), switches, routers, data storage devices, load balancers, wire cages or closets, vaults, racks, and related equipment. Data centers store, manage, process, and exchange digital data and information and provide application services or management for various data processing, such as web hosting internet, intranet, telecommunication, and information technology. Cisco Powered cloud services are offered from the data center.

definitive hardware store (DHS): One or more physical locations in which hardware configuration items are securely stored when not in use. All hardware in the DHS is under the control of change and release management and is recorded in the CMDB. The DHS contains spare parts, maintained at suitable revision levels, and may also include hardware that is part of a future release.

definitive software library (DSL): One or more locations in which the definitive and approved versions of all software configuration items are securely stored. The DSL may also contain associated CIs such as licenses and documentation. The DSL is a single logical storage area even if there are multiple locations. All software in the DSL is under the control of change and release management and is recorded in the CMDB. Only software from the DSL is acceptable for use in a release.

direct partner: A partner that has a direct product resale agreement with Cisco, including systems integrators and Service Provider Resale.

distributor: A distributor authorized by Cisco to distribute products and services in accordance with the direct purchase agreement between Cisco and such distributor ("Cisco Distribution Partner" or "CDP" or "Distributor"); (ii) a distributor ("Cisco Authorized Distributor" or "CAD") authorized by Cisco Distribution Partner to distribute the products and services within EMEA in accordance with the terms of the Cisco distribution partner or distributor's agreement with Cisco (including, without limitation, Cisco's then current guidelines relating to the appointment of and agreement with any such Cisco Authorized Channel).

escalation: An activity that obtains additional resources when these are needed to meet Service Level targets or customer expectations. Escalation may be needed within any IT service management process, but is most commonly associated with incident management, problem management and the management of customer complaints.

error: A design flaw or malfunction that causes a failure of one or more configuration items or IT services. A mistake made by a person or a faulty process that impacts a CI or IT service is also an error. See known error.

event: A change of state that has significance for the management of a configuration item or IT service. Events may indicate normal activity or an event may indicate that something is not functioning correctly and lead to an incident being logged.

event management: The process responsible for managing events throughout their lifecycle.

fault: Synonym for error.

fault data: Time series of error data.

gap audit: A gap audit is an audit where only the incremental requirements are audited based on a partner's other program participation. For example a partner who is Gold certified today, who is wanting to pursue a Master Specialization, will only be audited on the "gaps" or those items that have not yet been covered by the Gold audit (except where otherwise noted).

get-well plan: An action plan defined by the partner to address noncompliance of requirements. Failure to complete get-well plans within predetermined timeframes will result in decertification or downgrade to the next eligible level.

in-band management: Where the control and management data shares the same network as the data being processed. Incident: An unplanned interruption to an IT service or reduction in the quality of an IT service. Any event that could affect an IT service in the future is also an incident.

hybrid IT: a service produced by one company (the Producer) that other companies (the resellers) resell to end customers.

incident ticket: A record, typically electronic, containing details of an incident.

incident closure: The act of changing the status of an incident to closed when the customer is satisfied than an incident has been resolved.

incident management: The process responsible for managing the lifecycle of all Incidents. The primary objective of incident management is to return the IT service to customers as quickly as possible.

indirect partner: A partner that does not have a direct product resale agreement with Cisco.

infrastructure: Means shared network elements, such as core, aggregation, multiservice edge Internet Protocol (IP) structures that are used by a partner to build, deploy, and maintain network services. The infrastructure is used to support multiple network services and is used as a shared resource to convey the traffic of multiple end users. Except in the case of virtual managed service providers, the partner generally owns the infrastructure.

ISO 27001: An information security management system (ISMS) standard first published in October 2005 by the International Organization for Standardization ("ISO") and the International Electrotechnical Commission (IEC). ISO/IEC 27001 specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving a documented ISMS within the context of the organization's overall business risks. The standard specifies requirements for the implementation of security controls customized to the needs of individual organizations or parts thereof.

knowledge base: A database containing information about incidents, problems and known errors. The knowledge base is used to match new Incidents with historical information, improving resolution times and first time fix rates.

known error: A problem that has a documented root-cause and a workaround.

managed service: Information technology delivered as a finished solution where the partner proactively manages and monitors the entire solution and can remediate said solution from the service desk, (NOC) or through an authorized NOC services provider according to a defined Service Level Agreement between the provider and the customer.

managed services reseller: A Cisco partner that has met the managed services reseller requirements and acts as an aggregator, agent, or broker and resells CMSP partners' managed services as if they were its own services. This relationship is reflected in a contractual agreement between CMSP partner and managed services reseller.

mean time to notify (MTTN): A metric for measuring and reporting notification of faults. MTTN is the average time taken to notify a customer measured from initial system detection of a fault.

mean time to restore service (MTRS): A metric for measuring and reporting maintainability. MTRS is the average time taken to restore a configuration item or IT service after a failure. MTTR is measured from when the CI or IT service fails until it is fully restored and delivering its normal functionality to the customer or end user.

network operations center (NOC): A central location from which administrators supervise, monitor and maintain networks. A network operations center (NOC) is a room containing visualizations of the network(s) that are being monitored, workstations at which the detailed status of the network can be seen, and the necessary software to manage the networks. network operations center, A virtual network operations center (virtual NOC) allows partners to provide the functions of the NOC, distributed across multiple locations to allow for reduced cost and better resource utilization.

NOC services provider: A service provider that a CMSP partner has an executed, documented contract with (including a signed SLA with penalties) for the management of its NOC operations.

objective evidence: Objective evidence is physical; evidence that someone, when reviewing an audit report, can inspect and evaluate for oneself. It provides compelling evidence that the review or audit was actually performed as indicated, and that the criteria for the audit was upheld.

onsite troubleshooting response time: A metric for measuring and reporting the time it takes for a technician to arrive at the customer's site upon determining that onsite troubleshooting is required.

out-of-band management: Where a separate network is maintained for management access and control data.

outsourcing of NOC operations: Outsourcing of ITIL processes and people by CMSP partners who may or may not own NOC assets.

partner: Partner, as used in this document, refers to the organization seeking certification (or recertification) within the Cisco Channel Partner program, or an authorized person within that organization. Criteria and metrics herein apply to the partner organization within the country (or country grouping) for which the certification is applied. All partners, regardless of their business model, are required to meet the same certification requirements.

performance/performance data: Non-binary data that typically varies over time (e.g., memory utilization).

proactive monitoring: Means that the partner, at a minimum, utilizes centralized network management systems and processes to automatically detect service failures and problems impacting the product.

problem: The root-cause of one or more incidents.

problem management: The process responsible for managing the lifecycle of all problems. The primary objectives of problem management are to prevent incidents from happening, and to minimize the impact of incidents that cannot be prevented. Problem management includes problem control, error control and proactive problem management.

problem signature: The trend or repetition of faults that indicates a chronic problem.

provider: may be Cisco, a CMSP partner with Cisco Powered Service offerings or a partner selling their own Cisco Based Power Service.

release management: The process responsible for planning, scheduling, and controlling the movement of releases to test and live environments. Release management works closely with configuration management and change management.

request for change (RFC): A formal proposal for a change to be made. An RFC includes details of the proposed change, and may be recorded on paper or electronically.

reseller: A partner who sells to end-user customers and cannot sell to other partners.

resolution: Action taken to repair the root-cause of an incident or problem, or to implement a workaround.

root-cause analysis (RCA): Investigation to identify the underlying or original cause of an incident or problem.

security management: The process that manages the confidentiality, integrity and availability of an organization's assets, information, data and IT services.

service desk: The single point of contact between the service provider and the users. A typical service desk manages Incidents and service requests, and also handles communication with the users.

service level agreement (SLA): A contractual agreement between an IT service provider and a customer. The SLA describes the IT service, documents service level targets, and specifies the responsibilities of the IT service provider and the customer.

stakeholder: All people who have an interest in an organization, project, IT service etc. Stakeholders may be interested in the activities, targets, resources, or deliverables. Stakeholders may include customers, partners, employees, shareholders, owners, etc.

subcontracting: To engage a third party to perform under a subcontract, all or part of, work included in an original contract.

third-party: Someone who may be indirectly involved but is not a principal party to an arrangement, contract, deal, or transaction.

Appendix 3: Program Policies

Policy	Resale		Master Specialization			Cloud & Managed Services		
	G	S	Collab	Sec	CB	M	A	E
A3.1 Annual Recertification/Specialization Qualification	•	•	•	•	•	•	•	•
A3.2 Audit Waiver	•	•	•	•	•	•	•	•
A3.3 Get-Well Plans	•	•	•	•	•	•	•	•
A3.4 Certification Downgrade	•	•	•	•	•	•	•	•
A3.5 Third Party Contracting (or Subcontracting)	•	•	N/A	N/A	N/A	•	•	•
A3.6 Mergers, Acquisitions, Divestiture, and Affiliates	•	•	•	•	•	•	•	•
A3.7 CCIE/CCDE/CCNP Voice/CCNP Security Hiring and Terminating	•	•	•	•	•	•	•	•
A3.8 CCIE/CCDE/CCNA/CCNP Sharing	•	•	N/A	N/A	N/A	N/A	N/A	N/A
A3.9 CCIE/CCDE Contracting	•	•	•	•	N/A	N/A	N/A	N/A
A3.10 Competitor Policy	•	•	•	•	•	•	•	•
A3.11 Centers of Excellence (CoE)	•	•	N/A	N/A	N/A	N/A	N/A	N/A
A3.12 Language Requirements	•	•	•	•	•	•	•	•
A3.13 CMSP Finance Policies and Procedures	N/A	N/A	N/A	N/A	N/A	•	•	•

A3.1 Annual Recertification/Specialization Qualification

Policy regarding annual renewal of certifications and specializations.

Applies to: G, S, Collab, Sec, CB, M, A, E (See Table)

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 review and potential audit and also through monthly compliance reports and automatic system checks.

- Certified partners must submit an online application for recertification by their certification anniversary date each year.
- Partners that have not submitted a complete application including all required documentation no later than 30 days after their certification anniversary date may be decertified.
- In order to maintain certification, the recertification audit must be conducted no later than 60 days after the partner's certification anniversary date (Cisco reserves the right to assign auditors based on availability)
- 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 the next anniversary date.

A3.2 Audit Waiver

Policy to waive the audit requirement for recertification for partners demonstrating outstanding performance within the program.

Applies to: G, S, Collab, Sec, CB, M, A, E (See Table)

In order to qualify, partners must have demonstrated exemplary performance during their prior year's audit, resulting in no audit action items and no 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 Certification Program Manager.

Partners must also meet all criteria outlined in the Certification and Specialization Terms and Conditions, plus relevant attach rate and service revenue metrics.

Changes to the program requirements, partner's support agreement, and merger/acquisition or business operations may disqualify partners from an audit waiver.

The decision to grant an audit waiver is made solely by the Cisco Certification Program Manager; partners do not need to request an audit waiver. Following submission of a renewal application, the Cisco Certification Program Manager will review the application for audit waiver eligibility. Cisco reserves the right, at its sole discretion, to deny an audit waiver to a Channel Partner applicant regardless of whether the applicant satisfies the substantive criteria set forth in the Cisco Channel Program Audit and Policies for audit waivers. If a partner meets criteria and may be granted an audit waiver, the Cisco Certification Program Manager will contact the partner and approve the recertification without an audit. If a partner does not meet audit waiver criteria, an audit will be requested and the partner will be contacted for an audit date.

Determination of an audit waiver for Gold or Silver partners is independent of the audit waiver review for CMSP/Master Collaboration/Master Security/Master CB even if the programs share the same anniversary date.

Partners who outsource their NOC operations will be audited annually and are not eligible for an audit waiver to ensure they continue to meet the program requirements. An audit will be required if the NOC is outsourced to a company other than one previously audited.

For Master Specializations (Collaboration, Security, Cloud Builder), the following additional requirements apply:
Determination of an audit waiver for Master Specializations is independent of the audit waiver review for any other certifications or specializations even if the programs share the same anniversary date. The Partner should submit a new application prior to or no later than the anniversary date each year. After review by the Cisco Certification Program Manager, the partner will be advised it they have qualified for an audit waiver.

For CMSP (Master, Advanced, Express), the following additional requirements apply:
In addition to the requirements listed above for Gold and Silver partners, CMSP partners must meet all prerequisites including the ITIL personnel requirement. Partners who outsource their NOC operations will be audited annually and are not eligible for an audit waiver to ensure they continue to meet the program requirements.

A3.3 Get-Well Plans

Policy regarding providing an extended time period to ensure compliance with an outstanding requirement for recertification.

Applies to: G, S, Collab, Sec, CB, M, A, E (See Table)
Partner will maintain current certification level during the get-well period if they remain compliant with all other specialization or certification requirements. Failure to meet the get-well plan requirements will result in loss of specialization and/or certification and corresponding discount. Eligibility for a get-well plan is based upon the discretion of the Cisco Certification Program Manager. Consecutive get-well plans (two get-well plans in one certification year) are not allowed; this rules does not apply to a CCIE get-well plan as a CCIE get-well plan may be issued in conjunction with one other get-well plan per certification year.

A3.4 Certification Downgrade

Policy regarding partner downgrade for noncompliance to program requirements.
Applies to: G, S, Collab, Sec, CB, M, A, E (See Table)
Cisco may decertify or downgrade a partner if the partner fails to comply with requirements during the certification term due to, but not limited to, the following:

- Failure to maintain current Indirect Channel Partner Agreement (ICPA) or Direct Agreement
- Failure to meet certified individual requirements
- Failure to meet the terms of a Get-Well Plan
- Failure to submit the renewal application 30 days from anniversary date
- As a result of competitive relationships with Cisco
- Submission of false, misleading, or incomplete information on the application
- Application submission representing Cisco certified individuals who do not work for the partner

For Resale (Gold, Silver) only, the following may also result in decertification or downgrade:

- Failure to meet specialization requirements during recertification or at any time throughout the year
- Failure to meet customer satisfaction (CSAT) requirements
- Failure to meet the service attach rate requirement
- Failure to meet the service revenue requirement

For CMSP (Master, Advanced, Express), the following additional requirements apply:
Cisco reserves the right to terminate a partner from participation in the CMSP for the following reasons:

- Submission of false, misleading, or incomplete CMSP information
- Failure to report change in NOC services provider in the case of outsourced NOC operations
- Other fraud or abuse of this or other Cisco marketing or sales programs
- Distribution of Cisco Products purchased from any source other than Cisco or an authorized Cisco Distributor
- Purchasing product in the Cloud and Managed Services Program and deploying product in non-managed environments

Downgrade from CMSP will result in the loss of privileges, branding, and rebates associated with the partner's CMSP designations (if applicable).

A3.5 Third Party Contracting (also referred to in this document as subcontracting)

Policy for subcontracting partner's support service (as required for certification and/or specialization) to a third party. This policy covers call center operation, technical support, and onsite service.
Applies to: G, S, M, A, E (See Table)
Call Center Operation:
The partner may outsource initial call-taking activities to a third party as long as the following requirements are met:

- The partner must demonstrate how the skills and capabilities of the subcontracted party are evaluated in determining suitability to provide such services, including the mechanism employed to monitor ongoing performance.
- The subcontracted 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 subcontracted party must receive phone calls in the local language through the partner's published service telephone number for the country.
- The subcontracted party must have appropriate access to the partner's call-tracking system to allow for immediate logging of customer calls.
- The subcontracted party must ensure callback by a partner engineer within one hour.
- The subcontracted 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 subcontracted 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 (Resale only):
For Resale (Gold/Silver) Partner Branded Services, technical support operation must remain in-house with the partner and cannot be subcontracted to a third party. Technical support refers to Level 2 or higher support activity; see Appendix 1 for detailed description of Support levels.

Onsite Hardware Replacement Services:
The partner may outsource onsite hardware replacement provided that the following requirements are met:

- The partner must demonstrate how the skills and capabilities of the subcontracted 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 subcontracted party to support Cisco products must be provided.

Service Continuance/Disaster Recovery (CMSP only):

- Service continuity/disaster recovery may be outsourced to a third-party so long as this can be done with seamless 24 x 7 coverage, without lapse in monitoring and support of customer SLAs.

NOTE: In order to maintain CMSP qualifications, partner must retain contractual relationship with the customer. Additional third-party contractual relationships are addressed on a per-designation basis in the Cloud and Managed Services Portfolio Requirements.

A3.6 Mergers, Acquisitions, Divestiture, and Affiliates

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.
NOTE: Should any of the above need to be conducted for your business, please work with your account team and/or open a case with Customer Service.
Applies to: G, S, Collab, Sec, CB, M, A, E (See Table)
The new, combined entity must inform Cisco of the integration or divestiture of the entities by providing the Cisco Certification Program Manager with a plan for integration or divestiture of processes, systems, labs, escalations, etc., as well as timelines for this integration or divestiture.

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 outlined 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 equivalent of full time employee means providing a minimum of 40 hours of

work per week for the partner seeking certification. 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

A fully owned subsidiary or the parent company of a certified partner can benefit from the same discount of the certified partner (Resale). 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. If the new entity has a direct buying contract, the merging entities will maintain their separate certification (and specialization) achieved until the new legal contract is signed, If the new entity has an indirect buying contract, documentation of the merger will be required and the ICPA will need to be re-signed after the merger is complete in the partner database.

An audit may 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 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 Cisco Certification 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.

CCIEs affected by Cisco-recognized mergers/acquisitions/divestitures, as defined in the merger policy above, are not subject to the CCIE 12-month move policy.

Affiliates (Applicable only for Resale discount sharing)

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, 50.1 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.

Divestiture

Divestitures are the sales, liquidation, or spinoff of a corporate division or subsidiary. Cisco certification will recognize as certified only the division or subsidiary that qualifies for the certification requirements. Certification will be awarded to both organizations when each divested organization qualifies for certification.

The partner must inform Cisco on the divestiture of any part of its company where the resources and staff relevant to the program are affected. Cisco will continue to grant certification or specialization only if the partner can demonstrate that those staff and resources after the divestiture continue to meet the requirements of the program.

The partner will need to provide the Cisco Certification Program Manager with a plan for the divestiture of processes, systems, labs, escalations, etc. as well as timelines for this divestiture.

CCIEs affected by Cisco-recognized mergers/acquisitions/divestitures, as defined in the merger policy above, are not subject to the CCIE 12-month move policy.

An audit may be required within 90 days of the divestiture in order to validate that the company continues to meet all requirements for that certification (and specialization). The requirement for an audit is to determine the level of divestiture and potential disruption in the pre-sales or post-sales functions of the business.

Franchise

A franchise is an independent business and does not receive any special recognition (branding or discounting) for the certification of the partner franchisors.

A3.7 CCIE/CCDE/CCNP Voice/CCNP Security Hiring and Terminating

Policy regarding loss of or hiring of a CCIE, CCDE/CCNP Voice or CCNP Security from another Cisco certified or specialized partner.

Applies to: G, S, Collab, Sec, CB, M, A, E (See Table)

Losing Partner

If the loss of a CCIE, CCDE, 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 nine months to replace the CCIE or CCDE, in order to avoid decertification or losing the specialization that requires a CCIE, CCDE,. A partner that voluntarily terminates the employment of a CCIE/CCDE 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. This recovery period does not protect other out of compliance issues, nor should it delay any standard process to include recertification and renewal.

If a partner does not notify Cisco of its noncompliance with the CCIE or CCDE 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 or CCDE in order to avoid decertification or losing the specialization that requires a CCIE or CCDE. This extension period will begin upon Cisco's notification to the partner of noncompliance.

NOTE: The above policy does not apply if partner is lacking more than one CCIE during the certification year; multiple extensions will not be granted and partner will be downgraded to next appropriate level of certification or to Registered Partner status; the CCIE 12-month policy does not allow the losing partner to continue counting the departing CCIE's badge towards their certification; a gaining partner is required to obtain a release letter from the losing partner if the gaining partner plans to count the individual's CCIE badge towards their certification.

Gaining Partner

If a partner hires a CCIE or CCDE (hereafter referred to as CCIE, et al) 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 employee or is willing to release the employee's badge to be used. In this case, Cisco will require documentation from the partner that it terminated the employee or released the employee. If the employee 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. The release letter must be on previous employer's company letterhead, stating that the employee was terminated or that they have released the CCIE, et al. to support another partner's certification. The letter must also include the last date of employment.

A3.8 CCIE/CCDE/CCNA/CCNP Sharing

Policy regarding sharing of CCIE/CCDE/CCNA/CCNP required for certification and/or specialization.

Applies to: Global and Multinational G,S (See Table)

A partner using the Center of Excellence (CoE) formerly known as Consolidated Service Center model (see CoE policy) may meet the CCIE/CCNA/CCNP requirement in the following manner:

- 50 percent of the required CCIEs must be located in the designated CoE. These engineers must be 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.
- If a partner has multiple CoEs, CCIEs can only be allocated* from the designated CoE that will provide remote support for the country applying for certification.
- 50 percent of the required CCNAs/CCNPs may be utilized from a CoE. These engineers must be distinct from those nominated for in-country certification for the CoE country or any other countries. The remainder of the required number of CCNAs/CCNPs must be located in the country applying for certification.
- The CCNA/CCNP being shared from the CoE must be associated** in the Partner Self Service Tool (PSS) to the location in which the 50% CCNAs/CCNPs are supporting. Example: If CCNA or CCNP is located in UK CoE, but supporting the partner location in Germany, the CCNA or CCNP must associate** their CSCO ID to the Germany location.
- If a remote country is not using a CoE, all CCIEs/CCNAs/CCNPs required for certification must be in-country.

*Allocation is completed by Cisco Certification Program Manager

**Association must be completed by the individual who wants to associate their CSCO ID to a particular country. This is done via the Partner Self Service Tool (PSS).

CMSP only: CCIE Sharing does not apply; CCIEs cannot be shared in CMSP.

A3.9 CCIE/CCDE Contracting

Policy regarding contracting out required CCIEs, including to Cisco Learning Solution Partners (CLSP).
Applies to: G,S, Collab, Sec (See Table)
CCIE/CCDE's 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 CCIE/CCDE's can be hired under contract provided that the following criteria are met:

- CCIE/CCDE 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 intact for at least 12 months from the audit date
- The lending or transfer of a CCIE/CCDE credential by its owner to a Channel partner who is not the owner's full-time employer or the equivalent of full time employed, e.g., 40 hours/week, is a violation of program policy and subject to sanctions. This is also true for partner companies who misuse CCIE/CCDE credentials, with or without CCIE/CCDE candidate consent, for unfair benefit. Candidates who violate policy as stated in the Cisco Career Certification and Confidentiality Agreement] may receive a permanent ban on future Cisco examinations and the cancellation of previously earned Cisco certifications. Channel Partners who violate these guidelines in their partner agreements will be immediately de-authorized.

CMSP only: CCIEs must be full time regular employees of the CMSP partner.

A3.10 Competitor Policy

Policy regarding direct competitors to Cisco not being eligible for certification or specialization.
Applies to: G,S, Collab, Sec, CB, M, A, E (See Table)
Direct competitors of Cisco Systems, or any entities owned, controlled, or acquired by a direct competitor of Cisco Systems (collectively, "Direct Competitors"), may not be granted Specialized or Certified Partner status pursuant to the Cisco Channel Partner Program Audit and Policies. "Owned or controlled" means any direct or indirect ownership share that gives a Direct Competitor effective control of a given Channel Partner or Channel Partner applicant. "Acquired" means any form of acquisition or merger, whether or not completed, by which the acquired entity becomes owned or controlled by a Direct Competitor.

Cisco may decertify a Direct Competitor (including without limitation a current Channel Partner that has become or been acquired by a Direct Competitor) at Cisco's sole discretion upon 30 days' written notice. Cisco's decision not to exercise its right to decertify a Direct Competitor in any instance shall not operate as a waiver of Cisco's right to decertify that or any other Direct Competitor at any time upon 30 days' notice.

Direct Competitors may, at Cisco's sole discretion, participate as registered resellers.

A3.11 Centers of Excellence (CoE) formerly known as Consolidated Support Center (CSC)

Policy that allows a partner to operate from a CoE location providing support and enablement to remote certified locations, through technology to ensure the viability of seamless support 24X7 within in the same GEO.
Applies to: Resale (CoE Gold, remote countries Silver or Gold)
Applies to: G,S (See Table)
A partner that operates a certified location in more than one country may have a Center of Excellence, consolidated support operations, NOC or data center in one or more regional centers. The term Center of Excellence (CoE) hereby denotes any of the described locations above which may be utilized to take, handle, resolve or escalate customer support cases in conjunction with the partner's local support organization.

NOTE: Partners with current CMSP qualification who own their NOC and want to use Consolidated Support model do not require a separate CoE audit.

Center of Excellence and Remote Country Audit Itinerary:

- Introductions and audit goals (auditor)
- Overview of audit methodology (auditor)
- Partner support strategy overview presentation, including regional and/or technology coverage, organization structure, SLA's and metrics

- Review of audit findings

Recommended participants either onsite or remote:

- The partner regional support or local technical lead, able to demonstrate the tools and case handling (typically a Support or Operations Manager, potentially a CCIE)
- Cisco account manager and Cisco SE responsible for partner relationship across geographic region, or local SE in country where CoE is located
- Technical Manager responsible for all service and support of Cisco technology

CoE Overview

The CoE must meet the following criteria as validated by showing evidence during certification audit:

- Must operate on a 24x7 schedule, either as a single entity or through a "follow-the-sun" coverage model
- Must follow operations and service delivery methodologies based upon an accepted industry standard such as the Information Technology Infrastructure Library (ITIL) framework
- Must employ a consistent process for handling and passing cases between the CoE and the remote country or countries as documented in the Service Desk and Incident Management Procedures.
- CoE and all countries utilizing the CoE must share the same IT infrastructure and tools
- Participating countries must have visibility through tools to real-time information on the status of cases as verified via the Call Tracking System.
- Partner can have more than one CoE 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 CoE (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, online and onsite response
- Integrated call tracking system with transparent escalation process (system must meet all program requirements)as shown via Escalation Process and documentation of TAC involvement
- Resources providing technical support must be available in the local language of the country being supported, as defined by SLA or one of the key international languages such as English, Spanish, French, Japanese, Chinese, Portuguese

During the CoE audit the partner must:

- Provide an overview of certified engineers providing remote support
- Outline lab equipment strategy and sparing strategy, including relationship to architectures and/or specializations in remote countries
- Demonstrate an 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 CoE CCIE's designated to support the remote country and how the management of both the CoE 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 CoE)
- Demonstrate that the lab is equipped to support the various remote country architectures/specializations
- Demonstrate the central lab's remote access capabilities and access across the different countries Demonstrate that support personnel in the CoE and the remote country seeking certification have full access to the call-tracking system in order to enter and update cases
- Provide the ratio assigned to in-country engineers versus remote counties supported as per role sharing requirements.
- Demonstrate consistent connectivity in accessing the lab and call tracking systems remotely particularly in the event of poor network infrastructure locations. Please provide process of how support continuity is managed, showing 24/7 support, if connectivity should be compromised.
- Demonstrate the CoE has technical personnel on duty to support customers in all languages of the supported remote countries (A duty roster for the local CCIE's must be presented to the auditor for review)

At the time of the audit the following CoE evidence will be validated:

- Monthly Service Reports, Records of KPI's, analytics and any additional tracking reports
- Random selection of contracts reviewed
- Partner must provide a list of resources from the CoE that are associated to support the remote countries, including names, title, CSCO id and the remote country location receiving the support of the resource from the CoE. This list will not include resources used to support the CoE certification.
- Lab Equipment for Partner Branded Services (Collaborative) Partners Equipment necessary to satisfy the demonstration and post-sales lab requirements for certification and specialization can be located in the CoE if the following criteria are met:

- Engineers in the remote country must have full access to equipment located in the CoE (on a 24-hour basis for Gold certified countries). Partner will be required to demonstrate this during the audit
- If a remote country is not using a designated CoE, all required equipment must be located in the remote country.
- If a partner utilizes a centralized lab (in a CoE) for achieving certification and/or architectures/specialization in remote countries, the CoE lab access and policy will be audited in concurrence with the remote country Certification Audit.

Audit Requirements: Remote Country Using Center of Excellence (CoE) Support
If a country operation seeking certification is using a CoE in another country, the following audit requirements apply (in addition to the standard audit itinerary):

- Partner must provide adequate documentation of the support processes managed between the CoE and the remote country seeking certification, including but not limited to, passing of cases between the two organizations. The audit will include a review of the implemented incident procedures across the organizations.
- Partner must provide evidence that the CoE CCIE's and/or SE's designated to support the remote country, as well as the management of both the CoE and support organization of the remote country are incorporated in the escalation process. This can be demonstrated in two sample cases.
- Partner must demonstrate that support personnel in the CoE and country seeking certification have full access to the call tracking system in order to enter and update cases
- Partner must provide evidence of execution of CoE recommendations at end customer installation.
- Partner must provide documented process outlining seamless escalation process to CoE.

Review of Service Desk and Incident Management Procedures:

- 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

A3.12 Language Requirements

Policy regarding language requirements for audit documents.
Applies to: G,S, Collab, Sec, CB, M, A, E (See Table)
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 Cisco account team in country in which the partner is applying.
If neither the auditor nor a Cisco employee can qualify the documents, the partner will be asked to translate them into English.

A3.13 Cloud and Managed Services Finance Policies and Procedures

Policy regarding discounts and rebates granted for program participation.
Applies to: M, A, E (See Table)
Partner CMSP Rewards Enrollment
Partners must enroll in either:
a) Simplified Pricing (available for CMSP Master and Advanced partners who offer at least one Cisco Powered service); or,
b) Use their Cisco Cloud and Managed Services Program tier discount structure and enroll in Cloud and Managed Services (CMS) track in Cisco's Value Incentive Program (VIP) every six months to earn payments on eligible cloud and managed booking.

Discount Structure
a) Simplified Pricing: Partners that desire a simple, consistent way to receive CMSP rewards may leverage Simplified Pricing and receive pre-approved, upfront equivalent discounts as set forth in the table below for eligible cloud and managed business, with no other additional payments or incentives except trade-in credits. This pricing may not be used for non-cloud/managed (resale) business. Partner may enroll in Borderless Network, Collaboration, or Data Center tracks to earn VIP payments for resale business. See Cisco Simplified Pricing for more information.

	Region	Area	Master CMSP	Advanced CMSP	Pricelist
1	EMEAR	Central Europe, Europe Austria, Europe France, Europe Germany, Europe Italy,	56%	52%	EMEA Global Price List

	Region	Area	Master CMSP	Advanced CMSP	Pricelist
		Europe Mediterranean, Europe North, Europe Switzerland, Europe UK			
2	EMEAR	Emerging Central, Emerging East	56%	52%	Global Price List Emerging
3	EMEAR	Russia	56%	52%	Global Price List Russia
4	Americas	US	54%	50%	Global Price List US Availability
5	Americas	Canada	54%	50%	Canadian Price List in CAN$
6	Americas	Brazil, Cansac, Mexico, SAS	53%	50%	Global Price List Latin America Availability
7	APJC	Anz-New Zealand, Asia (New Zealand, Thailand, Singapore)	54%	50%	Global Asia Pac Price List in US$
8	APJC	Asia, India (India, Philippines, Vietnam, Hong Kong, Taiwan)	56%	52%	Global Asia Pac Price List in US$
9	APJC	Asia (Indonesia, Korea, Malaysia)	57%	53%	Global Asia Pac Price List in US$
10	APJC	Greater China (China)	72%	69%	China Price List in US$
11	APJC	Anz-aust (Australia)	63.20%	60.10%	Australia Price list in AUD Ex-Tax
12	APJC	Japan	54%	50%	Nihon Price List in US$
13	APJC	Japan	54%	50%	Nihon Price List in Japanese Yen

NOTE: CMSP Express partners are not eligible to participate in Simplified Pricing.

b) CMSP with VIP: Alternatively, partners may use their CMSP tier discount structure and be eligible to enroll in Cloud and Managed Services (CMS) track in Cisco's VIP Program. If Partner chooses to enroll in the CMS track of VIP, partner is precluded from also enrolling in Simplified Pricing. See Cisco VIP Program for more information.

If partner chooses to use its Cisco Cloud and Managed Services Program discounts, Partner will be eligible to combine any available worldwide channel incentives that the Partner is eligible to receive (e.g. OIP, TIP, SIP, TMP).

The available discount at which a partner may purchase cloud or managed service Customer Premises Equipment (CPE) product is dependent upon the level/tier at which the partner has been approved (see below). Discounts are applicable only when buying direct from Cisco. Purchase pricing when buying from distributor are to be negotiated directly with them.

- Cloud and Managed Services Level I (Master) Discount: 42 percent off of Global Price List (GPL)
- Cloud and Managed Services Level II (Advanced) Discount: 40 percent off of GPL
- Cloud and Managed Services Level III (Express) Discount: 36 percent off of GPL

CMSP discounts will be available only for eligible cloud or managed service CPE. Product purchased through CMSP for a partner's internal use, core infrastructure, or resale without the provision of a Cloud or Managed Service that is managed directly by the CMSP partner's Data Center or Network Operating Center (NOC), are not eligible under the program. If Cisco discovers that the partner has ordered Cisco product and services for the aforementioned non-Managed/Cloud Services intended uses under the guise of CMSP, the partner risks having all pending rebates cancelled in part or in whole and participation in CMSP terminated by Cisco.

Valid Ordering Process

- All orders placed directly with Cisco must be submitted with Service Provision Use or Managed Services selected in the Intended Use field. Orders that are not submitted with "Service Provision Use or Managed Services" will not be granted the CMSP program's up-front discounts or the back-end net rebate where applicable. Retroactive credit will not be granted for orders placed incorrectly.
- All orders placed via Cisco distributors must be submitted with a valid CMSP DART (Deviation Authorization Request Tool). Orders that are not submitted with a valid CMSP DART will not be granted the program's up-front discounts nor the back-end net rebate where applicable. Retroactive credit will not be granted for orders placed incorrectly.

Discount & Rebate Eligibility

CPE will only be eligible for discounts and rebates if it is directly tied to a Cloud or Managed Service contractual arrangement between the CMSP partner and end users with terms of no less than 1 year where the partner pro-actively monitors the eligible CPE or cloud solution from a NOC.

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

Partners are responsible for keeping their own sales information. Cisco will provide partner access to program results via the CMSP tool. If partner believes there are any discrepancies between Cisco published bookings and its own records, it is 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 CMSP is dependent on partner enrollment in the "CMSP Rewards" option and are not eligible for any other Cisco rebate program unless otherwise stated by Cisco.

Partner Tax Liability
The back end rebate is considered by Cisco as reimbursement for partner's eligible CPE purchases. It may be that according to legislation in the countries in which partner operates, Partner is required to issue a tax invoice and/or pay (indirect) tax on the rebate cash amount paid by Cisco. It is the sole obligation of the partner to investigate any tax and administrative requirements. The reimbursement as paid out by Cisco is inclusive of any and all taxes that may be due by the partner. Cisco will not pay any indirect taxes on top of the agreed rebate.

Combination with other Programs and Rebate Stacking with Non-Standard Pricing Deals (i.e., DSA/MDM)
If partner is enrolled in CMSP Simplified Pricing, review Cloud and Managed Services Program (CMSP) – Simplified Pricing Terms and Conditions.

If partner is enrolled in Cloud and Managed Services track in VIP and not enrolled in Simplified Pricing option (a) listed above, CMSP rebates and/or discounts **cannot be** combined with any of the following:

- Cisco EUP promotions
- Infrastructure discounts
- Advanced Services

CMSP rebates and/or discounts **may** be combined with any of the following:

- Trade-In Migration Program (TMP) subject to theater availability
- Solution Incentive Program (SIP)
- Opportunity Incentive Program (OIP)
- Teaming Incentive Program (TIP)
- Value Incentive Program (VIP)
- Special product incentives or promotions if noted in the promotional terms and conditions
- Non-standard pricing agreements as registered through Deal Specific Agreements (DSA/MDM) are subject to the terms and conditions as provided by the in-theater Cisco controller. These terms may affect a partner's eligibility to use additional incentives or qualify for program rebate.
- Combination does not imply discount stacking from one program to another. Specific rules apply to program combinations and vary on a program-by-program basis. Please see your account manager or WW program team for specific instructions on program combinability.

CMSP Order Level Audit Policy (ALL partners are subject to this requirement)

- Cisco reserves the right to audit any and all orders made under CMSP.
- These order level audits are separate from the up-front CMSP enrollment and certification audit.
- The goal of this audit is to validate that orders which earn program incentives are in full compliance with the order eligibility requirements set forth in this document.
- Where applicable, the goal of the audit is also to validate that the monthly Point-of-Sale reports Partners provide Cisco are accurate and truthful.
- These order level audits will be conducted periodically by Cisco finance representatives and may be conducted onsite with the Partner or remotely.
- Partners should expect to be audited within 12 months of showing initial activity in the program.
- Thorough audits may be conducted annually thereafter or more frequently if program abuse is suspected.
- Spot audits of specific orders may be conducted at any time.
- In these audits a sampling of orders will be examined to verify several key points for each selected order:

- Accuracy of end user information (is a true end user with whom the partner has an CMSP eligible Cloud or Managed Service tied to the order and if applicable, is the true end user consistent with the end user specified in the PoS reports)
- Existence of a one year or greater Cloud or Managed Service contract with the end user (is the order tied to a valid contractual agreement with the true end user)
- Truly managed CPE (is the order being managed by the partner's Network Operating Center)
- Accuracy of order fulfillment (has the order been deployed and shipped to a legitimate end customer)

A sample size of up to 10 percent of all transactions will be randomly selected by Cisco Finance for the order level audits. For these transactions the specified documentation above has to be provided to Cisco to ensure that the transaction has complied with the main criteria by which Cisco defined within the program what is a Cloud or Managed Service offering. Based on the audit outcome, the accrued rebate amount will be corrected and additional, follow-up audits may be conducted.

CMSP Order Level Audit Documentation
For each of the orders selected for audit, copies of the following pieces of evidence will be requested for Cisco to retain, review and document:

- An end user agreement directly tied to the order with terms no less than 1-year to purchase CMSP designated Cloud or Managed Services from the partner with those Cloud or Managed Services being managed from the CMSP partner's data center or managed from their NOC.
- An invoice that specifies the end user has requested to purchase Cisco CPE for eligible Cloud or Managed Service(s) (e.g., a sales order/invoice document from the partner to the customer) or evidence that ties together the customer's Cloud and Managed Service agreement/contract and the Cisco CPE sold if the eligible Cloud or Managed Service is not specified in the customer agreement.
- A confirmation that the Cisco CPE in question has shipped to the end user (e.g., bill-of-lading specifying the end user details and the shipped CPE or a FedEx/UPS/DHL tracking number that confirms shipment).

All order level audits, documentation requested therein, and PoS data will be subject to standard Non-Disclosure Agreements as defined by the partner and/or Cisco.

PoS Requirement Policy (ONLY partners who place CMSP orders with Cisco or Cisco distributors where a true, eligible end user is not identified at the up-front point of order will be subject to this requirement or for partners who sell their cloud offers)

- Secondary PoS information must be provided on a monthly basis. By the 15th of each month, the partner will provide Cisco with PoS information for all orders placed in the prior month under CMSP where valid end user information was not provided to either Cisco or the Cisco distributor initially at the time of order.
- PoS CPE data will be mailed to the secure Cisco address: **cmsp_pos_data@cisco.com**

Please note that there are separate templates for PoS related to Cloud Services. One template will be used to capture Total Committed Units for a contract and the other to capture activations/consumption of the cloud services.

- Cisco may provide the partner with a list of CMSP orders for which it requires secondary PoS data.
- It is the responsibility of the partner to provide PoS information consistent with the PoS template found at www.cisco.com/go/cmsp.

Partners risk losing all incentives, outstanding rebates and continued enrollment in the program if required PoS is three or more months past due.

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 CPE rebates due to the partner will be put on hold and potentially cancelled. 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 (the 15th of any applicable month). If a valid explanation for the delay in PoS submission is accepted by Cisco, the partner will have an additional 30 days to recover and provide up to date PoS reporting information.

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 the potentially granted additional 30 days the partner still has not provided the required PoS data, any outstanding rebates will be permanently and irrevocably 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 only for the program period in which the PoS has become current.

Program Modifications & Governance Summary
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 and all related incentives and rebates for orders that do not comply with the intent of this program.

CPE Rebate is based on meeting the full payout criteria (Order Eligibility, Order Level Audit, PoS, etc.) detailed above.
Net bookings are used to qualify partner for CMSP revenue requirement. Net Bookings is equivalent to CMSP period bookings less CMSP period de-bookings. Bookings are recognized when an 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 specific 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 Cloud and Managed Services Program.

If the partner has an accounts receivable statement that is overdue by 15 days or more, the CMSP rebate will be withheld until the account is made current. Cisco reserves the right to add or remove cloud and 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 theater where net bookings/shipments originated. Enrolled partners should provide the appropriate bank routing information within each of the applicable regions and/or theaters.

Appendix 4: Partner Certification and Specialization Program Terms & Conditions

CISCO CHANNEL PARTNER PROGRAM

17-Nov-2014

These Terms and Conditions (the "Terms") are binding between Cisco and the company you listed in the applicable Certification and/or Specialization Application ("Company"). These Terms set forth the requirements for obtaining and maintaining the applicable certification (Gold, Silver, Premier, and Select) or specialization offered under the Cisco® Channel Partner Program and supplement the most current resale agreement in effect between Cisco ® and Company ("Agreement"). “Cisco” means the Cisco entity with which Company has entered into Agreement.

I. General Terms:

1. **Receiving Benefits**. Company's receipt of the benefits associated with a particular certification or specialization, including but not limited to additional discount, constitutes Company's continuing representation that it is in compliance with all specialization and certification requirements of the specialization or certification level for which Company has received benefits. In the event that Company receives specialization or certification benefits to which it is not entitled by reason of its failure to maintain particular specialization or certification requirements, and/or disclosing false or misleading information, Cisco reserves the right to revoke such specialization or certification and require Company to repay any financial benefits received directly or indirectly from Cisco as a benefit of that specialization or certification, including but not limited to additional discount.
2. **Changes to Program Requirements**. Cisco may change certification and specialization requirements as it deems appropriate and shall notify Company of any such changes, which notice may be through posting on the Cisco Channel Partner Program Website. Such changes may adversely impact Company's ability to qualify for specialization or certification. Any such changes to the specialization requirements will not affect Company's corresponding specialization for the remainder of the current 12-month specialization term. In addition, any such changes to the certification requirements will not affect Company's corresponding certification for the remainder of the current 12-month certification term. Cisco will provide Company with a minimum of 90 days’ notice prior to the effective date of any such changes.
3. **Non-Compliance**. If, while Company is specialized or certified, Cisco becomes aware that Company is no longer in compliance with the applicable specialization or certification requirements, Cisco reserves the right to revoke the specialization or certification. Cisco will notify Company of its non-compliance promptly, but in no event more than thirty (30) days after Cisco first becomes aware of Company’s non-compliance. Upon receipt of such notice, Company may qualify for an extension of time in which to become compliant with the applicable specialization or certification requirements. Company's failure to request an extension may disqualify Company from receiving such an extension. If no extension is granted or if Company fails to comply with the certification or specialization requirements by the end of the extension period, Cisco reserves the right to revoke the applicable specialization or certification immediately. Cisco may monitor Company's compliance with the applicable specialization or certification requirements of a previously granted specialization or certification at any time. If Cisco believes Company may no longer be in compliance with these requirements, Cisco reserves the right to conduct an audit (either onsite or remotely) of Company's qualifications at any time upon fifteen (15) days prior written notice.

II. Attaining and Maintaining Certification:

1. **Certification and Audit Requirement**. For each certification level, Company must meet the applicable requirements listed at **www.cisco.com/go/channelprograms** ("Certification Requirements"). Company acknowledges that each certification requires an audit by Cisco to assess Company's compliance with the certification requirements for the particular certification. Audits may be performed by Cisco personnel or independent third-party contractors retained by Cisco ("Auditor"). Auditor will not be a competitor of Company. Cisco or Auditor will enter into Cisco's standard Mutual Non-Disclosure Agreement with Company at Company's request.
    a. Audits for Gold and Silver Certification may require Cisco or Auditor to visit Company's site.
    b. Audits for Premier and Select Certifications are typically conducted without Cisco or Auditor visiting Company's site. However, Cisco reserves the right to require an audit (either onsite or remotely) before awarding or renewing a Premier or a Select Certification. In addition, Cisco will conduct random audit samplings for Premier and Select Certification when deemed appropriate.
2. **Audit Schedule**. Company will typically be audited once per certification year. If Company is already certified, Cisco will attempt to schedule Company's re-certification audit as close as possible to the anniversary date of Company's initial certification date.
3. **Audit Cancellation**. Audit cancellations and scheduling changes made by a Company are subject to associated cancellation/change fees as defined by the 3rd party auditing firm contracted by Cisco. All processes related to cancellation/change fees will be managed directly by the 3rd party auditing firm.
4. **Audit Compliance**. Company agrees to comply with reasonable informational requests made by Auditor, including but not limited to providing accurate responses to questions from Auditor and furnishing appropriate documents, including but not limited to verification of employment status for the Company employees that Company has identified as possessing individual Cisco Career Certifications (e.g., CCIE, CCNA, CCDP).
5. **Certification Decision**. Cisco shall decide whether or not to certify Company. No statements by Auditor or its personnel are binding upon Cisco.
6. **Award and Renewal of Certification**. Cisco shall base its Certification decision on Company's ability to meet all the certification requirements in effect on the date Company submits a valid application for certification or renewal. Company must renew its certification annually based on the current certification requirements in effect at that time.

III. Attaining and Maintaining Specialization:

1. **Specialization and Audit Requirements**. For each specialization, Company must meet the applicable requirements listed at **www.cisco.com/go/specialization** ("Specializations Requirements"). Company acknowledges that each specialization requires an audit by Cisco to assess Company's compliance with the specialization requirements for the particular specialization. Audits will typically require individuals to pass pre-defined exams. However, Cisco reserves the right to require audits (either onsite or remotely) by Cisco personnel or Auditor.
2. **Audit Schedule**. After the initial specialization audit, Company may be audited annually, on or before the anniversary of the date that the specialization was first granted.
3. **Audit Compliance**. Company agrees to comply with reasonable informational requests made by Cisco, Auditor or testing agencies providing accurate responses to questions from Auditor and furnishing appropriate documents, including but not limited to verification of employment status for employees of the Company that Company has identified as possessing individual Cisco Career Certifications (e.g., CCIE, CCNA, CCDP).
4. **Award and Renewal of Specialization**. Specialization designations are awarded for a period of one year. Every 12 months, Company must apply to renew each specialization. Cisco's initial and renewal decisions for each specialization will be based on the Company's ability to meet the applicable specialization requirements in effect on the date that Company submits a valid application for specialization or renewal.

Appendix 5: Cloud and Managed Services Program (“CMSP”) Program Terms and Conditions

The Cloud and Managed Services Program (“CMSP”) terms and conditions set forth herein and in the CMSP Audit and Policies Document (collectively the “Terms”) are between the company you listed in the applicable CMSP Application ("Partner") and the Cisco Systems entity(ies) (“Cisco”) in which Partner has entered into a Cisco Indirect Channel Partner Agreement (“ICPA”) with or other Pre-Existing Resale Agreement (“Resale Agreement”) (Collectively referred to hereafter as the “Agreement”). The Terms set forth the requirements for obtaining and maintaining the applicable level/tier offered under the CMSP and supplements the most current Agreement in effect between Cisco and Partner. All capitalized words have the meaning ascribed to them in Appendix 1 (“Definitions”) or as defined in the CMSP Audit and Policies Document or the Agreement.

The terms of the Agreement are incorporated herein by this reference. In the event of a conflict between the Agreement and the Terms, the Terms shall take precedence with regard to the subject matter herein.

1. **Receiving Benefits**. Partner's receipt of the benefits associated with a particular level/tier, including but not limited to rebate and/or discount, constitutes Partner's continuing representation that it is in compliance with the Terms including all certification requirements associated with the level/tier for which Partner has received benefits. In the event Partner receives program benefits for which it is not entitled by reason of its failure to maintain certification requirements, and/or providing false or misleading information, Cisco reserves the right to revoke Partner’s program status and require Partner to repay such financial benefits received directly or indirectly from Cisco as a program level/tier benefit, including but not limited to repayment of any additional discounts provided. All Partners, regardless of their business model, are required to meet the same program requirements.
2. **General Terms.** CMSP is available globally pursuant to the Terms. Product must be purchased only from authorized sources as set forth in Partner’s Agreement. In addition to any of its other remedies, Cisco reserves the right to terminate a Partner from participation in the CMSP for the following reasons: (a) submission of false, misleading, or incomplete CMSP information, including inaccurate claims for sales made under the CMSP; (b) fraud or abuse of CMSP or other Cisco marketing or sales programs; (c) the distribution of Cisco Products purchased from an unauthorized source as set forth in Partner’s Agreement; and, (d) the sale of Cisco Products to anyone other than an End User as defined in Partner’s Agreement. Cisco reserves the right to use third parties, who will act on behalf of Cisco to perform administrative functions of the CMSP. Partner agrees that for so long as it participates in the CMSP, when Partner purchases Customer Premises Equipment (“CPE”) for use in any Managed or Cloud Service offered by the Partner to End Users, Partner shall do so pursuant to the CMSP and its Agreement and shall not purchase CPE for use in a Managed or Cloud Service pursuant to any infrastructure purchase agreement with Cisco. Partners who participate in Cisco’s Specialization or ATP Program must abide by all Specialization or ATP rules. Product(s) covered under Cisco’s Specialization or ATP program and available by way of selective distribution must meet all Specialization or ATP program requirements for both bill to and ship to countries.
3. **Changes to CMSP.** Cisco may modify or cancel CMSP (including changes to the program level/tier requirements) as it deems appropriate and shall notify Partner of any such changes, which notice may be through posting on the Cisco Channel Partner Program Website. Such changes may adversely impact Partner's ability to qualify for program level/tier status. Any such changes to the program requirements will not affect Partner's corresponding program authorization for the remainder of the current 12-month term. Cisco will provide Partner with a minimum of 90 days notice prior to the effective date of any such changes.
4. **Non-Compliance with program level/tier Requirements.** If Cisco becomes aware that a Partner is no longer in compliance with the applicable requirements, Cisco reserves the right to revoke the program authorization. Partner agrees to promptly notify Cisco of any non-compliance with the applicable certification requirements, but in no event more than thirty (30) days after Partner first becomes aware of its non-compliance. Upon receipt of such notice, Cisco may in its sole discretion, provide Partner with a grace period in which to renew its compliance with the applicable certification requirements. Partner's failure to provide notice of non-compliance may disqualify Partner from receiving such grace period. If no grace period is granted or if Partner fails to comply with the requirements by the end of the grace period, Cisco reserves the right to revoke the applicable program status immediately or reclassify the eligible program level/tier. Cisco may monitor Partner's compliance with the applicable requirements of a previously granted program authorization at any time. If Cisco believes Partner may no longer be in compliance with the applicable certification requirements, Cisco reserves the right to conduct an onsite audit of Partner's qualifications at any time by providing fifteen (15) days prior written notice.
5. **Cisco Powered Logo Defined Terms.** “Cisco Powered Logo” means the logo which Partner may use to communicate that its Managed or Cloud Services are designated as Cisco Powered Managed Services or Cisco Powered Cloud Services (collectively known as “Cisco Powered Services”). “Cisco Powered Logo usage Guidelines” means the guidelines, which may be amended from time to time by Cisco in its sole discretion, for usage of the Cisco Powered Logo and the Designation Descriptor. “Designation Descriptor” means the Cisco pre-defined language which Partner may use in

conjunction with the Cisco Powered Logo trademark(s) to promote Partner's Cisco Powered Services designation status once Partner has achieved such designation.

6. **Logo License and Permission to Use Designation Descriptor Logo License.** Upon obtaining Cisco Powered Services designation status from Cisco, Cisco grants Partner a worldwide, nonexclusive, nontransferable, royalty-free, personal license to use the Cisco Powered Logo solely in connection with the Partner's service(s) which has met the applicable designation requirements and solely in the manner described in the Cisco Powered Logo usage Guidelines. Partner acknowledges that the Cisco Powered Logo is owned solely and exclusively by Cisco and Partner hereby acknowledges and agrees that, except as set forth herein, Partner has no rights, title or interest in or to the Cisco Powered Logo and that all use of the Cisco Powered Logo shall inure to the benefit of Cisco. Partner agrees that it will not adopt or use or attempt to register the Cisco Powered Logo or any confusingly similar mark. The license set forth herein supersedes any other license terms for the Cisco Powered Logo agreed to by Partner for the service(s) which have met the applicable Cisco Powered services designation requirements.
7. **Designation Descriptor**. Upon obtaining applicable designation status from Cisco, Cisco grants Partner the right to use the Designation Descriptor with the Cisco Powered Logo subject to the Logo License above and solely in connection with the Partner's service(s) which has met the applicable designation requirements and solely in the manner described in the Cisco Powered Logo usage Guidelines. Cisco reserves the right to review and approve prior to publication the form and content of advertising or promotional materials containing the Cisco Powered Logo and Designation Descriptor. Partner agrees to cooperate fully with Cisco in the review and shall use all commercially reasonable efforts to promptly make modifications in such materials as necessary to conform to the logo and Designation Descriptor guidelines. The right to use the Cisco Powered Logo and the Designation Descriptor will terminate no later than termination or expiration of the Agreement. Notwithstanding the foregoing, Cisco reserves the right to take action against any use that does not conform to these requirements; that infringes on Cisco's intellectual property or other rights; or that violates other applicable law. In any and all such cases, Cisco reserves the right to terminate the Partner's right to use the Cisco Powered Logo and the Designation Descriptor.
8. **Indemnification.** Partner will defend, indemnify and hold harmless Cisco and its officers, directors, employees, shareholders, customers, agents, successors and assigns from and against any and all loss, damages, liabilities, settlement, costs and expenses (including legal expenses and the expenses of other professionals) as incurred, (i) resulting from or arising out of Partner's use of the Cisco Powered Logo and the Designation Descriptor in connection with its services, business or products in any manner, including, without limitation, customer or user claims regarding misrepresentation, false advertising or breach of implied warranty and ii) anything related to Partner's services including but not limited to third party claims that Partner has not met its service level agreements or any contractual obligations or representations or warranties made between Partner and its customer or that Partner's service does not meet certain performance or other specifications or that the services do not meet the Cisco Powered Services or other applicable certification requirements. As a condition to such defense and indemnification, Cisco will provide Partner with reasonably prompt written notice of the claim and sole control of the defense and settlement of the claim. Cisco may employ counsel at its own expense to assist it with respect to any such claim.

9. RESPONSIBILITIES OF CMSP PARTNERS WHO OFFER CMSP CLOUD AND MANAGED SERVICES THROUGH CMSP SERVICES RESELLERS:

9.1 RESPONSIBILITIES OF CISCO POWERED SERVICES RESELLER, CLOUD AGGREGATORS AND THE CMSP PROVIDER

The CMSP Provider must at all times be in compliance with CMSP, their Agreement and the terms set forth herein. The Cisco Powered Services Reseller must at all times be in compliance with their Agreement and the terms set forth herein. The Cloud Aggregator must at all times be in compliance with the terms set forth herein.

Falsifying, or failing to disclose information in order to obtain a higher level of CMSP discounts, branding, or benefits may result in immediate termination of such partner's right to participate as a CMSP Provider, Cloud Aggregator or Cisco Powered Services Reseller.

A CMSP Provider entering into a Cisco Powered Service resale relationship with a Cisco Powered Services Reseller must enter into a contractual agreement with such CMSP Service Reseller outlining the responsibilities and deliverables of both parties. A Cloud Aggregator entering into a Cisco Powered Cloud Service resale relationship with a Cisco Powered Services Reseller (on behalf of a CMSP Provider) must enter into a contractual agreement with such CMSP Service Reseller outlining the responsibilities and deliverables of both parties. Such deliverables may include a service activation kit, hardware, software, End-User right to use licenses for the duration of the service contract (as authorized in the CMSP Provider's respective Agreement with Cisco), software updates, management configuration change administration, End User facing web portal, standard reports, training, access to subcontractor services, documented incident tickets, documented change requests, and operational reports. This contractual agreement and relationship are exclusively

between the CMSP Provider (or Cloud Aggregator on behalf of the CMSP Provider) and the Cisco Powered Services Reseller.

The Cisco Powered Services Reseller and CMSP Provider (or Cloud Aggregator on behalf of the CMSP Provider) must establish a set of escalation procedures including priority levels, procedures, and associated penalties, if missed.

The Cisco Powered Services Reseller and CMSP Provider (or Cloud Aggregator on behalf of the CMSP Provider) must establish a change control process for handling End User changes and a change control process for managing changes between the Cisco Powered Services Reseller and the CMSP Provider.

9.2 RESPONSIBILITIES OF THE CISCO POWERED SERVICES RESELLER

9.2.1 Either the Cisco Powered Services Reseller or CMSP Provider (as agreed between the Cisco Powered Services Reseller and CMSP Provider) shall designate a primary single point of contact to whom communications in regards to the Cloud Services and/or Managed Services may be addressed and who has the authority to act on all aspects of the Cloud Services and/or Managed Services.

9.2.2 Either the Cisco Powered Services Reseller or CMSP Provider (as agreed between the Cisco Powered Services Reseller and CMSP Provider) shall be available during Standard Business Hours and shall designate two backup contacts for when the primary single point of contact is not available. Hereafter, the single point of contact will be deemed the Customer Relationship Manager.

9.2.3 The Cisco Powered Services Reseller may: a) market the CMSP Provider's Cisco Powered Services acting on behalf of the CMSP Provider as a referral agent; and/or, b) sell the CMSP Provider's Cisco Powered Services: 1) acting on behalf of the CMSP Provider reselling such services directly to End Users under the CMSP Provider's brand; or, 2) acting as an OEM reselling such services as its own.

9.2.4 Either the Cisco Powered Services Reseller or CMSP Provider (as agreed between the Cisco Powered Services Reseller and CMSP Provider) shall own the Service Level Agreement with the End User, including associated penalties.

9.2.5 Where the Cisco Powered Services Reseller is responsible for product procurement, sales, and installation of Cisco equipment, they must have the appropriate credentials to obtain the Cisco Products including but not limited to an Agreement with Cisco and the appropriate Cisco certification, specialization, or ATP.

9.2.6 Either the Cisco Powered Services Reseller or CMSP Provider (as agreed between the Cisco Powered Services Reseller and CMSP Provider) must have comprehensive monitoring policies to apply to the Cisco devices to fulfill the obligations under the Service Descriptions and SLAs.

9.2.7 The Cisco Powered Services Reseller must provide details of service coverage.

9.2.8 The Cisco Powered Services Reseller shall create a Marketing Services Description (MSD). The MSD is a document produced by the Cisco Powered Services Reseller that describes the service offered and what features and benefits it provides. The MSD must be a published document.

9.3 GOVERNANCE.
Cisco shall have no obligations or liability arising from the transactions arranged between the CMSP Provider, Cloud Aggregator and the Cisco Powered Services Reseller.

9.4 CISCO SERVICES.
Where the Cisco Powered Services Reseller is responsible for product procurement and sales, the Cisco Powered Services Reseller shall attach Cisco Services to their (CPE) product sales. The Cisco Services may be procured either from Cisco or through a Cisco authorized distributor based on their services relationship as outlined in their Agreement.

DEFINITIONS

Cisco Powered Services Reseller refers to either a Cloud Services Reseller or Managed Services Reseller who has entered into a contractual relationship with a CMSP Partner for resale of Cisco Powered Cloud Services or Cisco Powered Managed Services respectively.

Network means a set of interconnected and inter-working Cisco supported hardware and software that is implemented, operated, and supported by CMSP Partner from a single Network Operations Center (“NOC”).

On Site means the Services are to be performed at the End User location (“Site”).

CMSP Partner means a Cisco partner that has met and maintains the CMSP requirements.

Standard Business Hours usually means Monday through Friday, 8am – 5pm local time.

NOC Services Provider means a service provider that a CMSP Partner has entered a written contract with (including an SLA with penalties) for the management of its NOC operations.

Appendix 6: Outsourcing NOC Operations

Introduction

CMSP partners may outsource some elements or the entire NOC operations to a single specialized NOC services provider who is not a Cisco competitor. Partner may or may not (owned by NOC services provider) own NOC assets.

Partners who outsource NOC operations are not eligible for an audit waiver; audits are conducted annually to ensure program requirements continue to be met. Should partner change their NOC services provider for any reason at any time, partner must notify Cisco within 30 days prepare for a recertification audit. An audit may be required within 90 days of the change in order to validate that the company continues to meet program requirements for that level/tier.

Below is a summary of program requirements that can be outsourced and the partner can still meet published requirements to be approved into the CMSP Program. CMSP partners who leverage the NOC outsourcing option are still required to meet the requirements of sections 5.2 -5.6. 5.8, 6.1-6.7, 7.1-7.8, and 8.1-8.3 listed below for the Cisco Powered services designation that they are pursuing; MSCP Express partners must also meet the requirements in section 3.3.
NOTE: Partner will receive CMSP level/tier and Cisco Powered Services designation upon audit approval.

Partner Responsibilities

Partners that outsource NOC operations:

- Must not outsource to a Cisco competitor.
- Must meet published requirements for the partner company and for each of the Cisco Powered services.
- Must create (R&D) Cisco Powered services.
- Must own end user customer SLA.
- Must own data center asset to offer all Cisco Powered cloud services, except TelePresence-as-a-Service.
- Must have an executed contract and a current, signed SLA including penalties with a NOC services provider.
- Must upload a NOC integrated process plan during application process and demonstrate objective evidence of definition and implementation during audit.

Prerequisites

A CMSP partner who outsources NOC operations to a specialized NOC services provider must upload a NOC integrated process plan consisting of the following:

- **End-to-end processes:** Flowchart of support process from problem reporting/logging to resolution
- **Systems and tools:** Listing of NOC assets and tools at CMSP Partner and/or NOC services provider sites
- **Support and escalation procedure:** Procedure to guarantee meeting of end customer SLAs in supporting Cisco Powered services offered by CMSP partner
- **Call tracking and monitoring systems between CMSP and NOC services provider:** Listing of call tracking systems used and the integration of the systems between CMSP and NOC services provider's systems
- **Access to CMSP/NOC services provider information (knowledge base sharing):** Description of common repository and access to CMSP related information, solution to customer issues etc., for knowledge base

Auditor validation

Auditor assessment and validation will consist of the following:

- **End-to-end processes**: Requires demonstration of closed loop processes from incident and problem reporting/logging by end customer to resolution by partner of all CMSP and Cisco Powered services related issues
- **Systems and tools**: Evidence of integrated processes between partner and NOC
- **Support and escalation procedure**: Sharing of documented procedures for support and escalation during normal business hours, after hours, and holidays to meet or exceed end customer SLA and SLA report showing evidence of percent of time SLA is met, and root cause analysis and action to resolve when it is not
- **Call tracking and monitoring systems between CMSP and NOC services provider**: Demonstration of secure access by authorized personnel from NOC services provider to the partner's call tracking system and vice-versa.
- **Access to CMSP/NOC services provider information (knowledge base sharing):** Demonstration of sharing of best practices, knowledge base by both CMSP partner and NOC services provider.

NOC Services Provider Responsibilities

- Must have at least 1 ITIL certified employee.
- Must have secure access by authorized personnel to CMSP partner network.
- May or may not be a Cisco Resale or a CMSP partner**.**
- Must provide network and personnel access to the auditor to validate processes, procedures etc. to meet CMSP partner requirements.

Outsourced NOC Services Requirements Overview

Requirement	Cloud & Managed Services		
	Master (M)	Advanced (A)	Express (E)
3 Pre-Sales Requirements			
3.3 Project Management			
3.3.1 Personnel	N/A	N/A	•
3.3.2 Project Plan	N/A	N/A	•
3.3.3 Project Objectives	N/A	N/A	•
3.3.4 Project Charter	N/A	N/A	•
3.3.5 Resource Management	N/A	N/A	•
3.3.6 Customer Requirements	N/A	N/A	•
3.3.7 Project Start Meeting	N/A	N/A	•
3.3.8 Risk Management	N/A	N/A	•
3.3.9 Project Milestones	N/A	N/A	•
3.3.10 Customer Communication Plan	N/A	N/A	•
3.3.11 Project Implementation	N/A	N/A	•
3.3.12 Project Review and Evaluation	N/A	N/A	•
5 Service Design Requirements			
5.2 Service Level Management			
5.2.1 SLAs/SLOs	•	•	•
5.2.2 Service Level Measurement and Reporting	•	•	•
5.2.3 Parts Replacement	•	•	•
5.3 Capacity Management			
5.3.1 Business Capacity	•	•	•
5.3.2 Service Capacity	•	•	•
5.3.3 Resource Capacity	•	•	•
5.3.4 Capacity Improvements	•	•	•
5.4 Availability Management			
5.4.1 Availability Measurement	•	•	•
5.4.2 Availability Reporting	•	•	•
5.4.3 Availability Review and Planning	•	•	•
5.4.4 Availability Improvements	•	•	•
5.5 IT Service Continuity/Disaster Recovery			
5.5.1 IT Infrastructure Monitoring	•	•	•
5.5.2 IT Infrastructure Problem Resolution	•	•	•
5.5.3 Service Continuity/Disaster Recovery Planning	•	•	•
5.5.4 Disaster Recovery Plan Testing	•	•	•
5.6 Information Security Management			
5.6.1 Security Policies and Procedures	•	•	•
5.6.2 Physical Security	•	•	•
5.6.3 Network Security	•	•	•
5.6.4 Server Security	•	•	•
5.6.5 Logical Data Security	•	•	•
5.8 Third Party Contracting (referenced by ITIL as Supplier Management)			
5.8.1 Third Party Contracted Activities and Services	•	•	•
5.8.2 Subcontractor Management	•	•	•
5.8.3 Subcontractor Contracts	•	•	•
5.8.4 Subcontractor Communication	•	•	•
5.8.5 Periodic Subcontractor Reviews	•	•	•

Requirement	Cloud & Managed Services		
6 Service Transition Requirements			
6.1 Transition Planning and Support			
6.1.1 Risk Management	•	•	•
6.1.2 Redundant Management Connection	•	•	•
6.2 Change Management			
6.2.1 Change Management Process	•	•	•
6.2.2 Change Rollback	•	•	•
6.2.3 Requests for Changes	•	•	•
6.2.4 Change Definitions	•	•	•
6.2.5 Standard Change Turnaround Time	•	•	•
6.2.6 Customer-Specific Change Control	•	•	•
6.2.7 Change Manager and Change Advisory Board	•	•	•
6.2.8 Change Management Tools	•	•	•
6.3 Release and Deployment Management			
6.3.1 Release and Deployment Process	•	•	•
6.3.2 Phased Release	•	•	•
6.3.3 Configuration Item (CI) Identification	•	•	•
6.3.4 Software and Hardware Repositories	•	•	•
6.3.5 Release Management Audits	•	•	•
6.4 Service Asset and Configuration Management			
6.4.1 Data Collection Process	•	•	•
6.4.2 Configuration Control Processes and Tools	•	•	•
6.4.3 Configuration Change Plans	•	•	•
6.5 Service Validation and Testing			
6.5.1 Service Validation and Testing Process	•	•	•
6.6 Service Evaluation			
6.6.1 Service Evaluation Process	•	•	•
6.7 Service Knowledge Management			
6.7.1 Information Availability and Accessibility	•	•	•
7 Service Operation Requirements			
7.1 Service Desk Function (Call/Contact Center)			
7.1.1 Customer Service Availability	•	•	•
7.1.2 Local Language Answering	N/A	N/A	N/A
7.1.3 One-Hour Callback	•	•	•
7.1.4 Call Logging	•	•	•
7.1.5 Incident Severity Level	•	•	•
7.1.6 Escalation Process	•	•	•
7.1.7 After-Hours Support	•	•	•
7.1.8 Service Desk Duty Manager	•	•	•
7.1.9 Computer-Based Call Tracking System	•	•	•
7.2 Request Fulfillment			
7.2.1 Service Request Process	•	•	•
7.2.2 Automated Service Request Tool	•	•	•
7.3 Event Management			
7.3.1 Event Management Process	•	•	•
7.4 Incident Management			
7.4.1 Incident Management Process	•	•	•
7.4.2 Managed Device Monitoring	•	•	•
7.4.3 Fault and Performance Data Monitoring	•	•	•
7.4.4 Management Platform	•	•	•

Requirement	Cloud & Managed Services		
7.4.5 Event Correlation	•	•	•
7.4.6 Incident Detection	•	•	•
7.4.7 Incident Logging and Querying	•	•	•
7.4.8 Customer Notification	•	•	•
7.4.9 Notification Methods	•	•	•
7.4.10 Incident Prioritization and Categorization	•	•	•
7.4.11 Stakeholder Updates	•	•	•
7.4.12 Incident Troubleshooting and Investigation	•	•	•
7.4.13 Handoff to Problem Management	•	•	•
7.4.14 Known Error Database	•	•	•
7.4.15 Incident Closure Authorities	•	•	•
7.4.16 Incident Closure Summary	•	•	•
7.5 Problem Management			
7.5.1 Problem Management Process	•	•	•
7.5.2 Root Cause Analysis	•	•	•
7.5.3 Closed Loop Corrective Action	•	•	•
7.5.4 Proactive Problem Management	•	•	N/A
7.6 Access Management			
7.6.1 Access Management Process	•	•	•
7.7 Onsite Response/Troubleshooting			
7.7.1 Onsite Response/Troubleshooting Description	•	•	•
7.8 Remote Troubleshooting Access			
7.8.1 Remote Access	•	•	•
8 Continual Service Improvement Requirements			
8.1 Service Improvement			
8.1.1 Continual Improvement Activities	•	•	•
8.1.2 Continual Improvement Methodology	•	•	•
8.2 Service Measurement			
8.2.1 Service Objectives	•	•	•
8.2.2 Mean Time to Notify (MTTN)	•	•	•
8.2.3 Mean Time to Restore Service (MTRS)	•	•	•
8.2.4 Onsite Troubleshooting Response Time	•	•	•
8.2.5 Customer Perception and Feedback	•	•	•
8.3 Service Reporting			
8.3.1 Service Reports	•	•	•
8.3.2 Cloud or Managed Service Contracts	•	•	•

Appendix 7: Master Security Fire Jumper and Practice Areas

Introduction

The Masters Security Specialization has unique requirements not found in other Specialization. These include having a Fire Jumper on staff and showing evidence of competence in three Security Practice Areas during the on-site audit. The sections that follow provide background and verification information for these requirements.

Fire Jumper

The Fire Jumper program is a recognition and reward framework as well as a mentorship program for Cisco champion pre-sales systems engineers with our partner community. The ideal Fire Jumper is considered to be amongst the best both technically and in salesmanship within a partner organization. Each partner may have a Fire Jumper in each of the four competency areas: Content Threat, Malware Threat, Network Threat, and Secure Access and Mobility. Fire Jumper status is annotated in Cisco internal tools and may be validated by Cisco Channel or Specialization program teams. To learn more about the Fire Jumper program, email us at FireJumper@cisco.com.

To become a Fire Jumper one must:

- Be in good standing with Cisco
- Have a Cisco CSE sponsor
- Be respected and valued within their organization
- Have written support of their leadership
- Achieve Stage 4 in at least one of the competency areas
- Demonstrate loyalty through contribution such as closing a large or complex sale, completing a public speaking engagement, publishing technical documents, or helping a partner to attain specific enablement goals

To maintain Fire Jumper status one must:

- Attend Fire Jumper calls quarterly
- Be the named SE on at least one sale per year
- Assist in elevating skills of peers by delivering training or encouraging them to take self-service training
- Give a presentation or write a technical paper at least once per year or engage in regular discourse on the security partner community (www.cisco.com/go/securitychannels)
- Engage with the Cisco CSE sponsor at least once per month

Practice Areas

In the new Masters Security model, the requirement for a NOC and the majority of the operate phase checklist requirements were removed. Instead of these generic capabilities, Masters Security Partner candidates will validate that they have mature security practice capabilities in three (3) of the following practices areas.

1.Threat Visibility

- Description: Threat Visibility provides awareness of network and application security posture through customer engagements. Threat Visibility reports provide customers with findings to include host and application risks, malware threats, and recommended actions.
- Potential Products & Tools
    - ThreatGrid
    - Talos
    - AMP for Endpoint
    - AMP for Network
    - AMP for Content
    - ESA, WSA, and CWS
    - FirePOWER Services
    - Open Source Offerings
    - Ecosystem Partners

2.Network Vulnerability Assessment

- Description: Network Vulnerability Assessments analyze customer networks with vulnerability scanning and penetration testing tools to provide insight into internal, external, and remote access threats. Assessment reports provide customers with findings to include descriptions of vulnerabilities and recommended corrective actions.
- Potential Products & Tools
    - Identity Services Engine
    - FirePOWER Services
    - Talos
    - Prime Infrastructure
    - IOS Software Checker
    - Open Source Offerings
    - Ecosystem Partners

3.Incident Management

- Description: Incident Management is an organized approach to addressing and managing the aftermath of a security breach. Services include response planning, incident investigation, forensics, infection containment, countermeasure development, and risk mitigation.
- Potential Products & Tools
    - ThreatGrid
    - Talos
    - AMP for Endpoint
    - AMP for Network
    - AMP for Content
    - FirePOWER Services
    - Open Source Offerings
    - Ecosystem Partners

4.Secure Cloud

- Description: Secure Cloud provides or builds a secure environment to meet specific business outcomes including threat protection, acceptable use, data security, secure access, and flexible workloads.
- Potential Products & Tools
    - Talos
    - ESA, ESAv, WSA, WSAv
    - ASA, ASAv
    - FirePOWER Services
    - Identity Services Engine
    - Intercloud Fabric
    - Open Source Offerings
    - Ecosystem Partners

5.Secure Data Center

- Description: Secure Data Center practices address security concerns in virtualized & orchestrated data center environments leveraging Cisco Validated Designs. Cisco solutions offer maximum performance, actionable security, ease of provisioning, and threat detection and defense.
- Potential Products & Tools
    - Application Centric Infrastructure
    - ASA, ASAv
    - FirePOWER Services
    - Identity Services Engine
    - TrustSec
    - Cyber Threat Defense
    - Open Source Offerings
    - Ecosystem Partners

6.Secure IoT

- Description: Secure IoT converges an organization's existing information technology (IT) and operational technology (OT) networks. Cisco offers physical and cyber security solutions to employ consistent security solutions with centralized management across the extended network while offering differentiated security policies and actionable security intelligence.

- Potential Products & Tools
    - AMP for Endpoint
    - AMP for Network
    - AMP for Content
    - Hardened ASA
    - Video Surveillance Manager
    - Physical Access Manager
    - IPICS
    - Open Source Offerings
    - Ecosystem Partners

For each area, Partner candidates will need to provide evidence by sharing the following materials during the onsite audit. Sensitive data may be obscured as required.

- Offer Data Sheet with Business Outcomes
- Sample Statement of Work (SOW)
- One of the Following Sample Deliverables
    - Customer Facing Report with Recommendations
    - Solution Design with Network Topology and Products
    - Service Agreement with SLAs
- Implementation or Operations Guide