



SC Content & Audit Management System Security Audit Partner Roles and Responsibilities

This document contains the information for Cisco Partners to use the Supply Chain Content and Audit Management System for Security Audit.

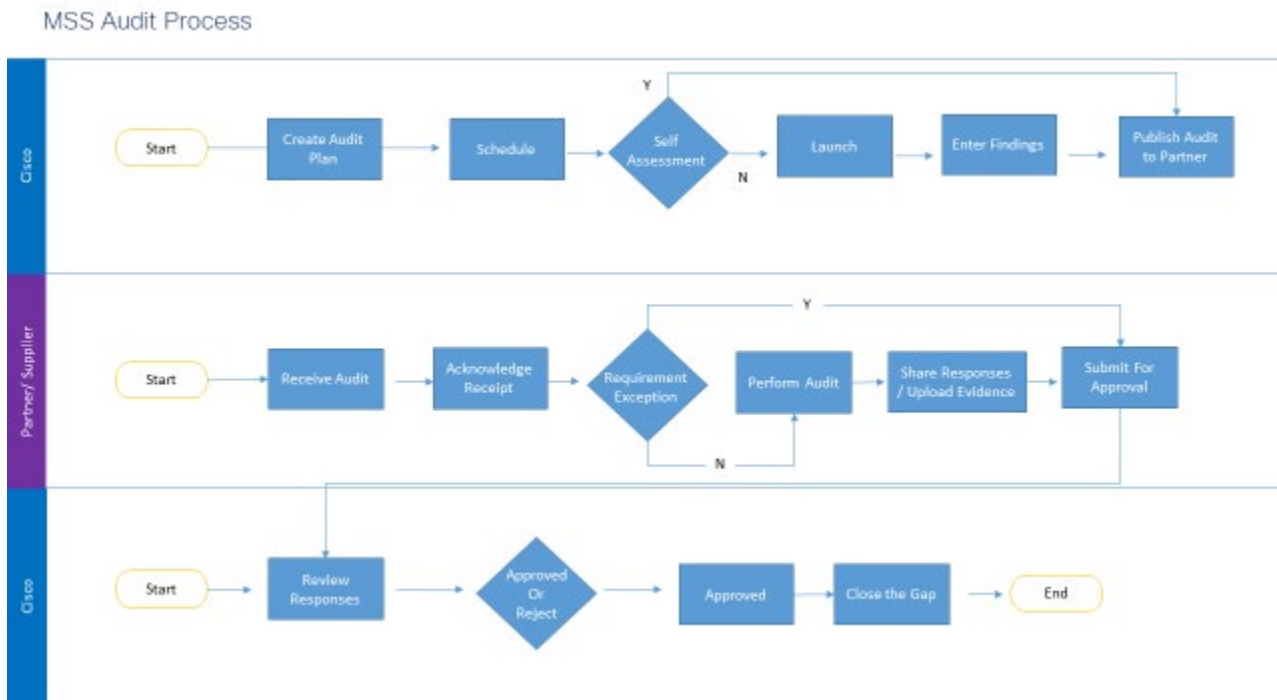
This system replaces previous methods for partners to acknowledge and complete security audits. If you have questions not covered by this documentation, contact your Cisco Regional Security Lead.

Table of Contents

Introduction of SC Security Audit Process Roles (Cisco & External)	2
The Different States of an Audit	2
Overview of Cisco Partner Roles	3
Getting Access to the Tool (link to separate doc)	4
Logging in to the Tool	4
Acknowledging an Audit	5
Submitting an Exception	7
Accepting the Audit	8
Completing and Submitting an Audit for Approval	8
Changing Partner Owner	11
SC Security ReelID CHIP Audit Process Roles	13
Responding to a ReelID CHIP Audit	13
Resubmitting a ReelID CHIP Audit	15

Introduction of SC Security Audit Process Roles (Cisco & External)

The SC Content and Audit tool replaces earlier systems used to distribute, receive and track audits. See below to follow the process of an audit from creation to final approval across Cisco roles (blue rows) and Partner ones (purple).



The Different States of an Audit

These are the different states of an audit.

- **Draft** -- when Cisco determines an audit of a partner company is needed, a Cisco auditor will begin the creation of an audit survey. This is the Draft phase of the audit.
- **Scheduled** – when the draft is complete, the auditor will schedule the audit to be published, and sent to the partner company on a specific date. The status now becomes scheduled. The schedule acts as an audit calendar for the audit owners.
- **Launched** – for audits that are conducted on-site, they may be launched so that a Cisco auditor can conduct the assessment at that time, or on a future date.
- **Published** – when the publish date arrives, the audit owner will publish the audit. The system will then send out notification emails to previously identified people at the partner company. If the audit is a self-assessment, the partner company will begin work on the controls. If it is an on-site assessment, conducted by Cisco, the published audit will include the input that Cisco has entered.
- **Acknowledged** – those identified people receive an email notifying them of the audit, and they enter the SC Content and Audit tool. One of those people will acknowledge the audit, becoming the Action owner, and the audit status changes to Acknowledged.
- **In Progress** – when that action owner starts working on the audit, its status is again changed, this time to In Progress. The audit will remain in this In Progress state until the audit is completed.
- **Closed** – when the Cisco audit owner sees that the partner company has completed the audit survey, and all approvals are complete for the audit responses, the Cisco audit owner will close the audit.

- **Unpublished** – after an audit is published, the Cisco auditor can un-publish an audit that is in the published state. In other words, before the partner company acknowledges the audit. This may be because a change needs to be made to the audit, or the auditor wants to cancel the audit. If making a change, the auditor can re-schedule the audit so it can be published with the changes and then sent to the partner company.

The states of an audit may be viewed on the main screen, color coded by the key at the bottom of the screen.

The screenshot displays the Cisco Supply Chain Audit Management interface. At the top, there are navigation tabs: "Manage Audit Plans", "Manage and Release Templates", and "Audit Planning and Scheduling". Below these are buttons for "View All - Audits", "Refresh", and "Change Audit Owner". The main area is a table with columns: Audit #, Audit Name, Last Update Date, Audit Status, Audit Owner, Supplier, Supplier Location, Audit Type, Schedule Date, and Audit Date. A red box highlights the first column (Audit #) and the legend at the bottom. The legend shows color-coded boxes for Draft (grey), Scheduled (yellow), Published (orange), UnPublished (purple), Acknowledged (green), In Progress (blue), and Closed (red). There are also checkboxes for "Action/s available" and "Action/s unavailable".

Audit #	Audit Name	Last Update Date	Audit Status	Audit Owner	Supplier	Supplier Location	Audit Type	Schedule Date	Audit Date
MSS-247	STD-MSS-4-FLEXTRONICS-FLEX - DOUMEN	10/30/2018 08:55:28	In Progress	ashevde	FLEXTRONICS	FLEX - DOUMEN	SELF-ASSESSMENT	10/30/2018	10/30/2018 08:55:28
MSS-246	STD-MSS-1-TRIPOD TECHNOLOGY CORPO...	10/30/2018 08:51:13	In Progress	ashevde	TRIPOD TECHNOLOGY...	TRIPOD - WUXI PCB 2	SELF-ASSESSMENT	10/30/2018	10/30/2018 08:51:13
MSS-244	STD-MSS-1-TRIPOD TECHNOLOGY CORPO...	10/29/2018 21:00:20	Published	maitinguy	TRIPOD TECHNOLOGY...	TRIPOD - WUXI PCB 4	SELF-ASSESSMENT	10/29/2018	
MSS-242	STD-MSS-1-TRIPOD TECHNOLOGY CORPO...	10/29/2018 17:44:56	In Progress	maitinguy	TRIPOD TECHNOLOGY...	TRIPOD - WUXI PCB 3	SELF-ASSESSMENT	10/29/2018	10/29/2018 17:44:56
MSS-243	CST-SELF-34-FLEXTRONICS-FLEX - DOUM...	10/29/2018 17:42:23	In Progress	ashevde	FLEXTRONICS	FLEX - DOUMEN	SELF-ASSESSMENT	10/29/2018	10/29/2018 17:42:23
MSS-241	STD-MSS-6-TRIPOD TECHNOLOGY CORPO...	10/29/2018 16:50:08	Published	maitinguy	TRIPOD TECHNOLOGY...	TRIPOD - WUXI PCB 2	SELF-ASSESSMENT	10/29/2018	
MSS-240	STD-MSS-1-TRIPOD TECHNOLOGY CORPO...	10/29/2018 11:47:14	In Progress	maitinguy	TRIPOD TECHNOLOGY...	TRIPOD - PINGJEN	SELF-ASSESSMENT	10/29/2018	10/29/2018 11:47:14
MSS-239	STD-MSS-11-TRIPOD TECHNOLOGY CORP...	10/29/2018 10:26:19	In Progress	maitinguy	TRIPOD TECHNOLOGY...	TRIPOD - PINGJEN	SELF-ASSESSMENT	10/29/2018	10/29/2018 10:26:19
MSS-238	STD-MSS-5-TRIPOD TECHNOLOGY CORPO...	10/29/2018 09:46:30	In Progress	maitinguy	TRIPOD TECHNOLOGY...	TRIPOD - WUXI PCB 4	SELF-ASSESSMENT	10/29/2018	10/29/2018 09:46:30
MSS-237	EDCS-15684112-TRIPOD TECHNOLOGY CO...	10/26/2018 15:13:06	In Progress	ashevde	TRIPOD TECHNOLOGY...	TRIPOD - WUXI PCB 3	SELF-ASSESSMENT	10/26/2018	10/26/2018 15:13:06
MSS-236	CST-SELF-35-TRIPOD TECHNOLOGY CORP...	10/26/2018 12:05:11	In Progress	ashevde	TRIPOD TECHNOLOGY...	TRIPOD - WUXI PCB 2	SELF-ASSESSMENT	10/26/2018	10/26/2018 12:05:11

Partner Roles

Security Partner Doc Owner

- Can acknowledge Audit plan
- Can add exception to the Audit plan
- Can accept the Audit plan

Note: the Audit template is sent to the company, multiple people at your company might be receiving the same notification. Any of the people receiving the notification can acknowledge that Audit template has been received.

Security Partner Audit Owner

- Can perform the Audit Plan
- Can submit Audit Results: Pass/ Fail / N/A
- Can submit Audit Result to Cisco for approval

Note: This can be the same person who has played the role of the Security Partner Doc Owner or not.

Getting Access to the Tool

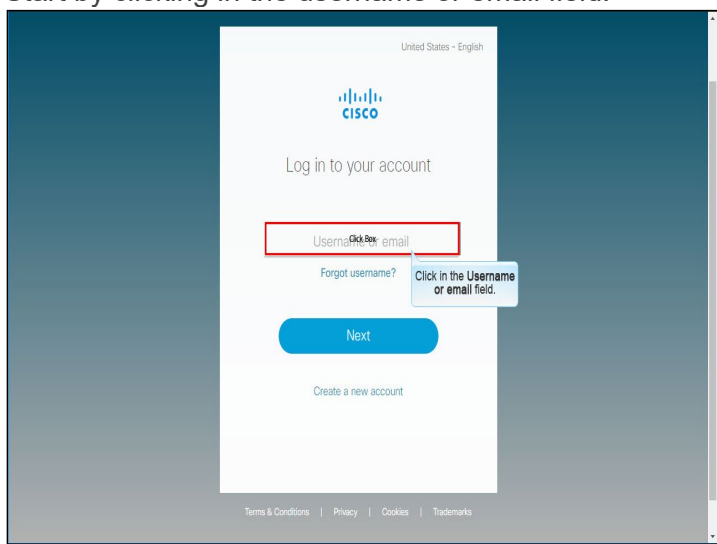
You will need to request access to the tool based on your current job role in your company. See the attached document for instructions on getting access and logging in.



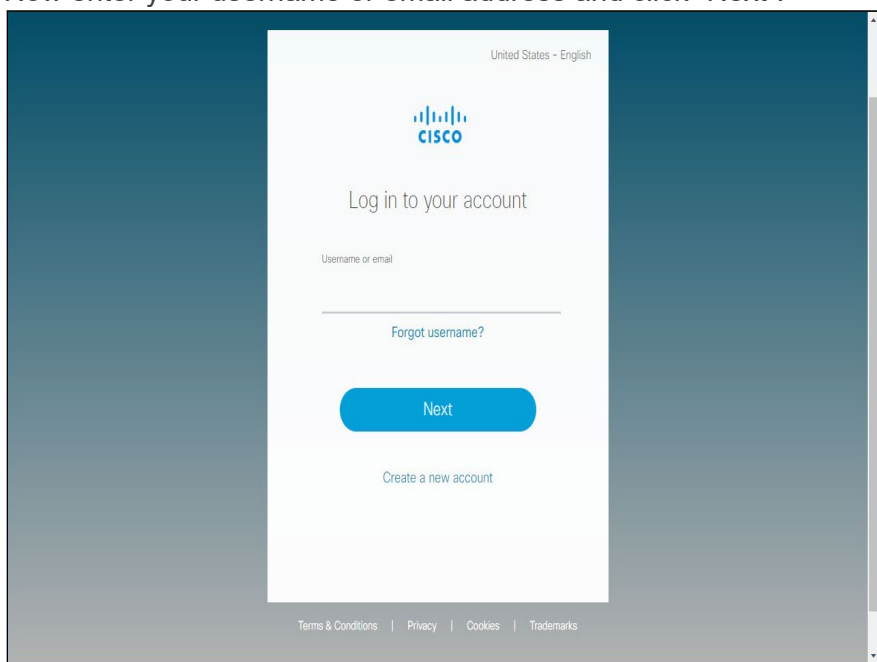
Training- Content Management - External User Onboarding.pdf

Logging in to the Tool

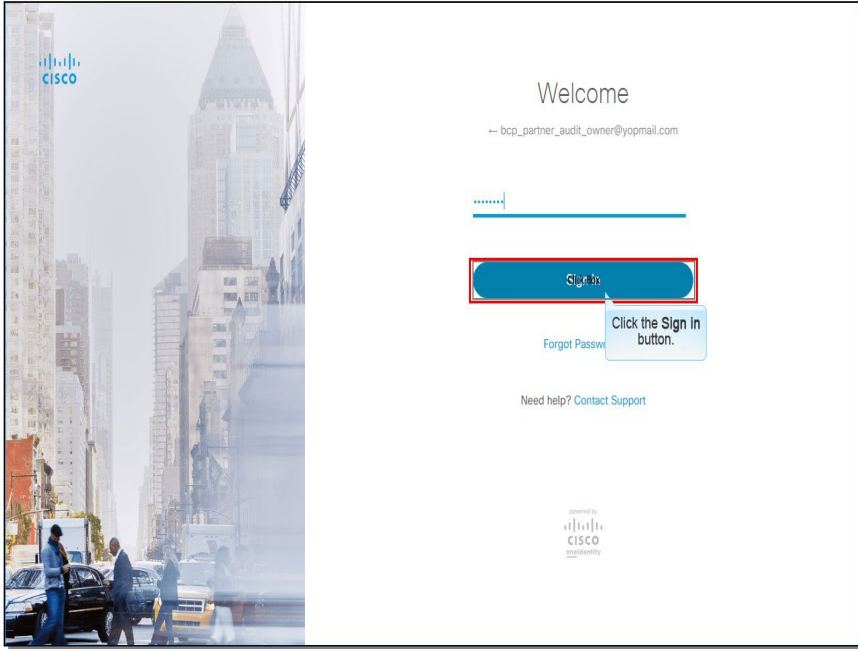
Note: You must have a CCO ID to access the tool. Clicking that link brings you to the Audit tool's log in page. Start by clicking in the username or email field.



Now enter your username or email address and click "Next".



Enter your password in the password field and click “Sign In”.



NOTE – The tool may only be accessed by a Chrome or Firefox Browser. It is NOT available via Internet Explorer.

Acknowledging an Audit

Description	Steps & Screenshot
	<p>The first step a partner takes in the audit process is to acknowledge receipt of the published audit. When the audit is published, a notification will be sent to the partner that it is time to acknowledge the audit. This notification is received via email and looks like this:</p> <p>*****</p> <p>Title: ACTION REQUIRED – Cisco Security Self-Assessment Audit (AUTO FILL IN DOC # (Example STD-MSS-1)) From: no-reply-sc-audit-notification@cisco.com Date: AUTO FILL IN</p> <p>Hello: A Cisco Security Self-Assessment Audit has been created for you NAME HERE</p> <p>Please acknowledge receipt of the audit by clicking here and taking appropriate actions.</p> <p>Your prompt action is appreciated. Thank you.</p> <p>*****</p> <p>Follow the steps to acknowledge the audit. You will need to log in (steps above). The person who acknowledges the audit will become the audit owner. The audit owner can easily be changed in the system by selecting the audit and clicking the “Change Partner Owner” button.</p>
<p>Entry Screen</p> <p>Check your role.</p> <p>Only the roles you have access to will show in the drop-down box.</p>	<p>Step 1. Choose role Security Partner Doc Owner.</p> <p>Step 2. View All Docs or a Subset of them by selecting from the drop-down list.</p>

Select the document and view the controls if needed.

Step 4. Select the link to view a document.

Step 3. Select the document. It will be in "Published to Partner" status.

Doc/Template #	Doc/Template Title	Last Updated Date	Action Status	Cisco Process Owner	Partner	Partner Site	Notes For Partner	Partner P O C	More Info
STD-MSS-1	Standard Template for...	10/01/2018 08:20:46	Published To Partner	rarahghw	FLEXTRONICS	FLEX - DOUMEN	*** Notes added on 1...		
STD-MSS-2	Standard Template for...	09/25/2018 12:09:03	Accepted	rarahghw	FLEXTRONICS	FLEX - DOUMEN	*** Notes added on 0...	security_partner_doc...	
STD-MSS-1	Standard Template for...	09/24/2018 18:28:23	Accepted	haogu	FLEXTRONICS	FLEX - DOUMEN	*** Notes added on 0...	security_partner_doc...	

View the controls and download the document for easier viewing if needed.

View all controls.

Use drop-down to export for easier review if desired.

Domain	Sub Domain	Control Number	Requirement	Audit Guidelines	Exception
Security Governance	Governance and Information Security ...	1.1.1	Supplier must develop and disseminate a security program th...	1. Verify if there is program document...	
Security Governance	Governance and Information Security ...	1.1.2	Supplier must review and update their information security pr...	1. Perform inquiry about the informat...	
Security Governance	Governance and Information Security ...	1.1.3	Supplier must identify roles and responsibilities within the Su...	1. Perform inquiry or verify if a team /...	
Security Governance		1.2.1	Supplier must develop policies, standards or procedures that ...	1. Verify if policies, standards...	
Security Governance		1.3.1	Supplier must prioritize and mitigate those risks which could L...	1. Perform inquiry or verify if...	
Security Governance	Security Risk Management	1.3.2	Supplier must monitor changes to the threat landscape perio...	1. Perform inquiry or verify if...	
Security Governance	Security Risk Management	1.3.3	Supplier must develop, document and follow a risk managem...	1. Perform inquiry or verify if...	
Security Governance	Security Compliance Management	1.4.1	Supplier must conduct self-assessments of their compliance ...	1. Perform inquiry or verify if a proces...	
Security Governance	Security Compliance Management	1.4.2	Supplier must develop and implement a plan of action to corr...	1. Verify if management action plan h...	
Security in Manufacturing and Oper...	Tracking and Accountability	2.1.1	Supplier must account for all items containing Cisco IP in any...	1. Perform inquiry or verify if a proces...	
Security in Manufacturing and Oper...	Security in Inventory Management	2.2.1	Supplier must conduct cycle counts as per the following sche...	1. Verify records of cycle counts as p...	

Once you are ready, you can return to the main screen to "Acknowledge" the document.

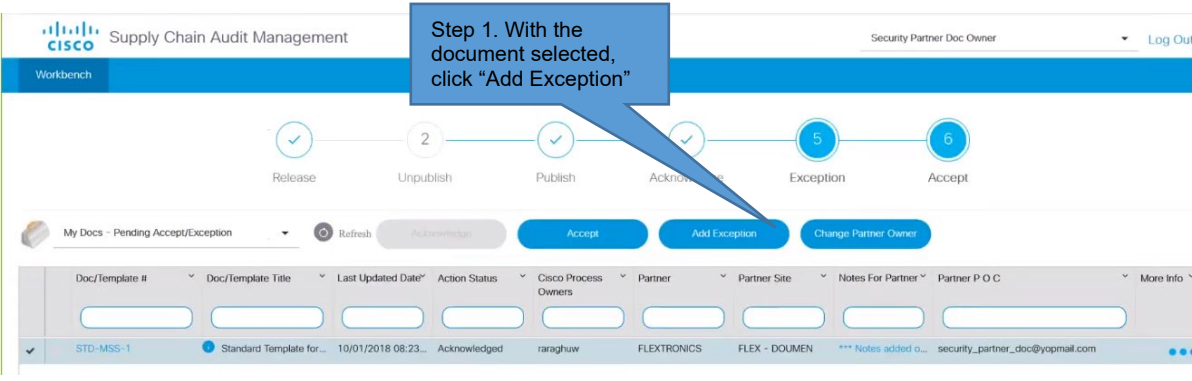
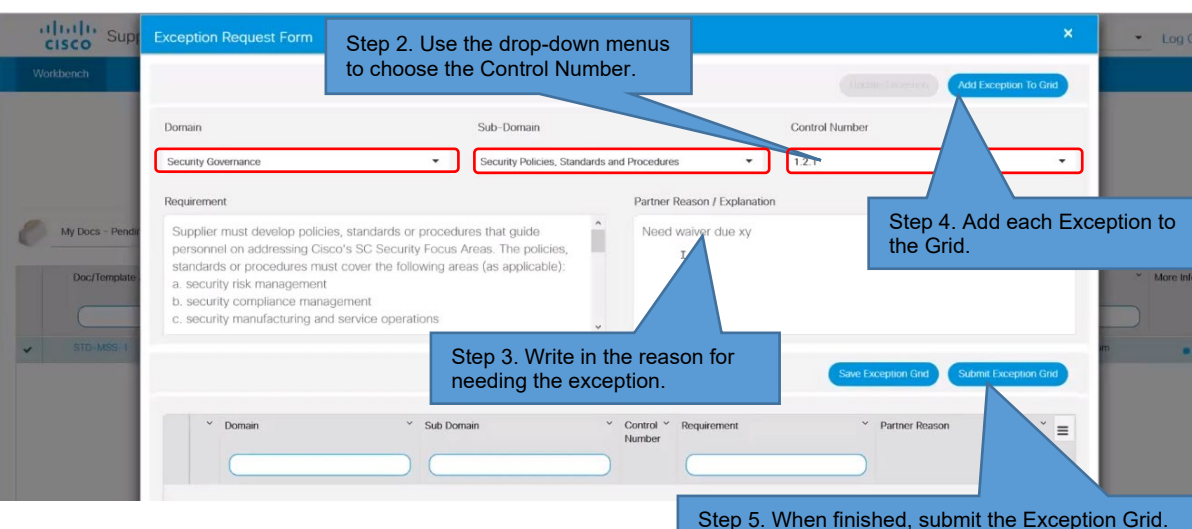
Step 5. Click "Acknowledge".

View document notes from Cisco.

Doc/Template #	Doc/Template Title	Last Updated Date	Action Status	Cisco Process Owner	Partner	Partner Site	Notes For Partner	Partner P O C	More Info
STD-MSS-1	Standard Template for...	10/01/2018 08:20:46	Published To Partner	rarahghw	FLEXTRONICS	FLEX - DOUMEN	*** Notes added on 1...		
STD-MSS-2	Standard Template for...	09/25/2018 12:09:03	Accepted	rarahghw	FLEXTRONICS	FLEX - DOUMEN	*** Notes added on 0...	security_partner_doc...	
STD-MSS-1	Standard Template for...	09/24/2018 18:28:23	Accepted	haogu	FLEXTRONICS	FLEX - DOUMEN	*** Notes added on 0...	security_partner_doc...	

The next step in the process will be to Accept the Audit or to Submit an Exception to it. If you have no Exceptions to enter, skip that step and proceed to "Accepting the Self-Assessment".

Submitting An Exception

Description	Steps & Screenshot
<p>If you need an exception to any of the controls, you can request "Add Exception".</p> <p>Shown here are steps to submit an exception.</p>	 <p>Step 1. With the document selected, click "Add Exception"</p>
<p>Enter the details on the Control number(s) you need Exceptions for & provide the reason(s) why.</p> <p>A pop-up menu will confirm, once you submit.</p>	 <p>Step 2. Use the drop-down menus to choose the Control Number.</p> <p>Step 3. Write in the reason for needing the exception.</p> <p>Step 4. Add each Exception to the Grid.</p> <p>Step 5. When finished, submit the Exception Grid.</p>

Accepting the Self-Assessment

Description	Steps & Screenshot
<p>Once Exception submission has been approved by Cisco, you will "Accept" the assessment & proceed with performing the Audit</p> <p>A confirmation message will appear. Click "OK"</p>	<p>Step 2. Click "Accept".</p> <p>Note: You can delegate to another person within your organization to perform the audit</p> <p>Step 1. Make sure you have the correct document selected for submission.</p>

Completing and Submitting an Audit for Approval

Description	Steps & Screenshot
<p>Entry Screen</p> <p>The audit itself will be completed by the Security Partner Audit Owner.</p> <p>This can be the same person as the one who acknowledged and/ or accepted the document if they had previously requested the Security Partner Audit Owner Role.</p>	<p>Step 2. Select "Audit Results/ Actions"</p> <p>Note: This is done from the Security Partner Audit Owner role.</p> <p>Step 1. Select/ highlight the audit document to complete.</p>

Go through and perform each controls listed.

Supply Chain Audit Management

Workbench

Security Partner Audit Owner Log Out

← Back Audit Action →

Audit # MSS-395 Audit Plan Name: STD-MSS-1-FLEXTRONICS-FLEX - DOUMEN

To take action, please select the question from

Pass
Fail - Create GAP
N/A

Step 4. Select Pass, Fail – Create GAP, or N/A from the drop-down menu.

Step 3. Select the control to respond to.

Note: For easier viewing, you may download the information into Excel.

Note: To view the full description, hover over the control number.

Completing a “Fail” for a control

Include your documentation and comments for each question. For a “Fail” designation, create a GAP as shown.

Workbench

← Back WHY - GAP WHAT - RCA/Mitigation Plan HOW - Upload Evidence

WHY - GAP

Requirement Details

Domain Security Governance Sub-domain Security Risk Management Control# 1.3.1

Requirement Supplier must prioritize and mitigate those risks ... Audit Guidelines 1. Perform inquiry or verify if a process exi... Exception

Enter GAP Details

GAP Title Failed due to xyz GAP Status Creation Date 10-01-2018

GAP Description Failed due to xyz

Comments for Approver Need your approval on the GAP

Step 1. Enter the GAP Title, Description and Comments for Approver in the WHY section.

Complete the details on WHAT the GAP is.

Most Visited Getting Started Audit Management

Failed due to xyz Need your approval on the GAP

WHAT - RCA/Mitigation Plan

Enter RCA/Mitigation Plan/Remediation

Risk no risk to Cisco ops

Root Cause internal flex network issue

Mitigation Plan We will replace xyz by Qz

Suggested Remediation

Step 2. Enter the Risk, Root Cause, Mitigation Plan, and Suggested Remediation in the WHAT section.

HOW - Upload Evidence

Save Cancel

In the HOW section, upload your evidence and save your work. A pop-up message will confirm.

Submitting to Cisco for Approval

Submit individual items for approval, once they are complete.

Domain	Sub Domain	Control Number	Requirement	Audit Guidelines	Audit Result	Result Status	Exception
Security Governance	Security Risk Management	1.3.1	Supplier must prioritize and mitigat...	1. Perform inquiry or verify if a proc...	Fail	Created	
Security Governance	Governance and Information Securi...	1.1.3	Supplier must identify roles and res...	1. Perform inquiry or verify if a team...	N/A	Created	
Security Governance	Security Compliance Management	1.4.1	Supplier must conduct self-assess...	1. Perform inquiry or verify if a proc...	Pass	Created	
Security Governance	Governance and Information Securi...	1.1.1	Supplier must develop and dissemi...	1. Verify if there is program docum...	Pass	Approved	
Security Governance	Governance and Information Securi...	1.1.2	Supplier must review and update th...	1. Perform inquiry about the inform...	Fail	Approved	
Security Governance	Security Policies, Standards and Pr...	1.2.1	Supplier must develop policies, sta...	1. Verify if policies, standards and p...			19
Security Governance	Security Risk Management	1.3.2	Supplier must monitor changes to L...	1. Perform inquiry or verify if a proc...			
Security Governance	Security Risk Management	1.3.3	Supplier must develop, document a...	1. Perform inquiry or verify if a proc...			
Security Governance	Security Compliance Management	1.4.2	Supplier must develop and implem...	1. Verify if management action plan...			
3rd Tier Partner Security	Security during Contract Initiation	11.1.1	Supplier must ensure that their sup...	1. Perform inquiry or verify if a proc...			
3rd Tier Partner Security	Security during Contract Initiation	11.1.2	When procuring products or servic...	1. Perform inquiry or verify if a proc...			

A pop-up menu will confirm your submission.

Domain	Sub Domain	Control Number	Requirement	Audit Guidelines	Audit Result	Result Status	Exception
Security Governance	Governance and Information Securi...	1.1.3	Supplier must identify roles and res...	1. Perform inquiry or verify if a team...	N/A	Submitted for Cisco Approval	
Security Governance	Security Risk Management	1.3.1	Supplier must prioritize and mitigat...	1. Perform inquiry or verify if a proc...	Fail	Submitted for Cisco Approval	
Security Governance	Security Compliance Management	1.4.1	Supplier must conduct self-assess...	1. Perform inquiry or verify if a proc...		Submitted for Cisco Approval	
Security Governance	Governance and Information Securi...	1.1.1	Supplier must develop and dis...	1. Verify if there is program docum...		Approved	
Security Governance	Governance and Information Securi...	1.1.2	Supplier must review and upd...	1. Perform inquiry about the inform...		Approved	
Security Governance	Security Policies, Standards and Pr...	1.2.1	Supplier must develop policies	1. Verify if policies, standards and p...			198
Security Governance	Security Risk Management	1.3.2	Supplier must monitor changes to L...	1. Perform inquiry or verify if a proc...			
Security Governance	Security Risk Management	1.3.3	Supplier must develop, document a...	1. Perform inquiry or verify if a proc...			
Security Governance	Security Compliance Management	1.4.2	Supplier must develop and implem...	1. Verify if management action plan...			
3rd Tier Partner Security	Security during Contract Initiation	11.1.1	Supplier must ensure that their sup...	1. Perform inquiry or verify if a proc...			
3rd Tier Partner Security	Security during Contract Initiation	11.1.2	When procuring products or servic...	1. Perform inquiry or verify if a proc...			

Changing Partner Owner (optional step - only if needed)

Description

Entry Screen

If you need to pass responsibility for the audit to another qualified person at your company, you can click “Change Partner Owner” and then select and transfer the Action Owner status to another person.

Steps & Screenshot

The screenshot displays the 'Supply Chain Audit Management' interface. At the top, a progress bar shows the audit lifecycle: Plan Created (1), UnPublish (2), Schedule (3), Publish (4), Acknowledge (5), In Progress (6), and Closed (7). A 'Change Partner Owner' button is highlighted in the 'Audit Results/Actions' section. Below this is a table of audit documents.

Audit #	Audit Name	Last Update Date	Audit Status	Audit Owner	Action Owner	Supplier	Supplier Site	Audit Type
MSS-395	STD-MSS-1-FLEXTRONICS-FLEX - DOUMEN	10/01/2018 08:28:05	Published	haogu	security_partner_doc@yop...	FLEXTRONICS	FLEX - DOUMEN	SELF-ASSESSMENT
MSS-392	STD-MSS-1-FLEXTRONICS-FLEX - DOUMEN	09/25/2018 12:09:40	In Progress	raraghuw	security_partner_doc@yop...	FLEXTRONICS	FLEX - DOUMEN	SELF-ASSESSMENT
MSS-391	STD-MSS-1-FLEXTRONICS-FLEX - DOUMEN	09/25/2018 12:09:40	In Progress	haogu	security_partner_doc@yop...	FLEXTRONICS	FLEX - DOUMEN	SELF-ASSESSMENT

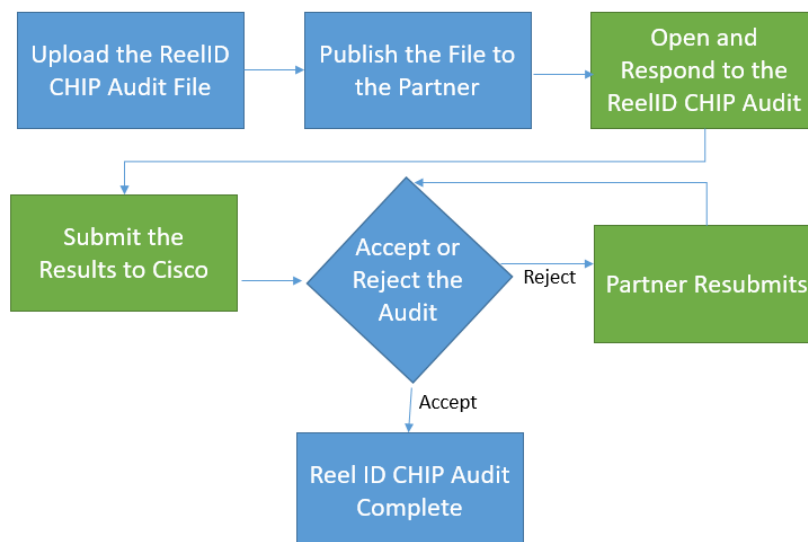
Step 1. Select/ highlight the audit document.

Step 2. Select “Change Partner Owner”

Note: This is done from the Security Partner Audit Owner role.

SC Security ReelID CHIP Audit Process Roles (Cisco & External)

The ReelID CHIP Audit Process is different than other Security Audits. Its purpose is to reconcile ACT2Chip usage at our Partner Sites. See the process flow below to see the steps in this process. (Cisco steps in Blue, Partner steps in Green).



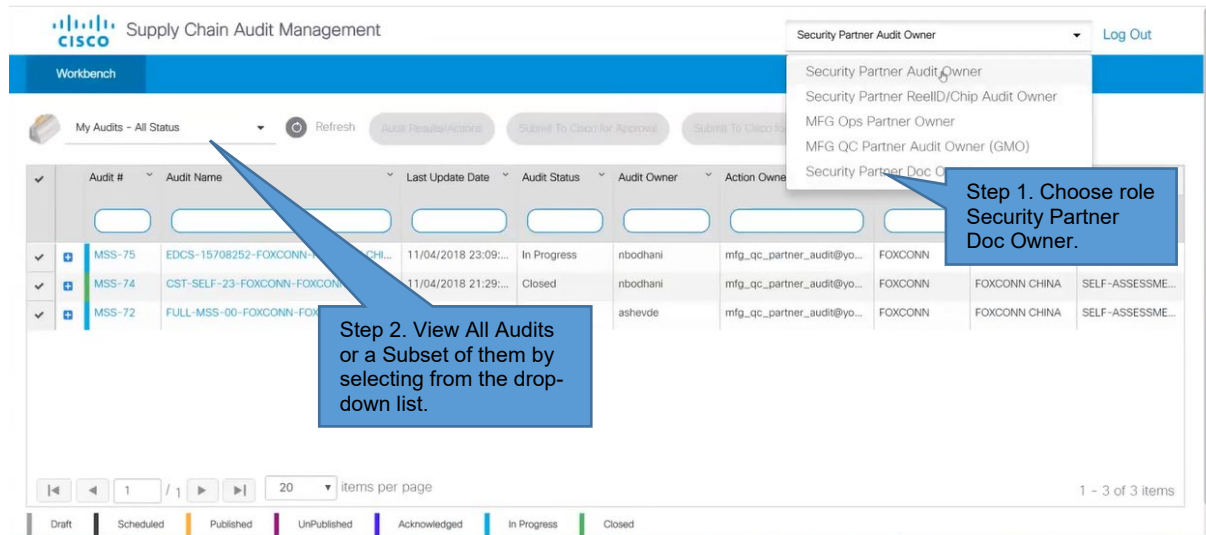
Responding to a Reel ID CHIP Audit

Description	Steps & Screenshot
	<p>The first step a partner takes in the Reel ID CHIP audit process is to respond to the Audit. The Partner will be notified of the audit via an email that will look like this:</p> <pre> ***** Title: ACTION REQUIRED – Cisco Security Self-Assessment Audit (AUTO FILL IN DOC # From: no-reply-sc-audit-notification@cisco.com Date: AUTO FILL IN Hello: There is a REEL Tracking Action required of you by NAME HERE to reconcile the usage of ACT-2 chips at your site. To take action, please click here . Thank you. ***** </pre> <p>The Partner will first need to log in (steps above). The audit owner can easily be changed in the system by selecting the audit and clicking the “Change Partner Owner” button.</p>

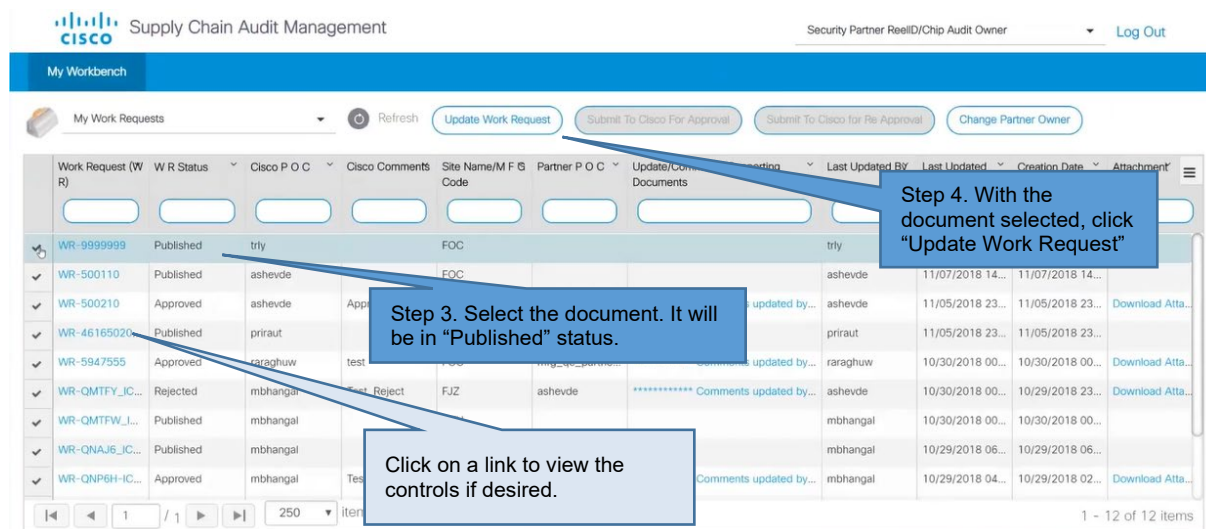
Entry Screen

Check your role.

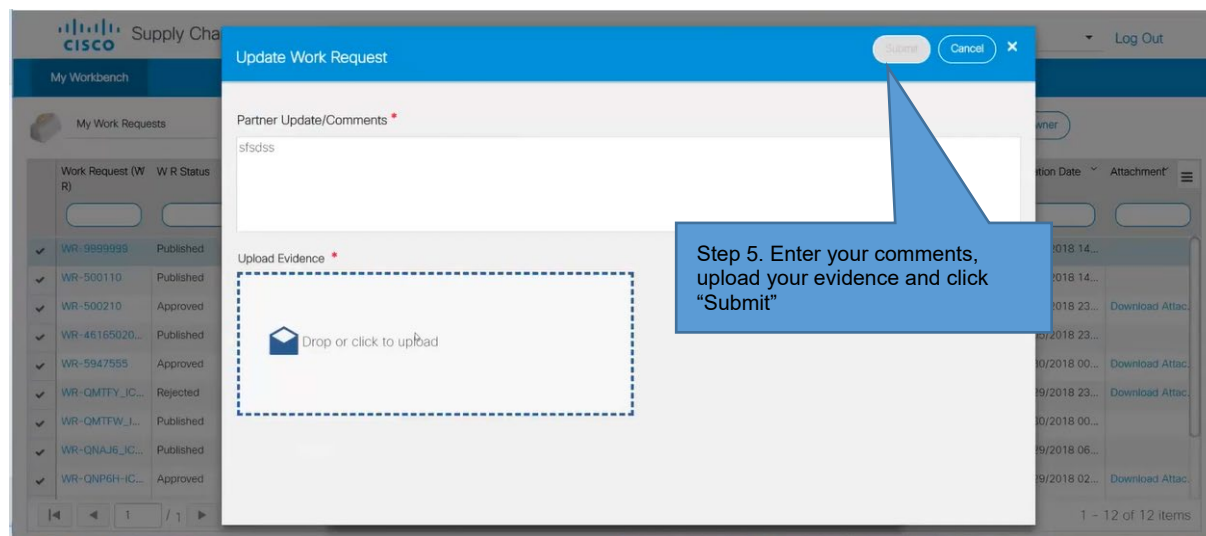
Only the roles you have access to will show in the drop-down box.



Select the document and view the controls if needed.

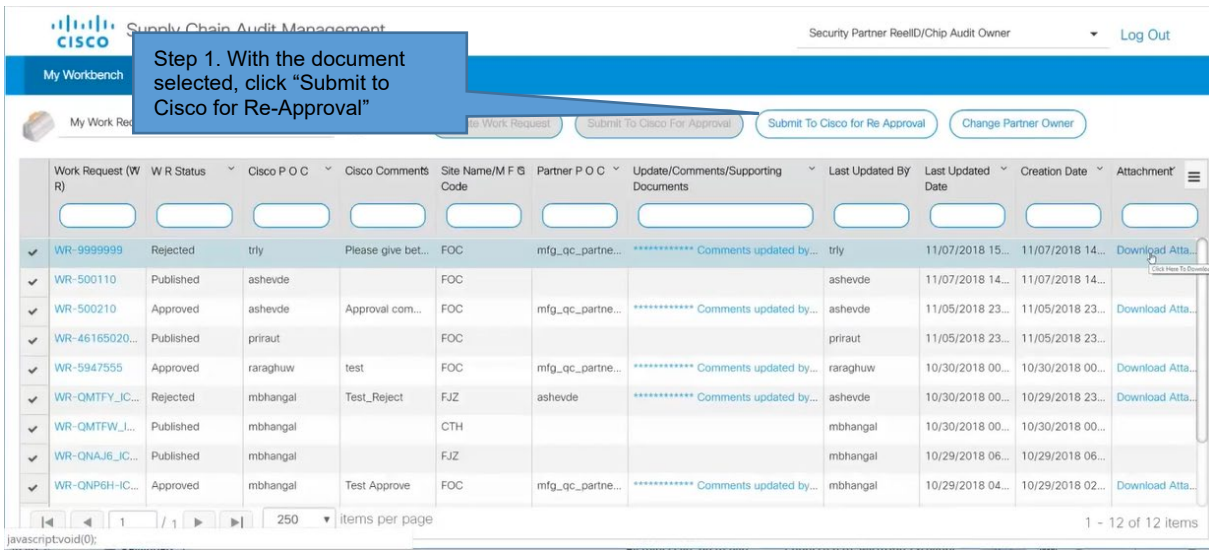
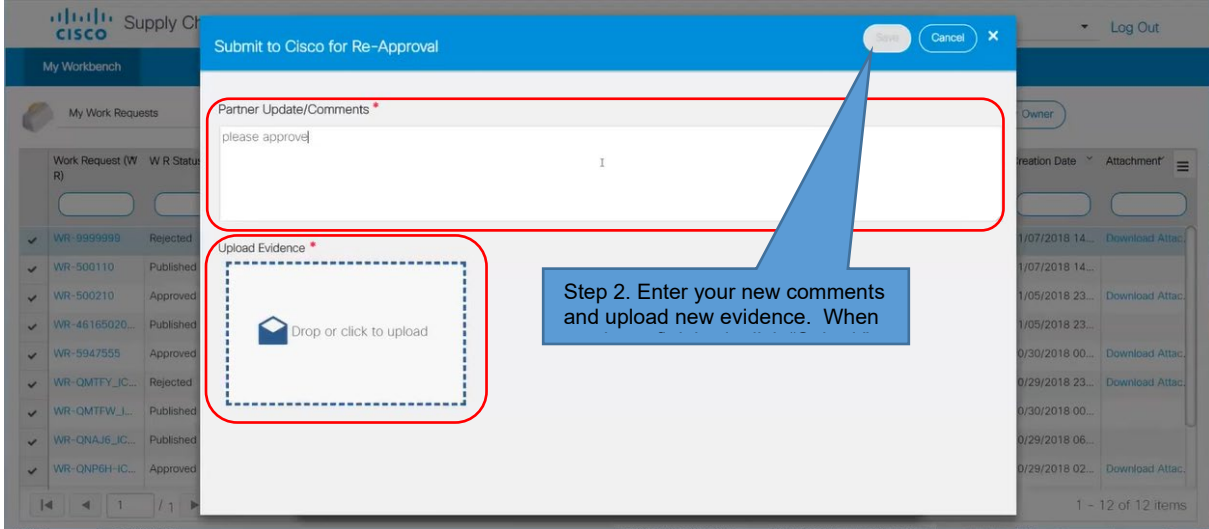


Enter comments and upload evidence before Submitting back to Cisco. If your audit is accepted by Cisco, this will be the final step. If it is not accepted, the audit will be returned to you and you should "re-submit" the audit per the instructions below.



Note – there are no exceptions to a ReelID CHIP Audit.

Resubmitting a Reel ID CHIP Audit after a Rejection

Description	Steps & Screenshot																																																																																																														
<p>If your Audit has been rejected by Cisco, you will need to resubmit it, with new comments and evidence.</p>	 <p>Step 1. With the document selected, click "Submit to Cisco for Re-Approval"</p> <table border="1"> <thead> <tr> <th>Work Request (WR)</th> <th>WR Status</th> <th>Cisco P O C</th> <th>Cisco Comments</th> <th>Site Name/M F S Code</th> <th>Partner P O C</th> <th>Update/Comments/Supporting Documents</th> <th>Last Updated By</th> <th>Last Updated Date</th> <th>Creation Date</th> <th>Attachment</th> </tr> </thead> <tbody> <tr> <td>WR-9999999</td> <td>Rejected</td> <td>trly</td> <td>Please give bet...</td> <td>FOC</td> <td>mfg_qc_partne...</td> <td>***** Comments updated by...</td> <td>trly</td> <td>11/07/2018 15...</td> <td>11/07/2018 14...</td> <td>Download Atta...</td> </tr> <tr> <td>WR-500110</td> <td>Published</td> <td>ashevde</td> <td>Approval com...</td> <td>FOC</td> <td>mfg_qc_partne...</td> <td>***** Comments updated by...</td> <td>ashevde</td> <td>11/07/2018 14...</td> <td>11/07/2018 14...</td> <td>Download Atta...</td> </tr> <tr> <td>WR-500210</td> <td>Approved</td> <td>ashevde</td> <td>Approval com...</td> <td>FOC</td> <td>mfg_qc_partne...</td> <td>***** Comments updated by...</td> <td>ashevde</td> <td>11/05/2018 23...</td> <td>11/05/2018 23...</td> <td>Download Atta...</td> </tr> <tr> <td>WR-46165020...</td> <td>Published</td> <td>priraut</td> <td>Approval com...</td> <td>FOC</td> <td>mfg_qc_partne...</td> <td>***** Comments updated by...</td> <td>priraut</td> <td>11/05/2018 23...</td> <td>11/05/2018 23...</td> <td>Download Atta...</td> </tr> <tr> <td>WR-5947555</td> <td>Approved</td> <td>rarahuw</td> <td>test</td> <td>FOC</td> <td>mfg_qc_partne...</td> <td>***** Comments updated by...</td> <td>rarahuw</td> <td>10/30/2018 00...</td> <td>10/30/2018 00...</td> <td>Download Atta...</td> </tr> <tr> <td>WR-QMTFY_IC...</td> <td>Rejected</td> <td>mbhangal</td> <td>Test_Reject</td> <td>FJZ</td> <td>ashevde</td> <td>***** Comments updated by...</td> <td>ashevde</td> <td>10/30/2018 00...</td> <td>10/29/2018 23...</td> <td>Download Atta...</td> </tr> <tr> <td>WR-QMTFW_L...</td> <td>Published</td> <td>mbhangal</td> <td>Approval com...</td> <td>CTH</td> <td>ashevde</td> <td>***** Comments updated by...</td> <td>mbhangal</td> <td>10/30/2018 00...</td> <td>10/30/2018 00...</td> <td>Download Atta...</td> </tr> <tr> <td>WR-QNAJ6_IC...</td> <td>Published</td> <td>mbhangal</td> <td>Approval com...</td> <td>FJZ</td> <td>ashevde</td> <td>***** Comments updated by...</td> <td>mbhangal</td> <td>10/29/2018 06...</td> <td>10/29/2018 06...</td> <td>Download Atta...</td> </tr> <tr> <td>WR-QNP6H-IC...</td> <td>Approved</td> <td>mbhangal</td> <td>Test Approve</td> <td>FOC</td> <td>mfg_qc_partne...</td> <td>***** Comments updated by...</td> <td>mbhangal</td> <td>10/29/2018 04...</td> <td>10/29/2018 02...</td> <td>Download Atta...</td> </tr> </tbody> </table>	Work Request (WR)	WR Status	Cisco P O C	Cisco Comments	Site Name/M F S Code	Partner P O C	Update/Comments/Supporting Documents	Last Updated By	Last Updated Date	Creation Date	Attachment	WR-9999999	Rejected	trly	Please give bet...	FOC	mfg_qc_partne...	***** Comments updated by...	trly	11/07/2018 15...	11/07/2018 14...	Download Atta...	WR-500110	Published	ashevde	Approval com...	FOC	mfg_qc_partne...	***** Comments updated by...	ashevde	11/07/2018 14...	11/07/2018 14...	Download Atta...	WR-500210	Approved	ashevde	Approval com...	FOC	mfg_qc_partne...	***** Comments updated by...	ashevde	11/05/2018 23...	11/05/2018 23...	Download Atta...	WR-46165020...	Published	priraut	Approval com...	FOC	mfg_qc_partne...	***** Comments updated by...	priraut	11/05/2018 23...	11/05/2018 23...	Download Atta...	WR-5947555	Approved	rarahuw	test	FOC	mfg_qc_partne...	***** Comments updated by...	rarahuw	10/30/2018 00...	10/30/2018 00...	Download Atta...	WR-QMTFY_IC...	Rejected	mbhangal	Test_Reject	FJZ	ashevde	***** Comments updated by...	ashevde	10/30/2018 00...	10/29/2018 23...	Download Atta...	WR-QMTFW_L...	Published	mbhangal	Approval com...	CTH	ashevde	***** Comments updated by...	mbhangal	10/30/2018 00...	10/30/2018 00...	Download Atta...	WR-QNAJ6_IC...	Published	mbhangal	Approval com...	FJZ	ashevde	***** Comments updated by...	mbhangal	10/29/2018 06...	10/29/2018 06...	Download Atta...	WR-QNP6H-IC...	Approved	mbhangal	Test Approve	FOC	mfg_qc_partne...	***** Comments updated by...	mbhangal	10/29/2018 04...	10/29/2018 02...	Download Atta...
Work Request (WR)	WR Status	Cisco P O C	Cisco Comments	Site Name/M F S Code	Partner P O C	Update/Comments/Supporting Documents	Last Updated By	Last Updated Date	Creation Date	Attachment																																																																																																					
WR-9999999	Rejected	trly	Please give bet...	FOC	mfg_qc_partne...	***** Comments updated by...	trly	11/07/2018 15...	11/07/2018 14...	Download Atta...																																																																																																					
WR-500110	Published	ashevde	Approval com...	FOC	mfg_qc_partne...	***** Comments updated by...	ashevde	11/07/2018 14...	11/07/2018 14...	Download Atta...																																																																																																					
WR-500210	Approved	ashevde	Approval com...	FOC	mfg_qc_partne...	***** Comments updated by...	ashevde	11/05/2018 23...	11/05/2018 23...	Download Atta...																																																																																																					
WR-46165020...	Published	priraut	Approval com...	FOC	mfg_qc_partne...	***** Comments updated by...	priraut	11/05/2018 23...	11/05/2018 23...	Download Atta...																																																																																																					
WR-5947555	Approved	rarahuw	test	FOC	mfg_qc_partne...	***** Comments updated by...	rarahuw	10/30/2018 00...	10/30/2018 00...	Download Atta...																																																																																																					
WR-QMTFY_IC...	Rejected	mbhangal	Test_Reject	FJZ	ashevde	***** Comments updated by...	ashevde	10/30/2018 00...	10/29/2018 23...	Download Atta...																																																																																																					
WR-QMTFW_L...	Published	mbhangal	Approval com...	CTH	ashevde	***** Comments updated by...	mbhangal	10/30/2018 00...	10/30/2018 00...	Download Atta...																																																																																																					
WR-QNAJ6_IC...	Published	mbhangal	Approval com...	FJZ	ashevde	***** Comments updated by...	mbhangal	10/29/2018 06...	10/29/2018 06...	Download Atta...																																																																																																					
WR-QNP6H-IC...	Approved	mbhangal	Test Approve	FOC	mfg_qc_partne...	***** Comments updated by...	mbhangal	10/29/2018 04...	10/29/2018 02...	Download Atta...																																																																																																					
<p>Enter your new comments and evidence. When you click "Submit", your document will be re-submitted.</p>	 <p>Step 2. Enter your new comments and upload new evidence. When</p>																																																																																																														