Requirements Guide

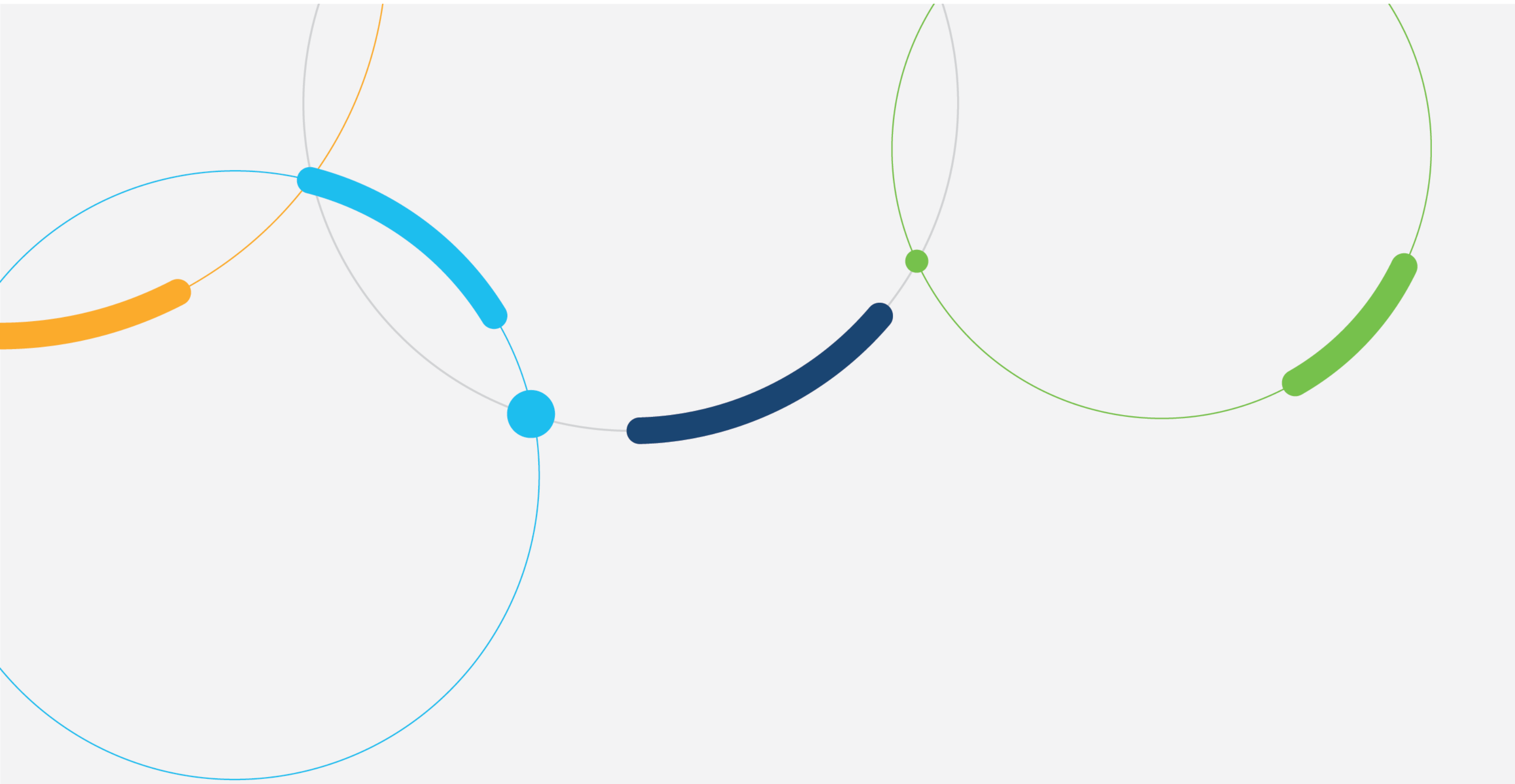
Cisco partner confidential

Cisco Partner Program Audit and Policies Document

Version 7.1 – August 2022

Document Number: EDCS-16475752 (Cisco Internal Tracking Number)

Policy Owner: Global Partner Organization



Policy Purpose: This document provides a detailed list of audit requirements and policies specific to the following Designations: Gold Integrator role (G), Master Specialization: Collaboration (Collab), Security (S), Data Center and Hybrid Cloud (DC), Networking (Net) Customer Experience Specialization (CES); and Provider role: Gold Provider (GP), Premier Provider (PP) and Select Provider (SP). Designation abbreviations (G, Collab, S, DC, Net, CES, GP, PP, SP) are intended only for the reference to requirements in this document specifically and are not to be confused with abbreviations or acronyms used by Cisco outside this document.

Policy Statement: The intent of this document is to serve as a guideline for the competencies and controls the auditor will review during the meeting. It is expected that you will show the auditor how these controls are documented and managed within your company.

If the findings of the audit are such that approval or renewal for the Designation being applied for cannot be achieved within required timelines, the Designation will be denied or removed entirely.

Revision History

Version	Summary of Changes – All Changes Highlighted in grey	Publication Date
6.0	View at www.cisco.com/go/audit/	11/21/2014
6.1	View at www.cisco.com/go/audit/	05/31/2015
6.2	View at www.cisco.com/go/audit/	04/15/2016
6.3	• 1.1 Audit Scheduling – removed Focused Audit Agenda • 1.1 Audit Scheduling – added Partner Capability Review (PCR) • 2.1.4 CSAT – updated low score quantity requirement from 1 or 2, to 1 – 4) • 2.1.5 Service Attach Rate – replaced references of Performance Metrics Central (PMC) with new tool: Total Program View (TPV) • 2.1.7 Hybrid IT Prerequisites – clarified the documentation requirements. • 2.2.2 Personnel – added Prince II Foundation or Practitioner as acceptable options for Master Collaboration and Master Security and contracted CCIE option • A3.6 CCIE/CCDE Hiring and Terminating – added BVP to policy (BVP subsequently removed from Gold requirement on 07-Oct-2017) • 5.6 – Removal of CMSP requirement. • A3.12 Cloud and Managed Services Finance Policies and Procedures – Updated CMSP Simplified Pricing Table. • Appendix 5: Cloud and Managed Services Program ("CMSP") Program Terms and Conditions – Updated Section 9.	04/30/2017
6.4	• Addition of Master Networking Specialization	04/30/2018
6.5	• Update of Master Data Center and Hybrid Cloud, Master Collaboration, and Master Security to new Master audit format	06/30/2018
6.6	• 1.1 Audit Scheduling - Update to a Partner funded model • 1.1 Audit Scheduling – Partner Capability Review (PCR) no longer a requirement for Master Specializations or the Cloud and Managed Services Program • Program Requirements Overview: Audit requirements removed for CMSP Advanced and Express • CMSP Pre-Qualification – Removal of certain requirements for CMSP Express • Appendix 3 - Program Policies – Removal of certain requirements for CMSP Advanced and Express • A3.12 Cloud and Managed Services Finance Policies and Procedures – Removed reference to VIP	09/09/2019

Version	Summary of Changes – All Changes Highlighted in grey	Publication Date
7.0	All changes highlighted in grey • Updated all references related the rebrand of Gold Certification and CMSP to Gold Integrator and Provider roles. • Updated all references of Authorizations to Specializations. • Table abbreviations for Provider role updated to GP (Gold Provider), PP (Premier Provider) and SP (Select Provider) from M, A, E respectively • Table abbreviation for Master Data Center and Hybrid Cloud updated from CB to DC • Updated language throughout to ensure consistency of terms • Updated Introduction and PCR sections • Removed Validation section • Included contact information for Partner to request estimated audit costs • 2.1.2 Specializations - Updated Specialization requirements and options for the Integrator role • 2.2.2 Personnel - Updated Fire Jumper requirement from Level 5 to Level 4 for Master Security • 2.2.8 Third party Credentials - Updated VMware Third-Party credentials for Master Data Center and Hybrid Cloud • 2.1.10 Proof of Value (POV) – Clarified POV documentation requirements • 2.3 Customer Experience – New section • 2.4 Provider role - Requirements moved from 2.3 to 2.4 • 5.7 Hybrid IT - Removed along with all Hybrid IT requirements/references for the Gold Integrator role • A3.5 Mergers, Acquisitions, Divestiture and Affiliates - Government Subsidiary language added • A3.6 - Hiring and Terminating - CSM added • Appendix 4 – Removed (Integrator Terms and Conditions part of application process) • Appendix 5 – General updates	5/5/2021
7.1	All changes highlighted in grey • 1.1 Audit Scheduling - Points Based Renewal section removed and updated PCR requirements for Gold Integrator • 1.4 - Important Timelines -Removed waiting period for failed audits, updated duration for unresolved applications and removed references of points renewal for Master Specializations • 2.1.2 - Specializations - Updated Specialization requirements for the Integrator Role • 2.2.6 – Master Specializations Customer References – Removed Customer Reference requirement for renewals • 2.2.12 - Master Specialization Renewals - Updated requirements • 2.4 Provider Role – Updated Gold & Premier requirements • 4.4 Subscription and recurring billing capabilities (NEW) • Appendix 2: Glossary – Added new Provider Role definitions • A3.5 Mergers, Acquisitions, Divestiture and Affiliates – Updated Government Subsidiary language • A3.6 - Hiring and Terminating – Updated Get-Well Plan duration for CCIE, CCDE and CSM • Appendix 5: Updated Services Reseller Terms	

Contents

Introduction

The Cisco Partner Program

The world is changing, and our customers are increasingly moving to SaaS, managed services, and cloud solutions. The Cisco Partner Program will help you prepare to increase your business agility, grow market relevance, and reach profitability goals through more flexible consumption models and reduced time to value.

The Cisco Partner Program recognizes your agility and the value you co-create with Cisco for your customers. We are expanding your ability to differentiate and showcase your unique value creation strategy. Greater differentiation is brought to all partners by aligning your strengths and unique value drivers with the four roles (Integrator, Provider, Developer, and Advisor) and levels (Gold, Premier, and Select).

The Cisco Partner Program also positions you for opportunities and increased profitability by shifting from a Product lifecycle to a customer lifecycle. Incentives are designed to drive synergy across roles, build on your existing investments, and accelerate value as you expand across multiple roles.

How to use this Document

This document provides a detailed list of audit requirements specific to: the Gold Integrator role (G), Master Specializations: Collaboration (Collab), Security (S), Data Center and Hybrid Cloud (CB), Networking (Net), Customer Experience Specialization (CES), and the Provider role: Gold Provider (GP), Premier Provider (PP) and Select Provider (SP).

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: Plan, Build and Managed (PDM). 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.).

The intent of this document is to serve as a guideline for the competencies and controls the auditor will review during the meeting. It is expected that you will show the auditor how these controls are documented and managed within your company. There is no need to create a power point or additional documentation in preparation for the audit.

1.0 Audit Process and Methodology

1.1 Audit Scheduling

An audit will be scheduled (as applicable) 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.

Effective October 27, 2019, Cisco moved to a partner-funded model. Partner is responsible for the cost of required program entry and renewal audits and reviews (as applicable) for the following programs:

- Cisco Global Gold
- Cisco Global Commerce Specialization
- Cisco Gold Integrator role
- Cisco Provider role
- Cisco Powered Services

- Advanced Customer Experience Specialization
- Cisco Master Specializations

Partner may request an estimated audit cost (and travel costs when applicable) from Cisco's Third-Party audit agency, NSF: supportteam@nsf.org.

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.

Cisco personnel authorized to attend a partner's audit will be noted on the audit confirmation. Cisco 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 renewal

Partners must submit an online application for renewal by their anniversary dates each year. This does not imply audit; however, there are no longer waivers because audits will no longer be conducted every year.

- You may require a Partner Capability Review (PCR) for the Gold Integrator role renewal (see next page)
- If there are no additions (e.g., adding the Provider role or a Cisco Powered Service), no applicable program changes, and compliance is maintained then renewal is complete.
- Exceptions may occur if renewal requirements are not met by the anniversary date of the Designation in question, or at the partner's request. In both instances, a PCR or full audit will be conducted solely at the partner's expense.

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 at risk of having their Designation removed entirely.

Designation

Partner Capability Review (PCR)

As of December 12, 2016, when you renew the Gold Integrator role, you will have a partner capability review (PCR). You will only be required to pass a single PCR three years after you initially achieve Gold Integrator and Global Gold Integrator status. Partners who have maintained their status for more than three years and successfully completed at least one PCR prior to June 29, 2022, will not be required to complete additional PCRs as part of the annual renewal process. The PCR is conducted with our Third-Party consulting firm, NSF International (https://ciscoservices.nsf.org/). For this PCR discussion, we are not expecting a long documentation exercise. Your experts can lead the conversation, as this is part of their daily business. Our intent is to significantly limit the number of hours required to complete documentation to prepare for this audit.

You will still need to file a submission to renew all Designations each year according to the standard process.

When a PCR is required to renew the Gold Integrator role, the PCR must be conducted no later than 60 days after the partner's Gold Integrator anniversary date.

The Partner Capability Review is not a requirement for renewal of Master Specializations or the Provider role (formerly CMSP).

The Partner Capability Review is not an option for a Gold Integrator that has been moved to the next eligible level. If an audit is required to regain the Gold Integrator role, Partner must submit to a regular full audit.

Please review the partner capability review document that outlines requirements, it can be found on the Audit Resource Website at www.cisco.com/go/audit/.

If you have any questions about the PCR, please contact your Certification Program Manager or email: certification-team@cisco.com.

Consulting Services

NSF International, a Third-Party auditing firm, offers a wide range of consulting services including the following:

- Pre-Audit Support—Initial guidance, best practices and gap analysis.
- Audit Preparation—Mid-preparation progress validation, review of previous audit findings, best practices and industry expert recommendations
- Readiness Review—Mock audit review and readiness feedback
- Custom Engagement—Defined by partner needs available on-demand.

A complete overview of the consulting services can be found at: https://ciscoservices.nsf.org/.

1.2 Role of Audit Participants

Role of the partner

Prior to the audit, the partner is expected to review all of the requirements, submit a complete online application with the requested pre-audit documents. On the day of the audit, the Partner is expected to show the auditor how controls are documented and managed with your company for each of the audit requirements specific to the Designation being applied for. Partner should also be prepared to provide any additional required documents on the day of the audit.

At the start of the Audit, 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 roles and specializations.

Role of the auditor and Subject Matter Expert (SME)

Cisco uses an independent Third-Party audit agency to conduct audits. An auditor (either business or technical) manages the audit process, and a subject matter expert (SME) may be present to assist in technical sections of the audit. During the audit, the auditor will verify whether the partner complies with the spirit and intent of all 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 requirements. All information or documentation provided to the auditor or SME is considered “confidential information” as defined in a nondisclosure agreement (NDA) signed by Cisco’s Third-Party auditors and SMEs, and will be treated accordingly by Cisco, the auditor and the SME. The audit report is not shared outside the immediate Cisco Certification Program Team.

Technical Evaluation sessions for Master specializations will be recorded, with recordings held confidential per above NDA. Partners who request to opt-out of recording the session(s) must inform the auditors prior to the session start and waive all rights to dispute auditor findings, including a score of "Fail" for all or any part of the audit.

Master Collaboration, Security, Networking and Data Center and Hybrid Cloud: The SME may aid the auditor during the 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 requirements have been satisfied.

Role of the Cisco Partner Account Manager (PAM)

Prior to the audit, it is the PAM's responsibility to ensure the partner fully understands requirements and to assist the partner in completing the online application. PAM should work in collaboration with the SE to interface with the Cisco Certification Program Manager, the Cisco Partner support representative and other Stakeholders as appropriate. The PAM is also responsible for ensuring that the appropriate subject matter experts employed by the partner are available (i.e., sales experts or engineers who normally perform customer demonstrations, relevant Product managers for Managed Services, and operational staff).

During audit sessions, 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 the PAM should make arrangements to attend the audit remotely, only if there is no option to attend in person.

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.
- Working in collaboration with the PAM to interface with the Cisco Certification Program Manager, the Cisco partner support representative and other Stakeholders as appropriate.
- Co-managing the sales demonstration portion of the audit with the PAM and the auditor for Gold and Provider audits. For Master Security Technical Evaluations, the Cisco SE will manage the virtual audit session. For Master Collaboration, Networking and Data Center and Hybrid Cloud, the Cisco SE is not required to attend the audit sessions as a technical SME will be present from the auditing firm.

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, or Consulting Systems Engineer [CSE]) should work with the PAM to understand the audit requirements and assist the partner in preparing for the technical portion of the audit, including demonstration.

Cisco Powered Services: 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 requirements have been satisfied.

Role of the Cisco Certification Program Manager (PM)

The Cisco Certification Program Manager (PM) is responsible for maintaining integrity, and as such, the decision to award or revoke Designations 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, when applicable.

If unable to close out open action items within 5 business days or if the action requires live demonstration, 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 or review 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 the Designation will not be made until the Corrective Action plan is satisfactorily completed.

For Masters Specializations, the Sales Evaluation and Foundation Evaluation (audit) may not be scheduled or conducted until after the Technical Evaluation has been successfully completed. Open action items from the Technical Evaluation must be closed prior to the Sales or Foundation Evaluation (audit) being scheduled. Renewing Master partners may not remain in Audit-Hold for more than 6 (six) months. Failure to resolve outstanding issues causing the Audit-Hold status within 6 (six) months may result in loss of the specialization.

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. The audit report is not shared outside the immediate Cisco Certification Program Team. Results will be emailed back to the primary contact within the partner organization. Sales Evaluation and Foundation Evaluation must be completed within 180 days of the Technical Evaluation being completed.

It is possible that the findings of the audit are such that approval or renewal of the Designation cannot be achieved within the stated get-well period. In this case, the Certification Program Manager may deny the Designation. If a partner fails to deliver an action plan within the agreed timeframe, the partner may also be denied approval or renewal of the Designation.

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 renewal application each year.
- The status for the Designation changes from “Approved” to "Re-cert" mode, 90 days prior to the anniversary date.
- Designation Renewal reminder notices are sent 90 days, 60 days, and 30 days prior to a partner's Designation anniversary date via the Partner Alert Updates generated from the Program Management & Application (PM&A) tool.

- 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 renewal application anytime during the renewal period for each Designation independently, but no later than 30 days after the anniversary date of the Designation due for renewal.
- If a partner does not submit a renewal application including all required documentation within 30 days from the anniversary date, the Designation 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.
- An audit reschedule or cancellation request by a partner must be communicated to Cisco no less than 15 business days prior to the audit, otherwise the audit will proceed as scheduled; the final decision is at the discretion of Certification Program Manager; audit reschedule, or cancellation fees will apply. Reschedule or cancellation fees for all partner-paid audits are managed between the partner and NSF directly.
  - Greater than 15 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 reschedule or cancellation fees will be managed directly by the 3rd party auditing firm.

If an audit is failed or stopped and determined by the auditor, SME and/or the Certification Program Manager that the audit may not continue due to insufficient evidence provided or due to an incomplete demonstration, the partner will be responsible for the cost of an audit revisit whether the revisit is onsite or remote. The final decision on the outcome is at the discretion of the Certification Program Manager.

If a partner is moved to the next eligible level from the Gold Integrator role, any Master Specialization and/or the Provider role, regardless of the reason for the move, the partner will be responsible to cover the cost of the audit for program re-entry (When Applicable).

- New program applications left unresolved for 120 days are deleted.
- Master specialization Technical Evaluations must be passed before a Sales Evaluation or Foundation Evaluation (audit) will be scheduled or conducted. Sales Evaluation or Foundation Evaluation (audit) sessions will not be scheduled less than 7 days after the Technical Evaluation. Sales Evaluation and Foundation Evaluation must be completed within 180 days of the Technical Evaluation being completed.
- 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.
- The definition of a "new" partner as it relates to audit requirements, is a partner that has not been approved at any level of the auditable Designation within the previous six months. Designations are valid for 1 year (partner must remain in compliance throughout the year).
- No waiver of rights under the Cisco Partner Program Audit and Policies by either party shall constitute a subsequent waiver of such right or any other right under the Cisco Partner Program Audit and Policies.

1.5 Refusal to Certify

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

Pre-Qualification Requirements Overview

Requirement	Integrator role
2.1 Integrator role Pre-Qualification	**G**
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	•

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

Requirement	Customer Experience (CES)
2.3 Customer Experience Specialization Pre-Qualification	**CES**
2.3.1 Agreements/Contracts	•
2.3.2 Personnel	•
2.3.3 Customer References	•
2.3.4 Validation	•

Gold Integrator Role (G); Master Specialization: Collaboration (Collab), Security (Sec); Networking (Net), Data Center and Hybrid Cloud (DC); Customer Experience Specialization (CES) Provider Role: Gold Provider (GP), Premier Provider (PP), Select Provider (SP)

Requirement	Provider role		
2.4 Provider role Pre-Qualification	**GP**	**PP**	**SP**
2.4.1 Personnel	·	·	N/A
2.4.2 Agreements/Contracts	·	·	·
2.4.3 Specializations	·	·	N/A
2.4.4 Specializations for restricted products	·	·	·
2.4.5 Network Operations Center (NOC)	·	·	N/A
2.4.6 Customer References	·	·	N/A
2.4.7 Service Offerings	·	·	·
2.4.8 SLA	·	·	·
2.4.9 Managed Services business interlock with Cisco	·	·	N/A

2.0 Pre-Qualification Requirements

2.1 Integrator Role

2.1.1 Personnel

Applies to: G (See Table)

Gold Integrator Role: Partner must have a minimum of 12 unique certified full-time employees, including minimum 4 CCIEs*, no more than 4 Selling Business Outcomes Individuals (SBOs), 4 Cisco Business Architecture Analysts (DTBAA) or 4 Introduction to Cisco Sales (ICS) 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 a role or specializations are 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 either a role or 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 the PM&A tool. 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 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 Partner out of compliance and at risk for disqualification.

The only exception to this is for CCIEs/CCDEs. Integrators 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).

2.1.2 Specializations

Applies to: G (See Table)

Gold Integrator Role: Integrators must hold the required number of Specializations listed in the most recent Requirements document posted to the Integrator website: https://www.cisco.com/c/en/us/partners/partner-with-cisco/integrator.html.

2.1.3 Agreements/Contracts

Applies to: G (See Table)

Integrators must have a valid resale support agreement with Cisco, including a Cisco Branded Services or a Partner Support Services (PSS) agreement. (This is validated by the Cisco Certification Program Manager via internal systems – Partner is not required to provide documentation during audit for this requirement). 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 Integrators 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 Integrators are required to offer Cisco Packaged Services to customers wishing to purchase service and support.

Integrators who transition from one type of support contract or agreement to another during the anniversary year should contact their Certification Program Manager to understand the impact on Gold Integrator requirements. For Direct Partners, lack of a valid support agreement may result in immediate removal of the Integrator role. This also applies to indirect Integrators in the Europe and Emerging Market regions (except Latin America). For Integrators that sell both Partner Support Services (PSS) and Cisco branded services, the Partner Support Services (PSS) performance metrics will be used for audit purposes.

2.1.4 CSAT Requirements

Applies to: G (See Table)

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

- January (Q2) measurement: Integrator 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: Integrator must enter Follow-Up activities in the PAL tool for all low scores (1 – 4) received for the current fiscal year (if any) If no low scores are received for the fiscal year, no action is required for the July (Q4) measurement.
- Evidence of results analysis and reinforcement of best practices for customer satisfaction must be captured by the Integrator, including evidence that a closed loop process is being used for addressing customer issues raised in customer satisfaction surveys.

For new Gold Integrator, the following CSAT requirements apply:

- Participation in CSAT activities starting at the first measurement after a full six months of attaining the Gold Integrator role.
- The definition of a “new” Integrator as it relates to the enforcement of the CSAT requirement is an Integrator that has not held the Integrator role at any level within the previous six months.
- Provide a minimum of 30 valid customer contact/email addresses for the January (Q2) measurement. Integrators are not 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. Integrator must enter Follow-Up activities in the PAL tool for all low scores (1 – 4) received for the current fiscal year (if any). If no low scores are received for the fiscal year, no action is required for the July (Q4) measurement.

- Premier Integrators moving to Gold Integrator 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 the Gold Integrator role.
- If a partner falls out of compliance with the requirements and their role is removed, if they attain the Gold Integrator role again within six months, they will be treated as renewing the Integrator role and will be responsible for meeting the CSAT requirements at the next measurement period.

For Gold Integrator renewals, the following CSAT requirements apply:

- Provide a minimum of 30 valid customer contact/email addresses for the January (Q2) measurement. Integrators are not 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. Integrator must enter Follow-Up activities in the PAL tool for all low scores (1 – 4) received for the current fiscal year (if any). If no low scores are received for the fiscal year, no action is required for the July (Q4) measurement.
- Failure to meet CSAT requirements will be considered lack of participation and is grounds for a move to the next eligible level. In this case, the Integrator 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 downgrade.

CSAT abuse (including but not limited to providing non-customer contact/email addresses) is considered a serious offense and will result in loss of the Integrator role entirely.

More details can be found on the CSAT website.

2.1.5 Service Attach Rate

Applies to: G (See Table)

Applies to both Cisco Branded Services and Partner Support Services (PSS).

Gold Integrators are required to have a minimum service attach rate of 40 percent during the prior four Cisco quarters. (Partners must show a minimum service attach rate of 40% in Total Partner View (TPV) at the time of application submission as TPV shows the average of the previous four quarters). For partners who have not previously held the Gold Integrator role, 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:

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

*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.

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 Total Program View (TPV) within the metrics section.

2.1.6 Revenue from Services

Applies to: G (See Table)

Applies to both Cisco branded services and Partner Support Services (PSS).

Gold Integrators 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 the Gold Integrator role.

2.2 Master Specializations

2.2.1 Specializations

Applies to: Collab, Sec, Net, DC (See Table)

Master Collaboration: Partner must have the Advanced Collaboration Architecture specialization.

Master Security: Partner must have the Advanced Security Architecture specialization.

Master Data Center and Hybrid Cloud: Partner must have the Advanced Data Center Architecture specialization.

Master Networking: Partner must have the Advanced Enterprise Networks Architecture specialization.

2.2.2 Personnel

Applies to: Collab, Sec, Net, DC (See Table)

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

- 1 CCIE Voice (or CCIE Collaboration)
- 1 PMP/Prince II Foundation or Practitioner

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

- 1 CCIE Security*
- 1 CCNP Security* (A unique CCIE Security may satisfy the CCNP Security role – one CCIE Security is not able to satisfy both the CCIE Security and CCNP Security roles, two CCIE Security employees would be required if utilizing this option)
- 1 Fire Jumper Level 4* or higher in any track
- 1 PMP/Prince II Foundation or Practitioner

*must be unique individuals

Master Data Center and Hybrid Cloud: Partner must have personnel to satisfy the roles for the Advanced Data Center Architecture specialization (CCNP or higher), plus the appropriate personnel to maintain third party credentials as noted in 2.2.8 below.

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

- 1 CCIE Route/Switch or Wireless*
- 1 Fire Jumper – Level 4 or higher in any track

*must be unique individuals

All Cisco certified personnel requirements must be satisfied by a unique certified, full-time, regular employee residing in the country where Master Specialization is sought and in good standing with Cisco. Partners may employ full-time contracted employees to fulfill the CCIE certified personnel requirements within Master Specializations. During the Sales Evaluation or Foundation Evaluation (audit), partner must provide evidence of full-time employment for each individual playing a role in Master specialization(s).

2.2.3 Agreements/Contracts

Applies to: Collab, Sec, Net, DC (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, Net, DC (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, Net, DC (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 Data Center and Hybrid Cloud: There are no incremental training requirements beyond the training requirements in the Advanced Data Center Architecture specialization.

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

2.2.6 Customer References

Applies to: Collab, Sec, Net, DC (See Table)

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

Partner must submit these documents into the Master Specialization application. Cisco will verify the customer reference documentation after it is uploaded into the Master Specialization application. Each of the reference accounts submitted must be from the past 18 months. References may not be repeated from past submissions. However, Partner may use the same Customer Reference account for requalification if there is a new sale within that account that meets all the current criteria.

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

Partner must submit these documents into the Master Specialization application. Cisco will verify the customer reference documentation after it is uploaded into the Master Specialization application. Each of the reference accounts submitted must be from the past 18 months. References may not be repeated from past submissions. However, Partner may use the same Customer Reference account for requalification if there is a new sale within that account that meets all the current criteria.

- Partner may use same customers for proof of value (POV) and Customer Reference accounts.
- Partner must submit documentation for 3 Partner executed POVs.

Master Data Center and Hybrid Cloud: Prior to the audit being scheduled, partner must submit documentation for a minimum of 3 direct reference accounts demonstrating complex deployments including third party integration. Each submission must contain the Master Data Center and Hybrid Cloud Customer Reference Checklist.

Partner must submit these documents into the Master Specialization application. Cisco will verify the Customer Reference documentation after it is uploaded into the Master Specialization application. Each of the reference accounts submitted must be from the past 18 months. References may not be repeated from past submissions. However, Partner may use the same customer Reference account for requalification if there is a new sale within that account that meets all the current criteria.

Master Networking: Prior to the audit being scheduled, partner must submit documentation for a minimum of 3 partner-executed proof of value (POV) assessments or direct reference accounts demonstrating complex deployments including third party integration. Each submission must contain the Master Networking Customer Reference Checklist or POV documentation. Partner may combine either POV or Customer References to satisfy the minimum of 3 submissions. (3 Customer References or 3 POVs or a combination of Customer References and POVs to equal a total of 3)

Partner should submit documents into the Master Specialization application. Each of the reference accounts submitted must be from the past 18 months. References may not be repeated from past submissions. However, Partner may use the same Customer Reference account for requalification if there is a new sale within that account that meets all the current criteria.

2.2.7 Demonstration

Applies to: Collab, Sec, Net, DC (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. This is achieved through two evaluation sessions scheduled independently of each other; the first is the Technical Evaluation which is technical skills focused, the second is the Sales Evaluation which is sales skills focused. The Technical Evaluation is limited to 3 hours and the Sales Evaluation session is limited to 2 hours. See Master Collaboration Specialization Solution Guideline.

Note: UCCE Specialized Partners (USA) will be provided with the option to meet the Customer Care requirements with either UCCE or UCCX if the UCCE Specialization lab audit has been conducted within 90-days prior to the Master Collaboration audit

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. This is achieved through two evaluation sessions scheduled independently of each other; the first is the Technical Evaluation which is technical skills focused, the second is the Sales Evaluation which is sales skills focused. The Technical Evaluation is limited to 3 hours and the Sales Evaluation session is limited to 2 hours. See Master Security Specialization Solution Guideline.

Data Center and Hybrid Cloud: 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. This is achieved through two evaluation sessions scheduled independently of each other; the first is the Technical Evaluation which is technical skills focused, the second is the Sales Evaluation which is sales skills focused. The Technical Evaluation is limited to 3 hours and the Sales Evaluation session is limited to 2 hours. See Master Data Center and Hybrid Cloud Solution Guidelines.

Networking: 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. This is achieved through two evaluation sessions scheduled independently of each other; the first is the Technical Evaluation which is technical skills focused, the second is the Sales Evaluation which is sales skills focused. The Technical Evaluation is limited to 3 hours and the Sales Evaluation session is limited to 2 hours. See Master Networking Specialization Solution Guidelines.

2.2.8 Third Party Credentials — Applies to: DC (See Table)

Master Data Center and Hybrid Cloud: During the application process, partner must upload documented proof of active certifications in one or more of the following:

Industry Certification

- VMware – Partner, Advanced or Principal
- Redhat – Premier or SI Certification
- Citrix – Gold or Platinum Certification
- Microsoft – Gold Certification

2.2.9 Integrated Infrastructure (Computer, Storage, and Network Components) — Applies to: DC (See Table)

Master Data Center and Hybrid Cloud: Customer solutions must be based on Cisco's Integrated Infrastructure stacks as described in the Master Data Center and Hybrid Cloud Solutions Guideline. Validation may 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.

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

Master Security: Partner must upload documentation for the 3 Proof of Value (POV) Assessments.

These POV customers may be from among the five deployment Customer Reference accounts, or they may be different customers.

There are five pieces of proof-of-performance documentation for the creation of each of the three POVs:

1. Data Collection Worksheet: Partner needs to fill out a checklist /analysis of the customer's current system environment.
2. Win criteria: Partner needs to fill a checklist which is used to demonstrate unique business value to the customer during the on-site engagement.
3. POV Outcome: Real-world customer use case including how solution was designed, configured and implemented to achieve the desired win criteria.
4. Customer Facing Reports: Partner needs to provide reports that were supplied to the customer to prove the implemented solution achieves desired win criteria.
5. BOM: Partner needs to create a Bill of Material (BOM) via CCW by positioning the right Products that they want to use

Examples of POV Best Practices may be found at: https://communities.cisco.com/docs/DOC-65405

Master Networking: Partner must upload documentation for any Proof of Value (POV) Assessments *if used to meet prerequisites instead of or in addition to Customer References*. Master Networking requires 3 Customer References or 3 POVs or a combination of Customer References and POVs to equal a total of three.

There are five pieces of proof-of-performance documentation for the creation of each of POVs:

1. Data Collection Worksheet: Partner needs to fill out a checklist /analysis of the customer's current system environment.
2. Win criteria: Partner needs to fill a checklist which is used to demonstrate unique business value to the customer during the on-site engagement.
3. POV Outcome: Real-world customer use case including how solution was designed, configured, and implemented to achieve the desired win criteria.
4. Customer Facing Reports: Partner needs to provide reports that were supplied to the customer to prove the implemented solution achieves desired win criteria.
5. BOM: Partner needs to create a Bill of Material (BOM) via CCW by positioning the right Products that they want to use

Examples of POV Best Practices may be found at: https://communities.cisco.com/docs/DOC-65405

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: https://www.cisco.com/c/dam/en_us/partners/downloads/specializations/masters-security-update-practice-areas.pdf

2.2.12 Renewals **Applies to: Collab, Sec, Net, DC (See Table)**

Partners must maintain all Pre-Audit validation requirements (except for Customer References) listed in the most recent Requirements documents posted to the Specialization website: https://www.cisco.com/c/en/us/partners/partner-with-cisco/expertise/specializations.html

2.3 Customer Experience Specialization

2.3.1 Agreements/Contracts

Applies to: CES (See Table)

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

2.3.2 Personnel

Applies to: CES (See Table)

Customer Experience

Four unique individuals required

- 2 Customer Success Manager Specialist (CSM)
- 1 Renewals Manager
- 1 Executive Sponsor

Advanced Customer Experience

Six unique individuals required

- 3 Customer Success Manager (CSM)
- Renewals Manager
- Customer Success Practice Leader
- Executive Sponsor

2.3.3 Customer References

Applies to: CES (See Table)

Partner must submit two Customer References. The Customer References will be reviewed and validated by the Third-Party auditing firm. Use the Customer Reference Template posted here for guidance.

2.3.4 Validation

Applies to: CES (See Table)

Customer Experience

After a Cisco Certification Manager validates your application, the manager will coordinate review of your Customer Success practice.

Advanced Customer Experience

After a Cisco Certification Program Manager validates your application, the manager will forward your application to the Third-Party auditing firm. Requirements for the Partner Capability Review are found here. Prepare accordingly.

2.4 Provider Role

General terms

The Provider role is available in multiple regions globally pursuant to the Terms if the Partner meets the tier level requirements in any of their geographical locations of presence unless otherwise specified.

2.4.1 Personnel Applies to: GP, PP, (See Table)

Gold Provider: Partner must have the following personnel: A minimum of four unique individuals (total) required. During the audit, Provider must provide evidence of full-time employment for each certified individual.

- An Executive Sponsor
- Minimum two individuals with Information Technology Infrastructure Library (ITIL) v3 or higher Foundation certificate
- One Cisco Managed Service Practice Lead
- Two Cisco MS Management Personnel, including one Product Manager for service creation and one Sales Specialist for service acceleration
- NOC personnel to ensure that NOC service is available 24x7x365 at the headquarters (as defined by the partner) where the partner is audited
- Customer Experience or Advanced Customer Experience specialization personnel at the headquarters or any other location where the partner has presence
- Personnel and any required specializations for Cisco Powered Service(s) offered

Premier Provider: Partner must have the following personnel:

A minimum of one unique individual (total) required. During the audit, Provider must provide evidence of full-time employment for each certified individual.

- Minimum one individual with Information Technology Infrastructure Library (ITIL) v3 or higher Foundation certificate
- One Cisco Managed Service Practice Lead
- NOC personnel to ensure that NOC service is available 24x7x365 at the headquarters (as defined by the partner) where the partner is audited
- Personnel and any required specializations for Cisco Powered Service(s)offered

2.4.2 Agreements/Contracts Applies to: GP, PP, SP (See Table)

Provider 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, Providers will be required to “click to accept” the Provider role Terms and Conditions (see Appendix 5). Providers enrolled in Provider role 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 a Gold or Premier Provider has outsourced NOC operations, Provider 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. Provider 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.)

2.4.3 Specializations Applies to: GP, PP (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.

Gold Provider must have Customer Experience or Advanced Customer Experience Specialization in headquarters (country where the application is submitted) location or any other location where they have presence.

2.4.4 Specializations for Restricted Products

Applies to: GP, PP, SP (See Table)

Specializations are required for any restricted 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 to access restricted Products for resale, or Cloud and Managed Services.

2.4.5 Network Operations Center (NOC)

Applies to: GP, PP (See Table)

Provider 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. (Provider may or may not own NOC assets.)

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

Provider 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, Provider must show auditor evidence of remote access to the NOC. This may be the Provider location with access to NOC or a service provider's NOC.

Together, Provider 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).

Outsourcing NOC operations

Providers 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:

- Provider and NOC Services Provider responsibilities
- Summary of program requirements that can be outsourced for partner to meet published Provider role requirements together with NOC Services Provider

2.4.6 Customer References

Applies to: GP, PP (See Table)

Providers must submit two Customer References for each Cisco Powered Service offered by completing the Provider Role Customer Reference Validation Template: Evidence will be validated during the audit.

Providers applying for new Cisco Powered Cloud Services are required to provide Customer References at the next renewal, rather than at the initial audit.

2.4.7 Service Offerings

Applies to: GP, PP, SP (See Table)

Gold Provider: Provider must have at least **three Cisco Powered Services** with a minimum of **one strategic** (see list below) Cisco Powered Service in their Gold Provider application.

Strategic Cisco Powered Services:

- Meraki Access
- Meraki SD-WAN
- Cisco SD-WAN (Viptela)
- Secure Access
- Cloud Calling
- Webex Contact Center
- Hybrid Cloud
- Cloud Managed Security
- Meraki Security
- Secure Access Services Edge (SASE)

Provider must upload the following documents for each Cisco Powered Service:

- Marketing description
- Completed customer reference template with 2 customers listed
- Service Level Agreement (SLA)

Premier Provider: Provider must have at least **1 Cisco Powered Service** offering.

Provider must upload the following documents for each Cisco Powered Service:

- Marketing description
- Completed customer reference template with 2 customers listed
- Service Level Agreement (SLA)

In order to receive certain benefits under the Provider role, Providers must provide point of sale (PoS) information.

Select Provider: Provider must deliver at least one Managed Service based on Cisco Enterprise Networking, Meraki or Security or Collaboration technologies.

Provider must upload the following documents:

- Marketing Services Description
- Screenshot of Remote Monitoring and Management tool
- Screenshot of Professional Services Automation tool (optional)

2.4.8 Customer Service Level Agreement (SLA)

Applies to: GP, PP, SP (See Table)

Provider must upload a currently active, signed Service Level Agreement (SLA) for each Cisco Powered Service.

The uploaded SLA should:

- be signed/accepted by a customer,
- include terms of 12 months or more for Managed Services
- describe service obligations.

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

2.4.9 Managed Services business interlock with Cisco — Applies to: GP (See Table)

Partner Executive Sponsor at Gold Provider must have business plan interlock meetings with Cisco throughout the year to review their Managed Services business KPIs.

- Existing Gold Providers must upload a completed MS Business interlock template starting at their audit anniversary in FY2023 and each year for renewal to maintain their Gold Provider level.
- New Gold Providers must upload a completed MS Business interlock template upon first-year application renewal and each year to maintain their Gold Provider level.

Program Requirements Overview

	Integrator Role	Master Specialization				Provider Role
Requirement	**G**	**Collab**	**Sec**	**Net**	**DC**	**GP**
3.1.1 General Requirements	·	·	·	·	·	·
3.2.1 Solution Demonstration	·	·	·	·	·	·
3.2.2 Demand Generation	N/A	N/A	N/A	N/A	·	N/A
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	·	·	·	·	·	·
3.4.1 Network Design Process	·	·	·	·	·	·
3.4.2 Design Documents	·	·	·	·	·	·
3.5.1 Training Plans	·	·	·	·	·	·
3.5.2 Training Records	·	·	·	·	·	·
3.5.3 List of Required Personnel	·	·	·	·	·	N/A
3.6.1 Customer Training Process	·	·	·	·	·	·
4.1.1 Budgeting and Financial Planning Processes	N/A	·	N/A	·	·	·
4.2.1 Portfolio Management Process	N/A	·	N/A	·	·	·
4.3.1 Demand Management Process	N/A	·	N/A	·	·	·
4.4.1 Subscription and recurring billing capabilities	N/A	N/A	N/A	N/A	N/A	·
5.1.1 Information about Services Offered	N/A	·	N/A	·	·	·
5.1.2 Professional Services	N/A	N/A	N/A	·	·	N/A

Gold Integrator Role (G); Master Specialization: Collaboration (Collab), Security (Sec); Networking (Net), Data Center and Hybrid Cloud (DC); Customer Experience Specialization (CES) Provider Role: Gold Provider (GP), Premier Provider (PP), Select Provider (SP)

	Integrator Role	Master Specialization				Provider Role
Requirement	G	Collab	Sec	Net	DC	GP
5.1.3 Service Catalog Maintenance	N/A	·	N/A	·	·	·
5.1.4 Service Catalog Updates	N/A	·	N/A	·	·	·
5.2.1 SLAs/SLOs	·	·	N/A	·	·	·
5.2.2 Service Level Measurement and Reporting	·	·	N/A	·	·	·
5.2.3 Parts Replacement	·	·	N/A	·	·	·
5.3.1 Business Capacity	N/A	·	N/A	·	·	·
5.3.2 Service Capacity	N/A	·	N/A	·	·	·
5.3.3 Resource Capacity	N/A	·	N/A	·	·	·
5.3.4 Capacity Improvements	N/A	·	N/A	·	·	·
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	·
5.5.1 IT Infrastructure Monitoring	N/A	·	N/A	·	·	·
5.5.2 IT Infrastructure Problem Resolution	N/A	·	N/A	·	·	·
5.5.3 Service Continuity/Disaster Recovery Planning	N/A	·	N/A	·	·	·
5.5.4 Disaster Recovery Plan Testing	N/A	·	N/A	·	·	·
5.6.1 Security Policies and Procedures	·	·	·	·	·	N/A
5.6.2 Physical Security	·	·	·	·	·	N/A
5.6.3 Network Security	·	·	·	·	·	N/A
5.6.4 Server Security	·	·	·	·	·	N/A
5.6.5 Logical Data Security	·	·	·	·	·	N/A
5.8.1 Third Party Contracted Activities and Services	·	N/A	N/A	N/A	N/A	·
5.8.2 Subcontractor Management	·	N/A	N/A	N/A	N/A	·
5.8.3 Subcontractor Contracts	·	N/A	N/A	N/A	N/A	·
5.8.4 Subcontractor Communication	·	N/A	N/A	N/A	N/A	·
5.8.5 Periodic Subcontractor Reviews	·	N/A	N/A	N/A	N/A	·
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	·
6.2.1 Change Management Process	·	·	N/A	·	·	·
6.2.2 Change Rollback	N/A	·	N/A	·	·	·
6.2.3 Requests for Changes	N/A	·	N/A	·	·	·
6.2.4 Change Definitions	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	·	·	·
6.2.7 Change Manager and Change Advisory Board	N/A	·	N/A	·	·	·
6.2.8 Change Management Tools	N/A	·	N/A	·	·	·

Gold Integrator Role (G); Master Specialization: Collaboration (Collab), Security (Sec); Networking (Net), Data Center and Hybrid Cloud (DC); Customer Experience Specialization (CES) Provider Role: Gold Provider (GP), Premier Provider (PP), Select Provider (SP)

Requirement	Integrator Role	Master Specialization				Provider Role
	G	Collab	Sec	Net	DC	GP
6.3.1 Change Management Process	N/A	·	N/A	·	·	·
6.3.2 Phased Release	N/A	·	N/A	·	·	·
6.3.3 Configuration Item (CI) Identification	N/A	·	N/A	·	·	·
6.3.4 Software and Hardware Repositories	N/A	·	N/A	·	·	·
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	·
6.5.1 Service Validation and Testing Process	N/A	N/A	N/A	N/A	N/A	·
6.6.1 Service Evaluation Process	N/A	N/A	N/A	N/A	N/A	·
6.7.1 Information Availability and Accessibility	N/A	·	N/A	·	·	·
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	·	·	·
7.1.8 Service Desk Duty Manager	·	·	N/A	·	·	·
7.1.9 Computer-Based Call Tracking System	·	·	N/A	·	·	·
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	·
7.3.1 Event Management Process	·	·	N/A	·	·	·
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	·	·	·
7.4.7 Incident Logging and Querying	N/A	·	N/A	·	·	·
7.4.8 Customer Notification	N/A	·	N/A	·	·	·
7.4.9 Notification Methods	N/A	·	N/A	·	·	·
7.4.10 Incident Prioritization and Categorization	N/A	·	N/A	·	·	·
7.4.11 Stakeholder Updates	N/A	·	N/A	·	·	·
7.4.12 Incident Troubleshooting and Investigation	N/A	·	N/A	·	·	·
7.4.13 Handoff to Problem Management	N/A	·	N/A	·	·	·
7.4.14 Known Error Database	N/A	·	N/A	·	·	·
7.4.15 Incident Closure Authorities	N/A	·	N/A	·	·	·

Gold Integrator Role (G); Master Specialization: Collaboration (Collab), Security (Sec); Networking (Net), Data Center and Hybrid Cloud (DC); Customer Experience Specialization (CES) Provider Role: Gold Provider (GP), Premier Provider (PP), Select Provider (SP)

	Integrator Role	Master Specialization				Provider Role
Requirement	**G**	**Collab**	**Sec**	**Net**	**DC**	**GP**
7.4.16 Incident Closure Summary	N/A	·	N/A	·	·	·
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	·	·	·
7.6.1 Access Management Process	N/A	·	N/A	·	N/A	·
7.7.1 Onsite Response/Troubleshooting Description	·	·	N/A	·	·	·
7.8.1 Remote Access	N/A	N/A	N/A	N/A	N/A	·
8.1.1 Continual Improvement Activities	·	·	N/A	·	·	·
8.1.2 Continual Improvement Methodology	·	·	N/A	·	·	·
8.2.1 Service Objectives	·	·	N/A	·	·	·
8.2.2 Mean Time to Notify (MTTN)	N/A	·	N/A	·	·	·
8.2.3 Mean Time to Restore Service (MTRS)	N/A	·	N/A	·	·	·
8.2.4 Onsite Troubleshooting Response Time	·	·	N/A	·	·	·
8.2.5 Customer Perception and Feedback	·	·	N/A	·	·	·
8.3.1 Service Reports	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

3.0 Pre-Sales Requirements

3.1 Support Lab

3.1.1 General Requirements

Applies to: G, Collab, Sec, Net, DC, GP (See Table)

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

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 Integrators 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 Integrators "CBS or SMARTnet only" applying for Master specializations or the Provider role 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 Data Center and Hybrid Cloud lab can be anywhere, so long as the lab setup can support the business and be readily accessed remotely.

Note: 3: Requirements for support lab (3.1.1) do not apply for Gold Providers who offer one or a combination of the following services only: Cisco Powered IaaS or Cisco Powered TPaaS.

Note: 4: Gold Providers offering Cloud Services may use a virtualized lab to demonstrate this requirement. (Applicable to Cisco Powered UC as a Service based on HCS and Cisco Powered Contact Center as a Service based on HCS)

3.2 Demonstration and Demand Generation

3.2.1 Solution Demonstration Applies to: G, Collab, Sec, Net, DC, GP (See Table)

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

The evaluation demonstration(s) may 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

For the Gold Provider role, the components of an end-to-end demonstration are not required to reside in the same location.

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

Note: 1: Gold Integrators must not demonstrate the same solution for two successive audit years. A demonstration may not be required for renewal audits, as determined and documented by the Certification Program Manager. Gold Integrators are allowed to use dCloud for their on-site audit demonstration.

Note: 2: Master specialized partners must complete evaluation demonstrations using either the pre-defined customer scenario or one of their own to develop demonstrations that incorporate the criteria defined in the Solutions Guideline document. Master Security, Master Networking, Master Collaboration and Master Data Center and Hybrid Cloud Specialized Partners may utilize dCloud as a demo option. Master demonstrations will be evaluated and scored as described in the Master Collaboration, Master Security, Master Networking or Master Data Center and Hybrid Cloud Solutions Guidelines.

Note: 3: Providers 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: DC (See Table)

Master Data Center and Hybrid Cloud 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 Gold Providers 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 TPaaS, Cisco Powered Architecture for the Microsoft Cloud Platform, or Cisco Powered HSS.

3.3.1 Personnel Applies to: G, Collab, Sec, Net, DC, GP (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.*

3.3.2 Project Plans Applies to: G, Collab, Sec, Net, DC, GP (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, Collab, Sec, Net, DC, GP (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 Data Center and Hybrid Cloud 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, Collab, Sec, Net, DC, GP (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 and provide evidence of how the project charter is included in the project plan.

3.3.5 Resource Management — Applies to: G, Collab, Sec, Net, DC GP (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, Collab, Sec, Net, DC, GP (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 and provide evidence of how customer requirements are detailed in project plans.

3.3.7 Project Start Meeting — Applies to: G, Collab, Sec, Net, DC, GP (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, Collab, Sec, Net, DC, GP (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 and provide evidence of 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, Collab, Sec, Net, DC, GP (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 and provide evidence of how milestones are tracked (e.g., in a project plan).

3.3.10 Customer Communication Plan

Applies to: G, Collab, Sec, Net, DC, GP (See Table)

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

Partner must explain and provide evidence of how customer communication plans are developed.

3.3.11 Project Implementation

Applies to: G, Collab, Sec, Net, DC, GP (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, Collab, Sec, Net, DC, GP (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 and provide evidence of how project review and evaluation is completed.

3.4 Design

Note: Requirements for Design (3.4.1-3.4.2) do not apply for Gold Providers 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 TPaaS, Cisco Powered Architecture for the Microsoft Cloud Platform, or Cisco Powered HSS.

3.4.1 Network Design Process

Applies to: G, Collab, Sec, Net, DC, GP (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 and provide evidence of how network design is accomplished, e.g., in a documented procedure/flowchart, or a detailed explanation of the design process.

Note: Providers offering Cloud Service(s) must demonstrate how virtualized environment is provisioned and accomplished.

3.4.2 Design Documents

Applies to: G, Collab, Sec, Net, DC, GP (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, Collab, Sec, Net, DC, GP (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, Collab, Sec, Net, DC, GP (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, Collab, Sec, Net, DC (See Table)

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

3.6 Post-Implementation Customer Training

3.6.1 Customer Training Process

Applies to: G, Collab, Sec, Net, DC, GP (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: Providers 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.

4.0 Service Strategy Requirements

4.1 IT Financial Management

4.1.1 Budgeting and Financial Planning Processes

Applies to: Collab, Net, DC, GP (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, Net, DC, GP (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, Net, DC, GP (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 Data Center and Hybrid Cloud 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.

4.4 Subscription and recurring billing capabilities

4.4.1 Subscription and recurring billing capabilities

Applies to: GP (See Table)

New Gold Providers must have capabilities to charge customers at predefined intervals (weekly, monthly, annually, or custom intervals), subscription or consumption based Managed Services.

- Partner must have operational processes, tools or platform, and budgeting processes in place to deliver subscription and recurring billing capabilities to end customers.
- Partners must show accounting methods to account for subscriptions, tools that are utilized for this process and provide an example of a recent transaction.

Cisco Lifecycle Services: Build

5.0 Service Design Requirements

5.1 Service Catalog Management

5.1.1 Information About Services Offered — Applies to: Collab, Net, DC, GP (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 Data Center and Hybrid Cloud requirements, and collaboration-specific services for Master Collaboration requirements.

5.1.2 Professional Services — Applies to: Net, DC (See Table)

Partner must describe and provide evidence of which professional services are offered.

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

During the audit, Master 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, Net, DC, GP (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 Data Center and Hybrid Cloud requirements, and Collaboration-specific services for Collaboration requirement.

5.1.4 Service Catalog Updates — Applies to: Collab, Net, DC, GP (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 Data Center and Hybrid Cloud requirements, and collaboration-specific services for Master Collaboration requirements.

5.2 Service Level Management

5.2.1 SLAs/SLOs Applies to: G, Collab, Net, DC, GP (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 Integrators 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 Integrators "CBS or SMARTnet only" applying for Master specializations or the Provider role 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 Networking and Data Center and Hybrid Cloud Specialized partners must show post-implementation agreements with customer showing post-deployment responsibilities for software and hardware upgrades, and ongoing maintenance. Alternately, Master Networking and Data Center and Hybrid Cloud 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, Collab, Net, DC, GP (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 Integrators 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 Integrators "CBS or SMARTnet only" applying for Master specializations or the Provider role 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 Networking or Data Center and Hybrid Cloud 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: Provider 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, Collab, Net, DC, GP (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 Networking or Data Center and Hybrid Cloud 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 Provider 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 Architecture for the Microsoft Cloud Platform, Cisco Powered HSS or Cisco Powered TPaaS (when the TPaaS partner is not supplying the Customer Premises Equipment-CPE).

Note: 3: Gold Integrators and Master specialized 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, Net, DC, GP (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 and provide evidence of 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, Net, DC, GP (See Table)

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

Partner must explain and provide evidence of 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, Net, DC, GP (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 and provide evidence of 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, Net, DC, GP (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 Data Center and Hybrid Cloud 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: GP (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 and provide evidence of how the availability of all managed components and sub-systems is measured.

5.4.2 Availability Reporting

Applies to: GP (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: GP (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.

5.4.3 Availability Improvements

Applies to: GP (See Table)

Partner must provide recommendations for availability improvements to the customer, e.g., in a stewardship report. Partner must describe and provide evidence of 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 Networking or Data Center and Hybrid Cloud 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, Net, DC, GP (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 and provide evidence of how the availability, capacity, and performance of the IT Infrastructure are monitored.

5.5.2 IT Infrastructure Problem Resolution

Applies to: Collab, Net, DC, GP (See Table)

Partner must have a documented process for responding to issues that arise from the monitoring of internal systems.

Partner must explain and provide evidence of 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, Net, DC, GP (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, Net, DC, GP (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 not audited during the year, they will be required to upload evidence of periodic testing at the time of renewal. 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.

All Security policies and procedures in this section must be

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

5.6.1 Security Policies and Procedures **Applies to: G, Collab, Sec, Net, DC (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.

5.6.2 Physical Security **Applies to: G, Collab, Sec, Net, DC (See Table)**

Partner must have methods and procedures for maintaining physical security and must describe and provide evidence of 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, Collab, Sec, Net, DC (See Table)**

Partner must have methods and procedures for maintaining network security and must describe and provide evidence of 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, Collab, Sec, Net, DC (See Table)

Partner must have methods and procedures for maintaining server security and must describe and provide evidence of 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, Collab, Sec, Net, DC (See Table)

Partner must have methods and procedures for maintaining logical data security and must describe and provide evidence of 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.

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

5.8.1 Third Party Contracted Activities and Services Applies to: G, GP (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 Integrator 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 Providers 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 or Cisco Powered TPaaS (when the TPaaS partner is not supplying the Customer Premises Equipment-CPE).

Note: For Gold Integrator Partner Support 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, GP (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 and provide evidence of 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, GP (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, GP (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, GP (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 and provide evidence of how any issues resulting from these reviews are resolved.

6.0 Service Transition Requirements

6.1 Transition Planning and Support

6.1.1 Risk Management Applies to: GP (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: GP (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 Provider 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 TPaaS, Cisco Powered Architecture for the Microsoft Cloud Platform, or Cisco Powered HSS.

6.2 Change Management

6.2.1 Change Management Process

Applies to: G, Collab, Net, DC, GP (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 and provide evidence of 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, Net, DC, GP (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 and provide evidence of how rollback is accomplished by providing examples of rolled back changes, if available.

6.2.3 Requests for Changes

Applies to: Collab, Net, DC, GP (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, Net, DC, GP (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: GP (See Table)

Partner must offer 24-hour turnaround for standard changes.

Partner must describe and provide evidence of 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, Net, DC, GP (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 and provide evidence of 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, Net, DC, GP (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, Net, DC, GP (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, Net, DC, GP (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, Net, DC, GP (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, Net, DC, GP (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 and provide evidence of 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, Net, DC, GP (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.

6.3.4 Release Management Audits

Applies to: Collab, Net, DC, GP (See Table)

Partner must conduct audits to determine whether releases have followed the Release Management process.

Partner must explain and provide evidence of 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: GP (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 and provide evidence of 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: GP (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: GP (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: GP (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: GP (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, Net, DC, GP (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

7.0 Service Operation Requirements

7.1 Service Desk Function (Call/Contact Center)

Note: 1: Requirements for Service Desk (7.1.1–7.1.5, 7.1.7–7.1.9) do not apply to Gold Integrators 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 Integrators “CBS or SMARTnet only” applying for Master specializations or the Provider role 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 Integrator 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, Collab, Net, DC, GP (See Table)**

Partner must provide evidence that customer service is available 24x7, over internet-based systems, phone, fax, pager, or email.

7.1.2 Local Language Answering

Applies to: G, Collab, Net, DC, GP (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, Collab, Net, DC, GP (See Table)

Partner must provide one-hour callback in the local language, from a technical resource.

7.1.4 Call Logging

Applies to: G, Collab, Net, DC, GP (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, Collab, Net, DC, GP (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, Collab, Net, DC, GP (See Table)

Partner must have a documented and robust Escalation process through the partner management structure and, when necessary, to Cisco, and must explain and provide evidence of 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 Integrators 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, Net, DC, GP (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, Collab, Net, DC, GP (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, Collab, Net, DC, GP (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 and provide evidence of 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 and provide evidence of each of the above system capability requirements.

7.2 Request Fulfillment

7.2.1 Service Request Process

Applies to: G, Collab, Net, DC, GP (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: GP (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 and provide evidence of how automated service request tool is used.

7.3 Event Management

7.3.1 Event Management Process

Applies to: G, Collab, Net, DC, GP (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 and provide evidence of how events are handled through the appropriate process (e.g., management of events within a tool).

Note: This requirement does not apply to Gold Integrators 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 Integrators “CBS or SMARTnet only” applying for Master specializations or the Provider role 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, Collab, Net, DC, GP (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 Integrators 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 Integrators “CBS or SMARTnet only” applying for Master specializations or the Provider role 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: GP (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: GP (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: GP (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: GP (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, Net, DC, GP (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, Net, DC, GP (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, Net, DC, GP (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, Net, DC GP (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, Net, DC, GP (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, Net, DC, GP (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, Net, DC, GP (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, Net, DC, GP (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, Net, DC, GP (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 another similar tool). Users must demonstrate knowledge and awareness of the database and its capabilities.

7.4.15 Incident Closure Authorities

Applies to: Collab, Net, DC, GP (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, Net, DC, GP (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, Collab, Net, DC, GP (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 Integrators 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 Integrators "CBS or SMARTnet only" applying for Master specializations or the Provider role 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, Collab, Net, DC, GP (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 Integrators 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 Integrators "CBS or SMARTnet only" applying for Master specializations or the Provider role 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, Collab, Net, DC, GP (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 Integrators 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 Integrators "CBS or SMARTnet only" applying for Master specializations or the Provider role 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, Net, DC , GP (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 are 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, Net, GP (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, Collab, Net, DC, GP (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 and provide evidence of how onsite response and troubleshooting are provided to customers.

Note: 1: This requirement does not apply to Gold Integrators 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 Integrators “CBS or SMARTnet only” applying for Master specializations or the Provider role 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 Provider 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 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: GP (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 Provider partners offering one or a combination of the following services only: Cisco Powered IaaS, Cisco Powered DaaS, Cisco Powered DRaaS or, Cisco Powered Cloud Cell Architecture for SAP HANA.

8.0 Continual Service Improvement Requirements

8.1 Service Improvement

8.1.1 Continual Improvement Activities

Applies to: G, Collab, Net, DC, GP (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, Collab, Net, DC, GP (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, Collab, Net, DC, GP (See Table)

Partner must establish measurable objectives for service availability, SLA, 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 Integrators 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 Integrators “CBS or SMARTnet only” applying for Master specializations or the Provider role 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, Net, DC, GP (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, DC)	<20 minutes
Provider role	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, Net, DC, GP (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: Providers 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, Collab, Net, DC, GP (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
Gold Integrator	4 hours
Master Specialization: (Collab, CB)	4 hours, except • Cloud/Oil/Gas/Energy/Utilities: may vary by customer
Gold Provider	4 hours

Note: 1: This requirement does not apply to Gold Integrators 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 Integrators "CBS or SMARTnet only" applying for Master specializations or the Provider role 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 Provider partners offering one or a combination of the following services only: Cisco Powered IaaS or Cisco Powered Hybrid Cloud.

8.2.5 Customer Perception and Feedback

Applies to: G, Collab, Net, DC, GP (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, Net, DC, GP (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: Providers 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: GP (See Table)

Partner must provide evidence of a cloud or Managed Service(s) contract for orders placed within the last 12 months (applies to renewal 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.

CCDE: Cisco Certified Design Expert

CCIE: Cisco Certified Internetwork Expert

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.

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 MS Management - Product Management (Service Creation): Personnel responsible for defining the Managed Service, including the incorporation of current Cisco technologies to provide differentiated service capabilities that address customer needs. Works cross-functionally to create and launch the Managed Service based on target market and refine it over time.

Cisco MS Management - Sales Specialist (Service Acceleration): Personnel responsible for accelerating sale of provider created Managed Service and as-a-service offers.

Cisco MS Practice Lead: The Cisco MS Practice Lead is a senior leader of the partner's MS team who owns the MS business strategy and supports practice development and growth. Setting the strategy for the MS practice, includes new service/offer creation, resource allocation, and managing customer Escalations.

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.

Infrastructure Cloud Provider

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 Provider's Data Center.

Cloud and/or Managed Services Reseller refers to either a Cloud Services Reseller or Managed Services Reseller who has entered into a contractual relationship with a Provider for resale of Cloud Services or Managed Services respectively.

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 Designation purposes. This allows partners to pool their resources across countries in order to qualify for Designations. Designations are granted to partners for each country within a country grouping; see details.

Customer Premises Equipment (CPE): For purposes of the Provider role, 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 Provider role 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 enterprise operated from a hosting center.

Customer Success Manager (CSM): A Cisco Customer Success Manager owns and is accountable for customer success. Ensures customers maximize the value of their technology investments throughout their complete lifecycle.

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.

Designation: as used in this document, refers to either a role (Integrator or Provider), a Specialization, a Master Specialization or Customer Experience Specialization.

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.

Executive Sponsor: The Executive Sponsor owns the budget and profit/loss accountability for the Managed Service practice development and is responsible for alignment to senior leadership on Managed Services business strategy and execution.

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 a Gold Integrator 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 Integrator 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 removal or move 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.

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.

Integrator Role or Integrator: The Integrator Role describes partners selling Cisco technology and services, adding their unique value to solve critical customer business challenges. Integrators continue to provide industry leading solutions for our customers, and we are committed to invest, reward and build strong partnerships while increasing flexibility and profitability. (Previously referred to as Gold Certification/Gold certified).

ITIL Foundation (v3 or higher): Personnel certified in Information Technology Infrastructure Library (ITIL) Foundation v3 or higher.

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.

Level 1 Support: Support personnel taking the first level customer calls, triaging, and managing calls in the local language if needed.

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.

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. 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 Provider 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 Provider partners who may or may not own NOC assets.

Partner: Partner, as used in this document, refers to the organization seeking either a Role (Integrator or Provider), an Architecture Specialization, a Master Specialization or Customer Experience Specialization within the Cisco 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 Designation is applied. All Partners, regardless of their business model, are required to meet the same requirements.

Partner Management & Application (PM&A): the tool used for the Designation application process.

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.

Product: Products mean hardware and can include related software and documentation as listed on the current Price List.

Provider Role or Provider: The Provider Role describes partners that deliver as-a-service and managed solutions through flexible consumption models - aligning to customer business goals, reducing CapEx costs, and lower operating risk. Providers make it possible for customers to focus on what's most important - their business. (Previously referred to as CMSP).

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.

Renewals Manager (RM): A Renewals Manager owns renewal opportunities and manages recurring revenue risk assessment and drives renewal execution.

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.

Sales and Marketing BDM (Service Delivery): Personnel responsible for business development of partner created Managed Services offers.

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

	Gold Integrator	Customer Experience	Master Specialization				Provider Role		
Policy	G	CES	Collab	Sec	Net	DC	GP	PP	SP
A3.1 Annual Renewal Qualification	·	·	·	·	·	·	·	·	·
A3.2 Get-Well Plans	·	·	·	·	·	·	·	·	·
A3.3 Downgrade	·	·	·	·	·	·	·	·	·
A3.4 Third Party Contracting (or Subcontracting)	·	N/A	N/A	N/A	N/A	N/A	·	N/A	N/A
A3.5 Mergers, Acquisitions, Divestiture, and Affiliates	·	·	·	·	·	·	·	·	·
A3.6 CCIE/CCDE/CSM Hiring and Terminating	·	·	·	·	·	·	·	·	N/A
A3.7 CCIE/CCDE/CCNA/CCNP Sharing	·	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
A3.8 CCIE/CCDE Contracting	·	N/A	·	·	·	N/A	N/A	N/A	N/A
A3.9 Competitor Policy	·	·	·	·	·	·	·	·	·
A3.10 Centers of Excellence (CoE)	·	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
A3.11 Language Requirements	·	·	·	·	·	·	·	·	·
A3.12 Provider Role Finance Policies and Procedures	N/A	N/A	N/A	N/A	N/A	N/A	·	·	·

A3.1 Annual Renewal Qualification

Policy regarding annual renewal of Designations.

Applies to: G, CES, Collab, Sec, Net, DC, GP, PP, SP (See Table)

Designation is valid for 12 months. Partners are expected to remain in compliance with the requirements throughout the anniversary year. Partner compliance is validated through an annual renewal review and potential audit and also through monthly compliance reports and automatic system checks.

- Partners must submit an online application for renewal by their anniversary date each year.
- Partners that have not submitted a complete application including all required documentation no later than 30 days after their anniversary date may have their Designation removed entirely.
- In order to maintain Designation, any required renewal audit must be conducted no later than 60 days after the partner's anniversary date (Cisco reserves the right to assign auditors based on availability)
- If a partner's renewal is delayed for any reason, including a Corrective Action plan to address a deficiency, the partner's anniversary date will not be adjusted. The partner will still be due for renewal on the next anniversary date.

A3.2 Get-Well Plans

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

Applies to: G, CES, Collab, Sec, Net, DC, GP, PP, SP (See Table)

Partner will maintain current Designation during the get-well period if they remain compliant with all other requirements. Failure to meet the Get-Well Plan requirements will result in loss of Designation and corresponding discount (when applicable). 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 anniversary year) are not allowed; this rule 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 anniversary year.

A3.3 Downgrade

Policy regarding partner downgrade for noncompliance to Designation requirements.

Applies to: G, CES, Collab, Sec, Net, DC, GP, PP, SP (See Table)

Cisco may move to the next eligible level or remove a Designation entirely for a partner if the partner fails to comply with requirements during the Designation 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

Partners are considered “net new” after six-months of having the Designation removed.

For Gold Integrator only, the following may also result in removal or move to the next eligible level:

- Failure to meet specialization requirements during renewal 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 the Provider role, the following additional requirements apply:

Cisco reserves the right to terminate a partner from participation in the Provider role for the following reasons:

- Submission of false, misleading, or incomplete Provider 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 Provider role and deploying Product in non-managed environments

Downgrade from the Provider role will result in the loss of privileges, branding, and rebates associated with the partner's Provider role Designations (when applicable).

A3.4 Third Party Contracting (also referred to in this document as subcontracting)

Policy for subcontracting partner’s support service (as required for Designation) to a third party. This policy covers call center operation, technical support, and onsite service.

Applies to: G, GP (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 the role.
- 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 the role.
- 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 (Integrator only):

For Gold Integrator Partner Support 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 (Provider role 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 Provider role qualifications, Provider must retain contractual relationship with the customer. Additional Third-Party contractual relationships are addressed on a per-Designation basis in the Provider Requirements.

A3.5 Mergers, Acquisitions, Divestiture, and Affiliates

Policy related to Designation of a business entity formed by a merger or acquisition or where the resources and staff fulfilling the Designation requirements are controlled or employed by more than one legal entity.

Applies to: G, CES Collab, Net, Sec, DC, GP, PP, SP (See Table)

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.

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 Designation are controlled or employed by different companies within the same corporate group, Cisco will grant Designation 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, Designation is granted for a single company within a country/country group.

Cisco requires that the resources and staff relevant to the applicant's Designation 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 Designation qualification, certified individuals must be full-time or full-time equivalent employees of the company based within the country for which Designation 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 Designation. 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 an Integrator can benefit from the same discount of the Integrator. The non-certified business division will not be able to use the branding of the division holding the Integrator role.

Notwithstanding the foregoing, in the case where Company in the United States is owned or controlled by a foreign entity, and the United States Federal Government ("USFG") has ordered Company to create a separate business entity or subsidiary to conduct all Federal business ("Government Subsidiary"), such Government Subsidiary will be granted all Designations of the Company if, and during such time that the following conditions are met:

1. Company must currently hold the Gold Integrator role in good standing.
2. Company must provide a USFG approved and signed Affiliate Operations Plan that specifies the resources that will be shared between Company and the Government Subsidiary.
3. Company must go through the process, with the assistance of their Partner Account Manager (PAM), to request and be approved for a separate Business Entity Geography (BE GEO) ID for the Government Subsidiary.
4. The Government Subsidiary will be required to submit to Cisco's standard Gold Integrator Partner Capability Review ("PCR"), set forth under the Partner Capability (PCR) section, within 90 days of notifying Cisco of their intent to share the Gold Integrator role and Architecture Specializations. The Government Subsidiary will need to show how the shared resources will maintain all the required processes outlined in the PCR. The Government Subsidiary will be responsible for the cost of the PCR. The PCR must only be completed once by the Government Subsidiary.
5. The Government Subsidiary's Resale of Cisco products and services will be solely to the USFG. Resale to any other customers will result in the revocation of all the Government Subsidiary's Designations.
6. If the Company's Gold Integrator role is removed for any reason, the Government Subsidiary will also have all Designations removed.
7. Cisco reserves the right to review the terms set forth herein at any time and modify (including rights to discontinue) the Designations for the Government Subsidiary.

Mergers

Regardless of when companies merge, Cisco 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 Designations achieved until the new legal contract is signed, If the new entity has an indirect buying contract, documentation of the merger will be required (e.g., email confirmation from the Cisco Customer & Partner Data Operations Team).

An audit may be required within 90 days of the merger in order to verify that the combined company meets all requirements for that Designation. 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.

If the above criteria is indeed achieved, the affiliate location would be able to leverage the Gold Integrator direct discount if purchasing direct from Cisco, however, the affiliate entity would not appear as a Gold Integrator in Partner Locator.

Divestiture

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

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 Designation only if the partner can demonstrate that those staff and resources after the divestiture continue to meet the requirements of the Designation.

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 Designation. 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 Designation of the partner franchisors.

Joint Venture

An enterprise undertaken jointly by two or more parties which otherwise retain their distinct identities and does not receive any special recognition (branding or discounting) for the Designation of the partner party.

A3.6 CCIE/CCDE/CSM Hiring and Terminating

Policy regarding loss of a CCIE, CCDE or CSM or hiring of a CCIE, CCDE or CSM from another Cisco partner holding a Designation.

Applies to: G, CES Collab, Sec, Net, DC, GP, PP (See Table)

Losing Partner

If the loss of a CCIE, CCDE, or CSM takes a partner below the number of individuals required for a Designation, partner is to notify Cisco of its noncompliance within 30 days. (Notification may be made either via email to Partner Account Manager (PAM), to the Cisco Systems Engineer (SE), to the Certification Program Manager (PM) or by opening a case with Customer Service).

Upon receipt of such notice, partner may qualify for a Get-Well Plan of up to 12 months to replace the CCIE, CCDE or CSM, in order to avoid losing the Designation that requires a CCIE, CCDE or CSM. During the Get-Well Plan period, the partner will retain its Designation as long as all other Designation requirements are met. This Get-Well Plan period does not protect other out of compliance issues, nor should it delay any standard process to renew. Two consecutive Get-Well Plans (back-to-back) for CCIE, CCDE or CSM are not allowed.

If a partner does not notify Cisco of its noncompliance with the CCIE, CCDE or CSM 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, CCDE or CSM in order to avoid losing the Designation that requires a CCIE, CCDE or CSM. 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, CCDE or CSM during the anniversary year; multiple Get-Well Plans will not be granted, and partner will be moved to next eligible level of the role, Specialization or to Registered Partner status (Designation removed entirely); the CCIE, CCDE, CSM 12-month policy does not allow the losing partner to continue counting the departing CCIE, CCDE or CSM's badge towards their Designation; 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. CCDE or CSM badge towards their Designation.

Gaining Partner

If a partner hires a CCIE, CCDE or CSM away from another Cisco partner holding a Designation, Cisco will not count this individual towards a Designation for the hiring partner for a period of 12 months from the termination date of the previous partner. This rule does not apply if the losing Cisco 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 partner holding a Designation 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, CCDE or CSM to support another partner's Designation. The letter must also include the last date of employment.

A3.7 CCIE/CCDE/CCNA/CCNP Sharing

Policy regarding sharing of CCIE/CCDE/CCNA/CCNP required for the Integrator role.

Applies to: G, and Multinational Certification (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 Gold Integrator role for the CSC country or any other countries. The remainder of the required number of CCIEs must be located in the country applying for the Gold Integrator role.
- 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 the Gold Integrator Role.
- 50 percent of the required CCNAs/CCNPs may be utilized from a CoE*. These engineers must be distinct from those nominated for in-country Gold Integrator 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 the Gold Integrator role.
- If a remote country is not using a CoE, all CCIEs/CCNAs/CCNPs required for the Gold Integrator role must be in-country.
- Partners with a current Provider role who own their NOC and want to use Consolidated Support model do not require a separate CoE audit and may utilize the CCIE/CCNA/CCNP allowances outlined above.

*Allocation is completed by Cisco Certification Program Manager

A3.8 CCIE/CCDE Contracting

Policy regarding contracting out required CCIEs, including to Cisco Learning Solution Partners (CLSP).

Applies to: G, Collab, Sec, Net (See Table)

CCIE/CCDE's required for the Integrator role or Master Specialization must be legally employed by the applying partner in the country where the partner is seeking Designation. 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 Designation 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 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 Designations. Partners who violate these guidelines in their partner agreements will be immediately de-authorized.

Provider Role only: CCIEs must be full time regular employees of the Provider.

A3.9 Competitor Policy

Policy regarding direct competitors to Cisco not being eligible for Designations.

Applies to: G, CES, Collab, Sec, Net, 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 any Designation status pursuant to the Cisco 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 Partner or 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 remove a Designation entirely for a Direct Competitor (including without limitation a current 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 remove a Designation entirely for a Direct Competitor in any instance shall not operate as a waiver of Cisco's right to remove a Designation 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.

A3.10 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: Integrator Role
Applies to: G, (See Table)

A partner that operates a Gold Integrator 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 who currently hold the Provider role 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 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 role 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 Designation 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 Designation.
- Lab Equipment for Partner Support Services (PSS) (Collaborative) Partners Equipment necessary to satisfy the demonstration and post-sales lab requirements for Designation 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 Integrator 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 Designations in remote countries, the CoE lab access and policy will be audited in concurrence with the remote country Audit.

Audit Requirements: Remote Country Using Center of Excellence (CoE) Support

If a country operation seeking Designation 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 Designation, 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 Designation 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

A3.11 Language Requirements

Policy regarding language requirements for audit documents.

Applies to: G, CES, Collab, Sec, Net, DC, GP, PP, SP (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.

A3.12 Provider Role Finance Policies and Procedures

Policy regarding Ordering Process Validation and Order Audit Policy

Applies to: GP, PP, SP (See Table)

Provider Pricing:

See http://www.cisco.com/go/provider.html for more information including the definition of eligible Products for Provider Pricing.

Valid Ordering Process

All orders placed for Products used in a Managed or Cloud Service 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 Provider Pricing. Retroactive credit will not be granted for orders placed incorrectly.

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

Provider Order Level Audit Policy (ALL Providers are subject to this requirement)

- Cisco reserves the right to audit any and all orders made under the Provider role.
- These order level audits are separate from the up-front Provider enrollment and Provider role audit.
- The goal of this audit is to validate 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.
- Providers 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 a Provider 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.

Provider 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 Provider designated Cloud or Managed Services from the partner with those Cloud or Managed Services being managed from the Provider 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.

Appendix 5: Provider Role Program Terms and Conditions

The terms and conditions set forth in Appendix 5 (the “Terms”) are between the company you listed in the applicable Provider role Application ("Provider") and the Cisco entity(ies) (“Cisco”) in which Partner has entered into a Systems Integrator Agreement (“SIA”), Cisco Indirect Channel Partner Agreement (“ICPA”) or other pre-existing agreement with Cisco covering resale, Cloud Services or Managed Services Agreement (Collectively referred to hereafter as the “Agreement”). The Terms set forth the requirements for obtaining and maintaining the applicable level offered under the Provider role within the Cisco Partner Program and supplements the most current Agreement in effect between Cisco and Provider. All capitalized words have the meaning ascribed to them in Appendix 1 (“Definitions”) or as defined in the Cisco Channel Program 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.** Provider's receipt of the benefits associated with a particular level in the Provider role within the Cisco Partner Program, including but not limited to rebate and/or discount, constitutes Provider's continuing representation that it is in compliance with the Terms including all role requirements associated with the level for which Provider has received benefits. In the event Provider receives role benefits for which it is not entitled by reason of its failure to maintain role requirements, and/or providing false or misleading information, Cisco reserves the right to revoke Provider's role status and require Provider to repay such financial benefits received directly or indirectly from Cisco as a role level benefit, including but not limited to repayment of any additional discounts provided. All Providers, regardless of their business model, are required to meet the same role requirements.

2. **General Terms.** The Provider role is available globally pursuant to the Terms. Product must be purchased only from authorized sources as set forth in Provider's Agreement. In addition to any of its other remedies, Cisco reserves the right to terminate a Provider from participation in the Provider role within the Cisco Partner Program for the following reasons: (a) submission of false, misleading, or incomplete information, including inaccurate claims for sales made under the Provider role within the Cisco Partner Program; (b) fraud or abuse of the Provider role within the Cisco Partner Program or other Cisco marketing or sales programs; (c) the distribution of Cisco Products purchased from an unauthorized source as set forth in Provider's Agreement; and, (d) the sale of Cisco Products to anyone other than an End User as defined in Provider's Agreement. Cisco reserves the right to use third parties, who will act on behalf of Cisco to perform administrative functions. .Provider agrees that for so long as it participates in the Provider role within the Cisco Partner Program, when Provider purchases Customer Premises Equipment ("CPE") for use in any Managed or Cloud Service offered by the Provider to End Users, Provider shall do so pursuant to these Terms and its Agreement and shall not purchase CPE for use in a Managed or Cloud Service pursuant to any Infrastructure purchase agreement with Cisco. Providers who participate in Cisco's Specializations must abide by all Specialization rules. Product(s) covered under Cisco's Specializations and available by way of selective distribution must meet all Specialization requirements for both bill to and ship to countries.
3. **Changes to these Terms.** Cisco may modify or cancel these Terms (including changes to the role level requirements in the Provider role within the Cisco Partner Program) as it deems appropriate and shall notify Provider of any such changes, which notice may be through posting on the Cisco Channel Partner Program Website. Such changes may adversely impact Provider's ability to qualify for role level status. Any such changes to the requirements will not affect Provider's corresponding role for the remainder of the current 12-month term. Cisco will provide Provider with a minimum of 90 days' notice prior to the effective date of any such changes.
4. **Non-Compliance with role level Requirements.** If Cisco becomes aware that a Provider is no longer in compliance with the applicable requirements, Cisco reserves the right to revoke the role. Provider agrees to promptly notify Cisco of any non-compliance with the applicable requirements, but in no event more than thirty (30) days after Provider first becomes aware of its non-compliance. Upon receipt of such notice, Cisco may in its sole discretion, provide Provider with a grace period in which to renew its compliance with the applicable requirements. Provider's failure to provide notice of non-compliance may disqualify Provider from receiving such grace period. If no grace period is granted or if Provider fails to comply with the requirements by the end of the grace period, Cisco reserves the right to revoke the applicable role status immediately or reclassify the eligible role level. Cisco may monitor Partner's compliance with the applicable requirements of a previously granted Designation at any time. If Cisco believes Provider may no longer be in compliance with the applicable requirements, Cisco reserves the right to conduct an onsite audit of Provider'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 Provider 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 Provider may use in conjunction with the Cisco Powered Logo trademark(s) to promote Provider's Cisco Powered Services Designation status once Provider 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 Provider a worldwide, nonexclusive, nontransferable,

royalty-free, personal license to use the Cisco Powered Logo solely in connection with the Provider's service(s) which has met the applicable Designation requirements and solely in the manner described in the Cisco Powered Logo usage Guidelines. Provider acknowledges that the Cisco Powered Logo is owned solely and exclusively by Cisco and Provider hereby acknowledges and agrees that, except as set forth herein, Provider 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. Provider 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 Provider 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 Provider the right to use the Designation Descriptor with the Cisco Powered Logo subject to the Logo License above and solely in connection with the Provider'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. Provider 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 Provider's right to use the Cisco Powered Logo and the Designation Descriptor.
8. **Indemnification.** Provider 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 Provider'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 Provider's services including but not limited to third party claims that Provider has not met its Service Level Agreements or any contractual obligations or representations or warranties made between Provider and its customer or that Provider's service does not meet certain performance or other specifications or that the services do not meet the Cisco Powered Services or other applicable role requirements. As a condition to such defense and indemnification, Cisco will provide Provider 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 PROVIDERS WHO OFFER CLOUD AND MANAGED SERVICES THROUGH SERVICES RESELLERS:**

   9.1 RESPONSIBILITIES OF SERVICES RESELLER PROVIDER

   The Provider and Services Reseller must at all times be in compliance with their respective Agreement and these Terms.

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

A Provider entering into a Cloud and/or Managed Service resale relationship with a Services Reseller must enter into a contractual agreement with such 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 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 Provider and the Services Reseller.

The Services Reseller and Provider must establish a set of Escalation procedures including priority levels, procedures, and associated penalties, if missed.

The Cloud and/or Managed Services Reseller and Provider must establish a change control process for handling End User changes and a change control process for managing changes between the Services Reseller and the Provider.

9.2 RESPONSIBILITIES OF THE SERVICES RESELLER

9.2.1 Either the Services Reseller or Provider (as agreed between the Services Reseller and Provider) shall designate a primary single point of contact to whom communications regarding 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 Services Reseller or Provider (as agreed between the Services Reseller and 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 Services Reseller may: a) market the Provider's Cloud and Managed Services (including the Cisco Powered Designation for Provider's Cisco Powered Cloud and Managed Services) acting on behalf of the Provider as a referral agent; and, b) sell the Provider's Cloud and/or Managed Services: 1) acting on behalf of the Provider reselling such services directly to End Users under the Provider's brand; or, 2) acting as an OEM reselling such services as its own.

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

9.2.5 Where the 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 Designation.

9.2.6 Either the Services Reseller or Provider (as agreed between the Services Reseller and 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 Services Reseller must provide details of service coverage.

9.2.8 The Services Reseller shall create a Marketing Services Description (MSD). The MSD is a document produced by the 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 Provider and the Services Reseller.

9.4 CISCO SERVICES.

Where the Services Reseller is responsible for Product procurement and sales, the 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.

10. HCS Software Restrictions. Providers who have purchased Cisco collaboration Software from Cisco for the purpose of reselling a hosted collaboration solution (“HCS Software”), shall not use such HCS Software as part of a FedRAMP authorized solution.

Definitions

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

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

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

Provider means a Cisco partner that has met and maintains the Provider role within the Cisco Partner Program

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

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

Appendix 6: Outsourcing NOC Operations

Introduction

Providers may outsource some elements or the entire NOC operations to a single specialized NOC Services Provider who is not a Cisco competitor. Provider may or may not (owned by NOC Services Provider) own NOC assets.

Providers 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 renewal audit. An audit may be required within 90 days of the change in order to validate that the company continues to meet role requirements for that level.

Below is a summary of Provider requirements that can be outsourced, and the Provider can still meet published requirements to be approved into the Provider role. Provider 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; Select Providers must also meet the requirements in section 3.3.

Note: Partner will receive Provider level and Cisco Powered Services Designation upon audit approval.

Provider Responsibilities

Providers 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 Providers 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 Provider 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 Provider.
- **Call tracking and monitoring systems between Provider and NOC Services Provider:** Listing of call tracking systems used and the integration of the systems between Provider and NOC Services Provider’s systems
- **Access to Provider /NOC Services Provider information (Knowledge Base sharing):** Description of common repository and access to Provider 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 Provider 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 Provider 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 Provider/NOC Services Provider information (Knowledge Base sharing):** Demonstration of sharing of best practices, Knowledge Base by both Provider and NOC Services Provider.

NOC Services Provider Responsibilities

- Must have at least 1 ITIL certified employee.
- Must have secure access by authorized personnel to Provider's network.
- May or may not be an Integrator or a Provider partner.
- Must provide network and personnel access to the auditor to validate processes, procedures etc., to meet Provider partner requirements.

Outsourced NOC Services Requirements Overview

Requirement	Provider role
	Gold Provider (GP)
3.3.1 Personnel	N/A
3.3.2 Project Plan	N/A
3.3.3 Project Objectives	N/A
3.3.4 Project Charter	N/A
3.3.5 Resource Management	N/A
3.3.6 Customer Requirements	N/A
3.3.7 Project Start Meeting	N/A
3.3.8 Risk Management	N/A
3.3.9 Project Milestones	N/A
3.3.10 Customer Communication Plan	N/A
3.3.11 Project Implementation	N/A
3.3.12 Project Review and Evaluation	N/A
5.2.1 SLAs/SLOs	·
5.2.2 Service Level Measurement and Reporting	·
5.2.3 Parts Replacement	·
5.3.1 Business Capacity	·
5.3.2 Service Capacity	·
5.3.3 Resource Capacity	·
5.3.4 Capacity Improvements	·
5.4.1 Availability Measurement	·
5.4.2 Availability Reporting	·
5.4.3 Availability Review and Planning	·
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	·
5.6.1 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	·

Requirement	Provider role
	Gold Provider (GP)
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	·
6.1.1 Risk Management	·
6.1.2 Redundant Management Connection	·
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	·
6.3.1 Change Management Process	·
6.3.2 Phased Release	·
6.3.3 Configuration Item (CI) Identification	·
6.3.4 Software and Hardware Repositories	·
6.4.1 Data Collection Process	·
6.4.2 Configuration Control Processes and Tools	·
6.4.3 Configuration Change Plans	·
6.5.1 Service Validation and Testing Process	·
6.6.1 Service Evaluation Process	·
6.7.1 Information Availability and Accessibility	·
7.1.1 Customer Service Availability	·
7.1.2 Local Language Answering	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	·
7.2.1 Service Request Process	·
7.2.2 Automated Service Request Tool	·
7.3.1 Event Management Process	·
7.4.1 Incident Management Process	·
7.4.2 Managed Device Monitoring	·

Gold Integrator Role (G); Master Specialization: Collaboration (Collab), Security (Sec); Networking (Net), Data Center and Hybrid Cloud (DC); Customer Experience Specialization (CES) Provider Role: Gold Provider (GP), Premier Provider (PP), Select Provider (SP)

Requirement	Provider role
	Gold Provider (GP)
7.4.3 Fault and Performance Data Monitoring	•
7.4.4 Management Platform	•
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	•
7.5.1 Problem Management Process	•
7.5.2 Root Cause Analysis	•
7.5.3 Closed Loop Corrective Action	•
7.5.4 Proactive Problem Management	•
7.6.1 Access Management Process	•
7.7.1 Onsite Response/Troubleshooting Description	•
7.8.1 Remote Access	•
8.1.1 Continual Improvement Activities	•
8.1.2 Continual Improvement Methodology	•
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	•
8.3.1 Service Reports	•
8.3.2 Cloud or Managed Service Contracts	•

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA

NG/LW-21003 08/2022