Master Security Specialization Requirements

Step 1: Pre-Audit Validation

These requirements will be validated remotely before the onsite audit is scheduled.

Requirement	Evidence
Advanced Security Architecture Specialization (ASAS)	Partner must hold the prerequisite. Check is done through an internal system validation through the Program Management and Application (formerly CSApp) web tool.
CCIE Security*	Assign individual in Program Management and Application
CCNP Security*	Assign individual in Program Management and Application
One Project Management Certification: PMI (PMP) or Prince 2	Partner uploads certificate to Program Management and Application
Fire Jumper*	Partner to designate a person holding Fire Jumper role in the new or renewing specialization application.
Partner Executed Proof of Value (POV)	Three POVs are required for each new and renewal Masters audit For detailed information, refer to the POV Consolidated Post on the Partner Security Community: https://communities.cisco.com/docs/DOC-65405 POVs must be for pre-sales customer opportunities not lab or post-sales deployments Note: Each of the POVs submitted must be from the past 18 months, POVs may not be re-used from previous audits. The following proof-of-performance items must be uploaded to PMA for each POV 1. Data Collection Worksheet 2. Win criteria 3. POV Outcome 4. Customer Facing Reports 5. Bill of Materials
Customer References: Documentation to validate five** sophisticated deployments based on specific qualifying security criteria (see Master Security Customer Reference & POV Checklist)	Complete the customer reference document, which includes customer reference account deployment summaries, for the five** customer references. **Recertification Applications require three customer references. A Cisco Channel Systems Engineer (SE) reviews the customer reference document and validates deployments. The SE must upload the customer reference checklist into Program Management and Application or sign the copy uploaded by the partner admin. This indicates review and validation of the customer reference checklist.

*Three (3) Unique individuals must fulfill pre-requisite CCIE, CCNP & Fire jumper roles

Step 2: Onsite Audit

After your application has been validated by a Cisco Certification Program Manager, he or she will forward your application to the third-party auditing firm who will contact you to arrange an audit date.

Requirement	Preparation
Onsite Audit Capabilities Validation (including Practice Areas)	All requirements for the onsite audit are found in Cisco Channel Program Audit & Policies document, including 'Practice Areas' where partners must validate proficiency in at least three (3) out of the six (6) available practice areas. Please prepare accordingly.
Onsite Audit Demonstration (New option for Master Security partners only to use dCloud. This is not required.)	Be prepared to perform a demonstration as per the Master Security Demonstration Checklist. A recommended list of resources for audit demonstration is available in the Master Security Audit FAQ.
Need Assistance? **Problem**	**Action**
Need additional information?	Visit Master Security FAQ for answers to commonly asked questions
If you are having issues with your online application, or Cisco online web tools:	Open a support case
If you have questions, issues, or concerns with regard to the audit process, demonstration requirements, or other issues related to this qualification:	Please contact your Partner Account Manager or Systems Engineer or send an email to Master-security@cisco.com

Note: If a partner does not remain in compliance with the applicable specialization or certification requirements, Cisco reserves the right to revoke the specialization or certification at any time. Partners must notify Cisco of its non-compliance promptly, but in no event more than thirty (30) days after partner first becomes aware of its non-compliance. Upon receipt of such notice, partner may qualify for an extension of time in which to renew its compliance with the applicable specialization or certification requirements. Partner's failure to provide such notice may disqualify partner from receiving such an extension. If no extension is granted or if partner fails to comply with the certification or specialization requirements by the end of the extension period, Cisco reserves the right to revoke the applicable specialization or certification immediately. Additional information regarding non-compliance may be found in the Audit and Policies Document.

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 10/17