

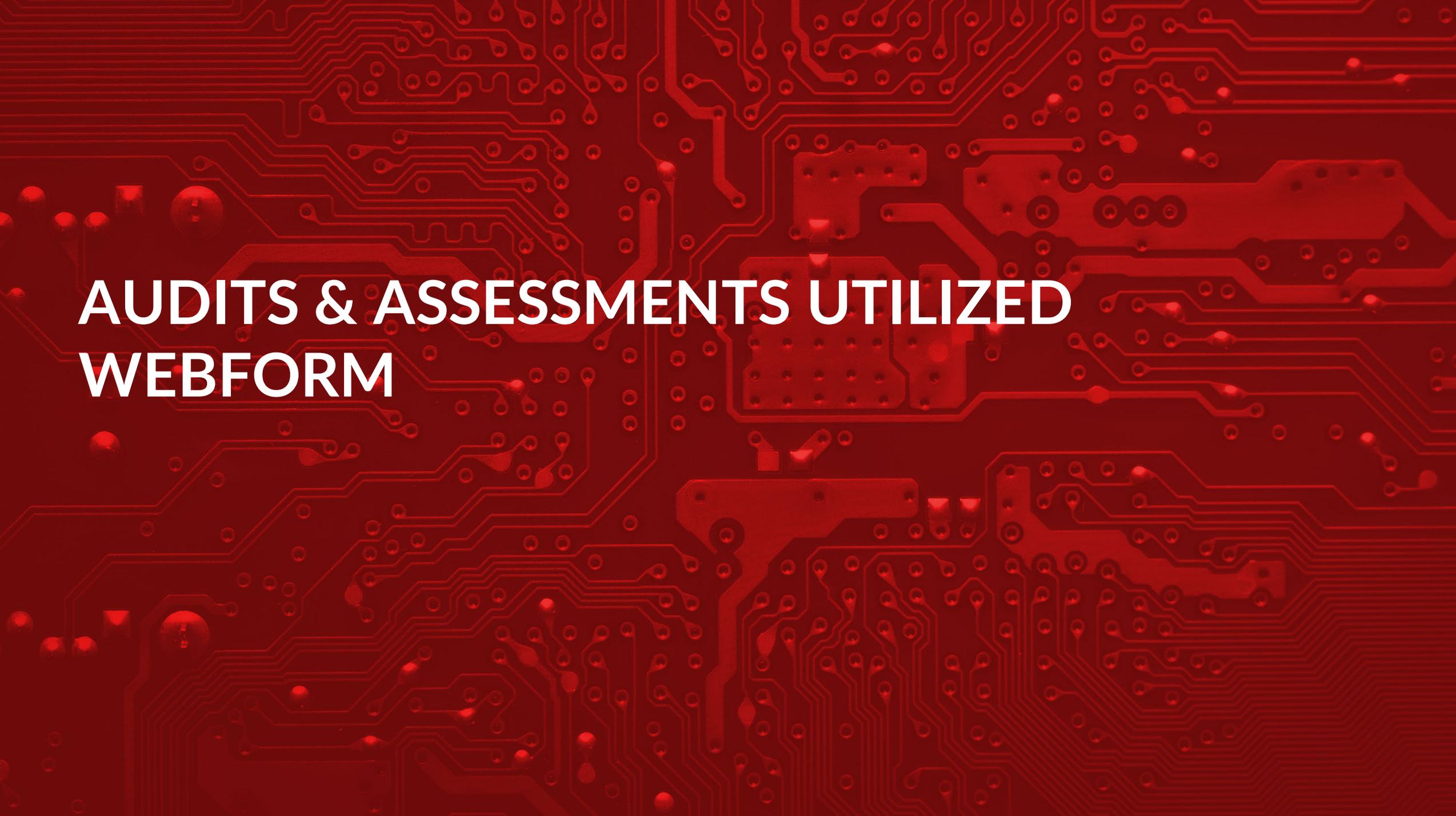


AUDITS & ASSESSMENTS UTILIZED

Instructions for the Completion of the Audits & Assessments Utilized Webform

Table of Contents

- **Summary:** Audits & Assessments Utilized Webform
- **Instructions:** How to complete the Audits & Assessments Utilized Webform when inheritance is applied
- **Instructions:** How to complete the Audits & Assessments Utilized Webform when relying on third-party audits and assessment



AUDITS & ASSESSMENTS UTILIZED WEBFORM

Summary: Audits & Assessments Utilized Webform

The Audits and Assessments Utilized webform is a table showing where reliance was placed on third-party reports and external inheritance was utilized.

- When external inheritance is utilized, the inherited report will automatically be added to the table and the Assessed Entity or External Assessor will complete all required fields that are not automatically populated.
- For third party reports, the Assessed Entity or External Assessor must tag the report as an attestation report issued by a third party for the reports to be added to the table. Then, the Assessed Entity or External Assessor will complete all required fields that are not automatically populated.

Assessment Utilized	Assessed Organization	Report Type	Report Date	Utilization Approach	Platforms	Location/Facilities	Assessment Domains
2021 Assurance Test - Data Center Assessment	XYZ Colocations	v9.3 VALIDATED	07/27/2021	Inheritance	PLATFORMS	FACILITIES	18 Physical & Environmental Security
SOC 2	XYZ Colocations	Period-of-ti	The assessment report's issuance date 06/03/2021	Reliance	PLATFORMS	FACILITIES	18 Physical & Environmental Security
			The assessment report's audit period start date *				
			10/01/2020				
			The assessment report's audit period end date *				
			04/30/2021				

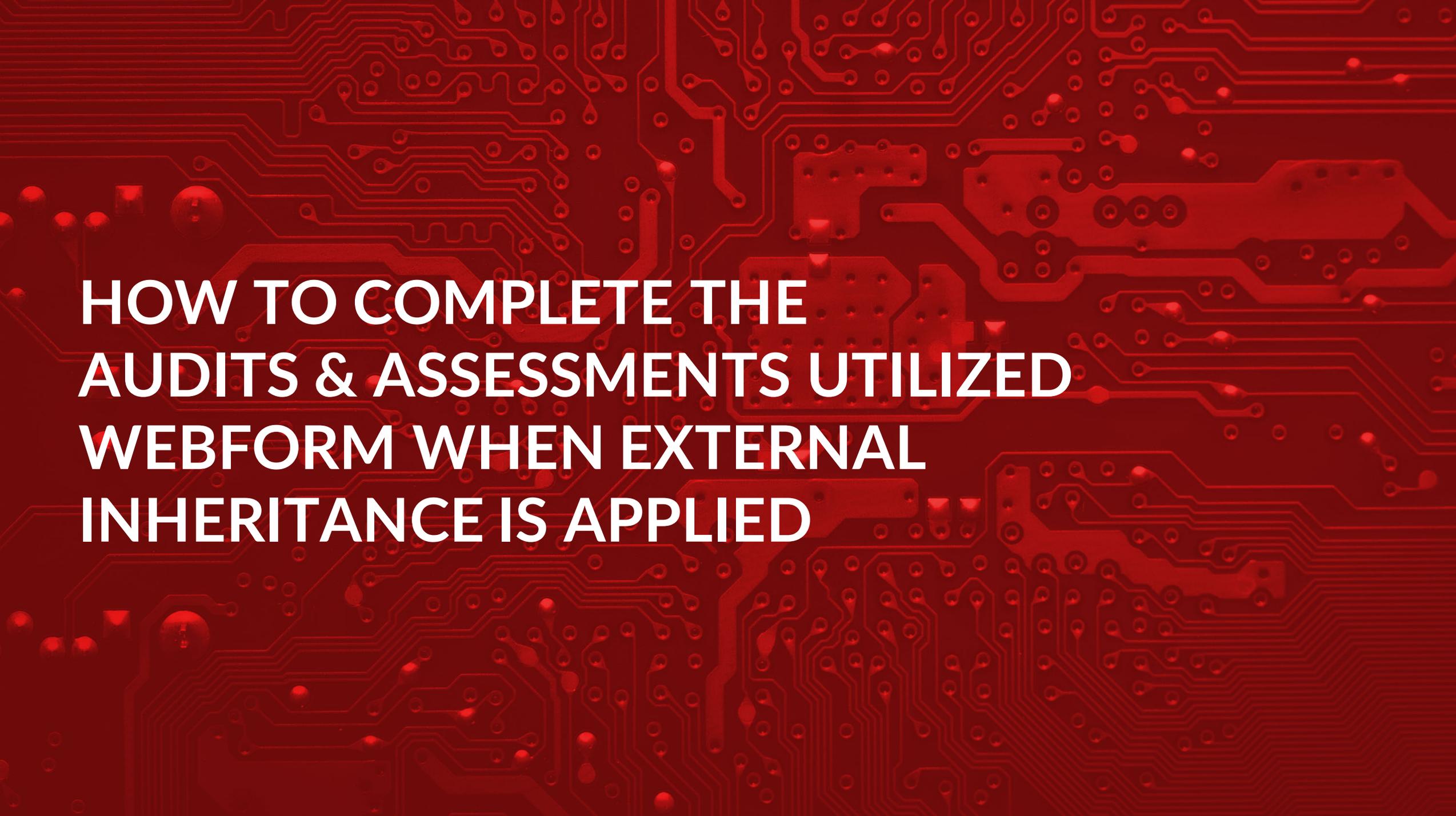
Summary: Audits & Assessments Utilized Webform

If external inheritance is not utilized and reliance is not placed on any third-party reports, the Audits and Assessments Utilized table will display a check box labeled “None Utilized”. The External Assessor should check this box to indicate that no audits or assessments have been inherited from or relied upon.

Audits and Assessments Utilized

Assessment Utilized 	Assessed Organization 	Report Type 	Report Date 	Utilization Approach 	Platforms 	Location/Facilities 	Assessment Domains 
<input checked="" type="checkbox"/> None Utilized							

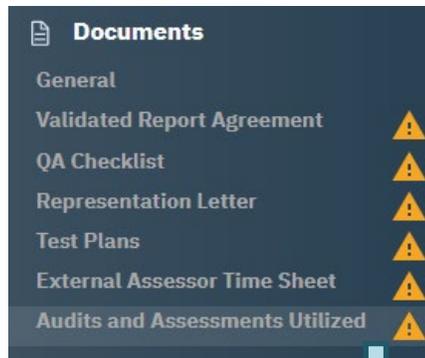
SAVE

The background of the image is a complex, glowing red circuit board pattern. It features a dense network of lines, nodes, and circular components, resembling a printed circuit board (PCB) or a microchip layout. The overall aesthetic is high-tech and digital.

HOW TO COMPLETE THE AUDITS & ASSESSMENTS UTILIZED WEBFORM WHEN EXTERNAL INHERITANCE IS APPLIED

Instructions: How to complete the Audits & Assessments Utilized Webform when external inheritance is applied

Step 1 – The External Assessor or Assessed Entity should access the assessment in MyCSF and navigate to the Audits and Assessments Utilized webform by clicking *Audits and Assessments Utilized* on the left sidebar.



After external inheritance has been applied to the assessment by the Assessed Entity, the Audits and Assessments Utilized webform will be automatically populated with the following information:

- Name of the inherited assessment
- Report Type
- Report Date
- Utilization Approach (Inheritance)
- Assessment Domain(s) containing requirement statement scoring that were inherited from this assessment

Audits and Assessments Utilized

Assessment Utilized	Assessed Organization	Report Type	Report Date	Utilization Approach	Platforms	Location/Facilities	Assessment Domains
2021 Assurance Test - Data Center Assessment	<input type="text" value="Enter Organization..."/>	v9.3 VALIDATED	07/27/2021	Inheritance	<input type="button" value="PLATFORMS"/>	<input type="button" value="FACILITIES"/>	18 Physical & Environmental Security

Instructions: How to complete the Audits & Assessments Utilized Webform when external inheritance is applied

Step 2 – The External Assessor or Assessed Entity should complete the remaining fields:

- Assessed Organization
- Platforms
- Locations/Facilities

Audits and Assessments Utilized

Assessment Utilized 	Assessed Organization 	Report Type 	Report Date 	Utilization Approach 	Platforms 	Location/Facilities 	Assessment Domains 
2021 Assurance Test - Data Center Assessment	<input type="text" value="Enter Organization..."/>	v9.3 VALIDATED	07/27/2021	Inheritance	<input type="text" value="PLATFORMS"/>	<input type="text" value="FACILITIES"/>	18 Physical & Environmental Security

Step 2a – The Assessed Organization field should contain the name of the organization that was assessed for the assessment mentioned in the Assessment Utilized field.

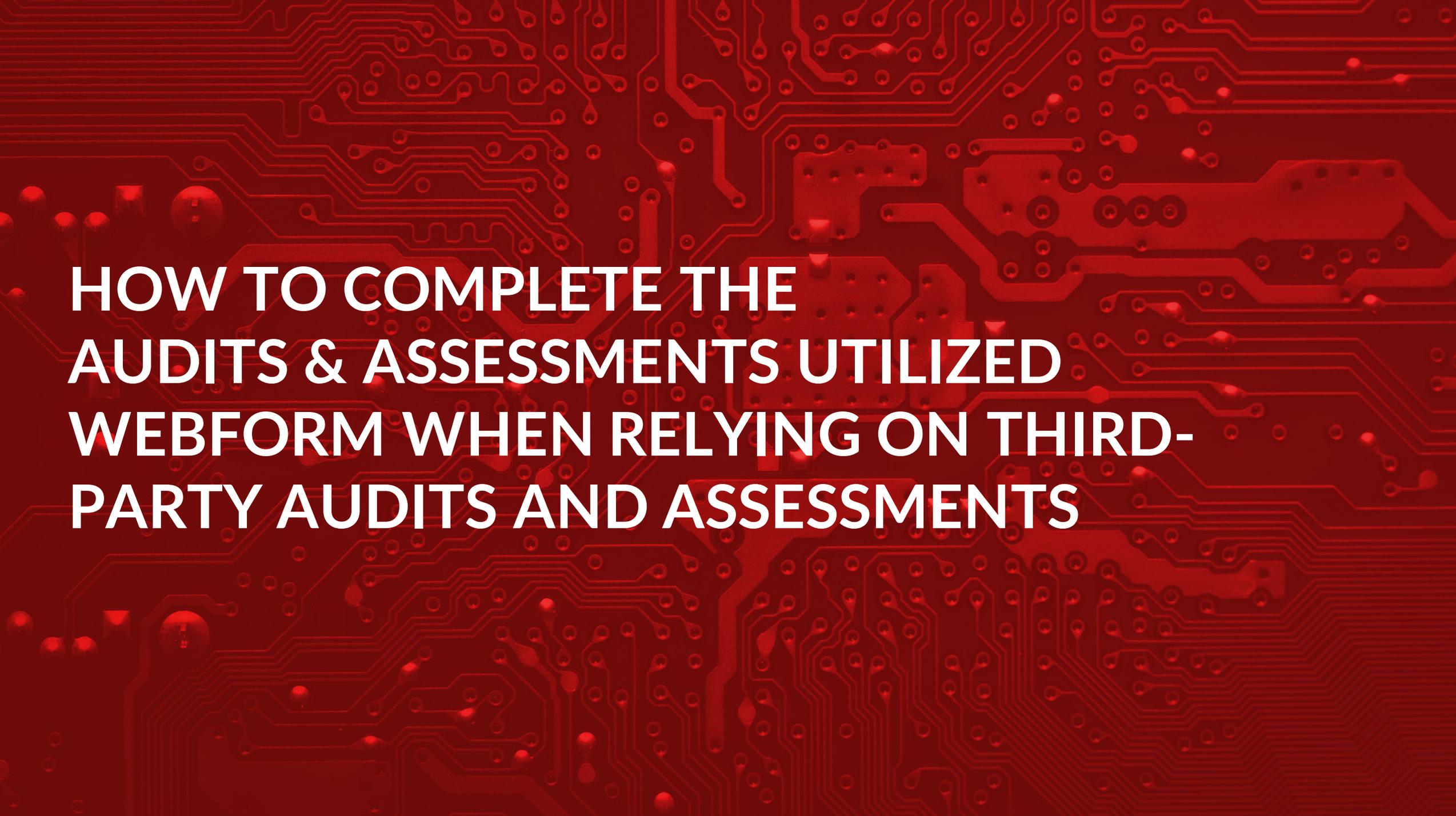
Instructions: How to complete the Audits & Assessments Utilized Webform when external inheritance is applied

Step 2b – The External Assessor or Assessed Entity should select the platforms that are relevant to the assessment utilized. The options listed will be the platforms/systems that were entered on the Scope of the Assessment page.

Assessment Utilized ¹	Assessed Organization ¹	Report Type ¹	Report Date ¹	Utilization Approach ¹	Platforms ¹	Location/Facilities ¹	Assessment Domains ¹
2021 Assurance Test - Data Center Assessment	XYZ Colocations	v9.3 VALIDATED	07/27/2021	Inheritance	PLATFORMS ▾ <input type="checkbox"/> Platform ABC	FACILITIES ▾	18 Physical & Environmental Security

Step 2c – The External Assessor or Assessed Entity should select the facilities that are relevant to the assessment utilized. The options listed will be the facilities that were entered on the Scope of the Assessment page.

Assessment Utilized ¹	Assessed Organization ¹	Report Type ¹	Report Date ¹	Utilization Approach ¹	Platforms ¹	Location/Facilities ¹	Assessment Domains ¹
2021 Assurance Test - Data Center Assessment	XYZ Colocations	v9.3 VALIDATED	07/27/2021	Inheritance	PLATFORMS ▾	FACILITIES ▾ <input type="checkbox"/> Data Center 123	18 Physical & Environmental Security

The background of the image is a complex, repeating pattern of red circuit board traces and components, creating a digital and technological aesthetic. The lines and shapes are intricate and vary in size, filling the entire frame.

HOW TO COMPLETE THE AUDITS & ASSESSMENTS UTILIZED WEBFORM WHEN RELYING ON THIRD- PARTY AUDITS AND ASSESSMENTS

Instructions: How to complete the Audits & Assessments Utilized Webform when relying on third-party audits and assessments

Step 1 – Enter the Document Name and check the box labeled “Is this an attestation report issued by a third party?”

When adding an attestation report issued by a third party to the document repository, whether the document is being uploaded or only the document name is being linked, the External Assessor or Assessed Entity should follow these steps:

The screenshot displays the 'External Assessor Documents' webform. On the left, a dark sidebar menu is visible with the following items: 'Documents', 'General', 'Validated Report Agreement', 'QA Checklist', 'Representation Letter', 'Test Plans', 'External Assessor Time Sheet', and 'Audits and Assessments Utilized'. The 'Audits and Assessments Utilized' item is highlighted in blue, and a blue arrow points from it to the main form area. The main form area is titled 'External Assessor Documents' and has three tabs: 'All', 'Subscriber 2', and 'External Assessor'. Below the tabs, there is a section titled 'Add a New External Assessor Document'. This section contains a text input field with 'SOC 2' entered, a 'Document Description' field, a 'CHOOSE A FILE' button, and a 'SAVE' button. Below these fields is a checkbox labeled 'Is this an attestation report issued by a third party?'. A blue arrow points from this checkbox to a second, identical form below it. In this second form, the checkbox is checked with a green checkmark. Below the checkbox, there are two required fields: 'Assessed Organization *' and 'Report Type *'. The 'Report Type *' field has three radio button options: 'Point-in-time assessment report (e.g. PCI DSS ROC, HITRUST CSF Validated Report without Certification)', 'Period-of-time assessment report (e.g. SOC 2 Type II)', and 'Future-looking assessment report (e.g. HITRUST CSF Validated Report with Certification, ISO 27001/2 Certification Report)'.

Instructions: How to complete the Audits & Assessments Utilized Webform when relying on third-party audits and assessments

Step 2 – Enter the name of the name of the organization that was assessed for the assessment being added to the repository.

Step 3 – Select the Report Type from the options:

- Point-in-time assessment report (e.g. PCI DSS ROC, HITRUST Validated Report without Certification)
- Period-of-time assessment report (e.g. SOC 2 Type II)
- Future-looking assessment report (e.g. HITRUST Validated Report with Certification, ISO 27001/2 Certification Report)

The screenshot shows a webform titled "External Assessor Documents". At the top, there are three tabs: "All", "Subscriber 2", and "External Assessor". Below the tabs is a section titled "Add a New External Assessor Document". This section contains several input fields and a list of report types. The "Document Description" field is empty. The "Assessed Organization" field is empty. The "Report Type" field has three radio button options: "Point-in-time assessment report", "Period-of-time assessment report", and "Future-looking assessment report". The "Future-looking assessment report" option is selected. There is a "CHOOSE A FILE" button and a "SAVE" button. A checkbox labeled "Is this an attestation report issued by a third party?" is checked.

External Assessor Documents

All Subscriber 2 External Assessor

Add a New External Assessor Document

SOC 2 Document Description

CHOOSE A FILE Or Drop a File Here. SAVE

Is this an attestation report issued by a third party?

Assessed Organization *

Report Type *

Point-in-time assessment report
(e.g. PCI DSS ROC, HITRUST CSF Validated Report without Certification)

Period-of-time assessment report
(e.g. SOC 2 Type II)

Future-looking assessment report
(e.g. HITRUST CSF Validated Report with Certification, ISO 27001/2 Certification Report)

Instructions: How to complete the Audits & Assessments Utilized Webform when relying on third-party audits and assessments

Step 4 – Enter the relevant report dates depending on the Report Type selected in Step 3. Then click *save*.

<p>Report Type *</p> <p><input checked="" type="radio"/> Point-in-time assessment report (e.g. PCI DSS ROC, HITRUST CSF Validated Report without Certification)</p> <p><input type="radio"/> Period-of-time assessment report (e.g. SOC 2 Type II)</p> <p><input type="radio"/> Future-looking assessment report (e.g. HITRUST CSF Validated Report with Certification, ISO 27001/2 Certification Report)</p>	<p>The assessment report's issuance date</p> <p>mm/dd/yyyy </p> <p>Date of the assessment's report *</p> <p>mm/dd/yyyy </p>
<p>Report Type *</p> <p><input type="radio"/> Point-in-time assessment report (e.g. PCI DSS ROC, HITRUST CSF Validated Report without Certification)</p> <p><input checked="" type="radio"/> Period-of-time assessment report (e.g. SOC 2 Type II)</p> <p><input type="radio"/> Future-looking assessment report (e.g. HITRUST CSF Validated Report with Certification, ISO 27001/2 Certification Report)</p>	<p>The assessment report's issuance date</p> <p>mm/dd/yyyy </p> <p>The assessment report's audit period start date *</p> <p>mm/dd/yyyy </p> <p>The assessment report's audit period end date *</p> <p>mm/dd/yyyy </p>
<p>Report Type *</p> <p><input type="radio"/> Point-in-time assessment report (e.g. PCI DSS ROC, HITRUST CSF Validated Report without Certification)</p> <p><input type="radio"/> Period-of-time assessment report (e.g. SOC 2 Type II)</p> <p><input checked="" type="radio"/> Future-looking assessment report (e.g. HITRUST CSF Validated Report with Certification, ISO 27001/2 Certification Report)</p>	<p>The assessment report's issuance date</p> <p>mm/dd/yyyy </p> <p>Date of the assessment's report *</p> <p>mm/dd/yyyy </p> <p>The assessment report's validity end date *</p> <p>mm/dd/yyyy </p>

Instructions: How to complete the Audits & Assessments Utilized Webform when relying on third-party audits and assessments

After the document has been identified as an attestation report issued by a third party, the Audits and Assessments Utilized webform will be automatically populated with the following information:

- Name of the assessment utilized
- Assessed Organization
- Report Type
- Report Dates
- Utilization Approach (Reliance)
- Assessment Domain(s) containing requirement statements for which the document has been linked



The screenshot shows a webform titled 'Audits and Assessments Utilized'. It has a header with several filter buttons: 'Assessment Utilized', 'Assessed Organization', 'Report Type', 'Report Date', 'Utilization Approach', 'Platforms', 'Location/Facilities', and 'Assessment Domains'. Below the header, the form is populated with the following information:

Assessment Utilized	Assessed Organization	Report Type	Report Date	Utilization Approach	Platforms	Location/Facilities	Assessment Domains
SOC 2	XYZ Colocations	Period-of-time	The assessment report's issuance date 06/03/2021	Reliance	PLATFORMS	FACILITIES	11 Access Control, 18 Physical & Environmental Security
			The assessment report's audit period start date *				
			10/01/2020				
			The assessment report's audit period end date *				
			04/30/2021				

Instructions: How to complete the Audits & Assessments Utilized Webform when relying on third-party audits and assessments

Note: To ensure that the Assessment Domains column is populated accurately, please be sure to only add the document to the document repository once and link that document to all relevant requirement statements across the assessment.

If the same document is added to the document repository multiple times, this will result in several instances of the same document within the Audits and Assessments Utilized table, each identifying the Assessment Domains in which the document was linked.

Audits and Assessments Utilized

Assessment Utilized	Assessed Organization	Report Type	Report Date	Utilization Approach	Platforms	Location/Facilities	Assessment Domains
SOC 2	XYZ Colocations	Period-of-time	The assessment report's issuance date 06/03/2021	Reliance	PLATFORMS	FACILITIES	11 Access Control, 18 Physical & Environmental Security
			The assessment report's audit period start date *				
			10/01/2020				
			The assessment report's audit period end date *				
			04/30/2021				

Instructions: How to complete the Audits & Assessments Utilized Webform when relying on third-party audits and assessments

Step 5 – After a document has been identified as an attestation report issued by a third party and has been linked to at least one requirement statement, the External Assessor or Assessed Entity should return to the Audits and Assessments Utilized webform to select the relevant Platforms and Facilities.

Step 5a – The External Assessor or Assessed Entity should select the platforms that are relevant to the assessment utilized. The options listed will be the platforms/systems that were entered on the Scope of the Assessment page.

SOC 2 XYZ Colocations Period-of-time The assessment report's issuance date Reliance PLATFORMS FACILITIES 11 Access Control, 18 Physical & Environmental Security

06/03/2021 The assessment report's

Platform ABC

Step 5b – The External Assessor or Assessed Entity should select the facilities that are relevant to the assessment utilized. The options listed will be the facilities that were entered on the Scope of the Assessment page.

SOC 2 XYZ Colocations Period-of-time The assessment report's issuance date Reliance PLATFORMS FACILITIES 11 Access Control, 18 Physical & Environmental Security

06/03/2021 The assessment report's

Data Center 123

Instructions: How to complete the Audits & Assessments Utilized Webform when relying on third-party audits and assessments

Note: To identify a previously added document as an attestation report issued by a third party, the group that uploaded the document (Assessed Entity or External Assessor) should:

- Click "...", then click *Edit*
- Check the box labeled "Is this an attestation report issued by a third party?"
- Enter the required information, then click *Update*

1 External Assessor Document

DOWNLOAD ALL...

All Subscriber 2 External Assessor 1

Add a New External Assessor Document

Document Name Document Description CHOOSE A FILE Or Drop a File Here. SAVE

Is this an attestation report issued by a third party?

SOC 2

LINKED STATEMENTS ...

Edit Delete

Edit Document

Name
SOC 2

Description
Document Description

CHOOSE A FILE Or Drop a File Here.

Is this an attestation report issued by a third party?

Assessed Organization *

Report Type *

Point-in-time assessment report
(e.g. PCI DSS ROC, HITRUST CSF Validated Report without Certification)

Period-of-time assessment report
(e.g. SOC 2 Type II)

Future-looking assessment report
(e.g. HITRUST CSF Validated Report with Certification, ISO 27001/2 Certification Report)

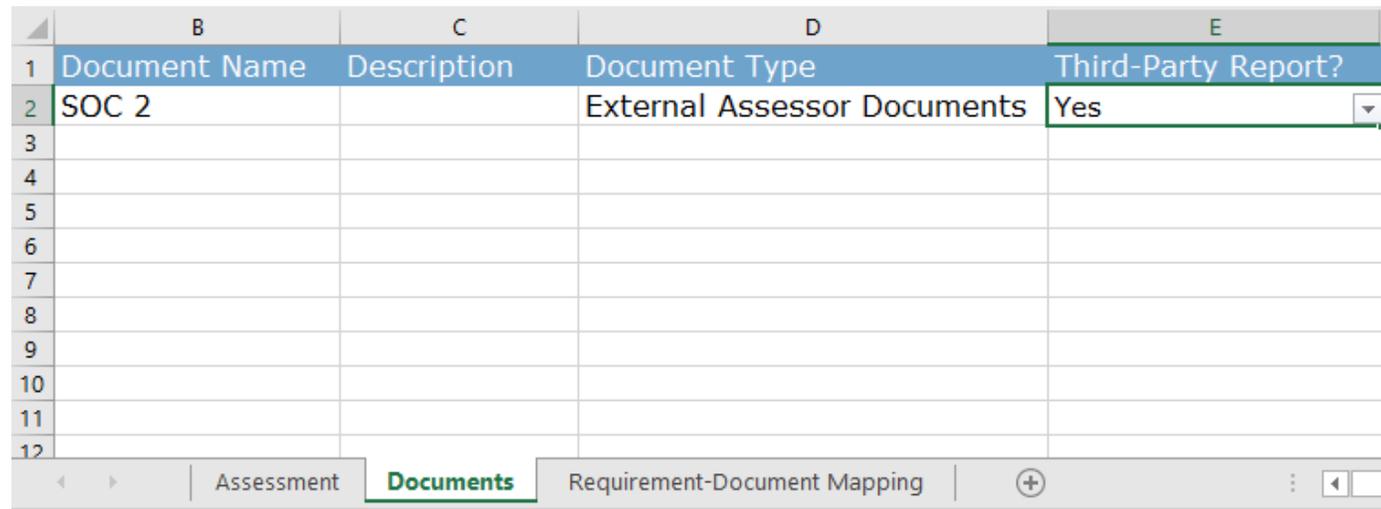
The assessment report's issuance date
mm/dd/yyyy

UPDATE CANCEL

Instructions: How to complete the Audits & Assessments Utilized Webform when relying on third-party audits and assessments

When adding an attestation report to the offline assessment, the External Assessor or Assessed Entity should follow these steps:

Step 1 – On the *Documents* sheet of the Offline Assessment workbook, enter the Document Name, Description (optional), and Document Type. Then set the value for “Third-Party Report?” to “Yes”.



	B	C	D	E
1	Document Name	Description	Document Type	Third-Party Report?
2	SOC 2		External Assessor Documents	Yes
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				

Instructions: How to complete the Audits & Assessments Utilized Webform when relying on third-party audits and assessments

Step 2 – After the Offline Assessment has been uploaded to MyCSF, the Audits and Assessments Utilized webform will be automatically populated with the following information:

- Name of the assessment utilized
- Utilization Approach (Reliance)
- Assessment Domain(s) containing requirement statements for which the document has been linked



Audits and Assessments Utilized

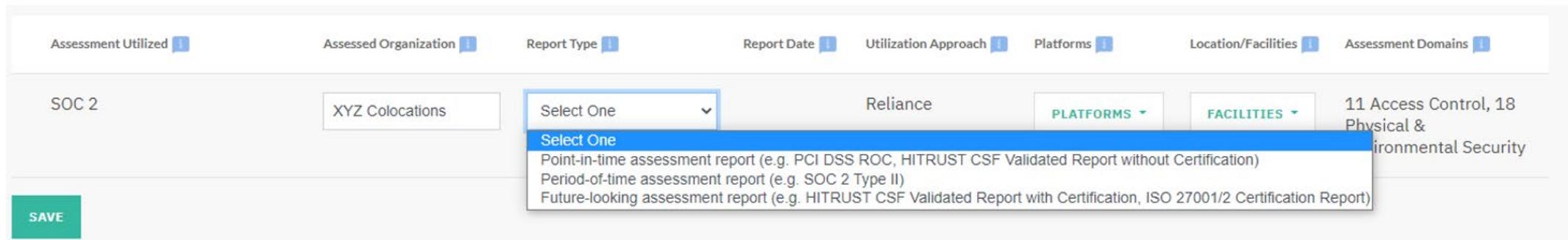
Assessment Utilized i	Assessed Organization i	Report Type i	Report Date i	Utilization Approach i	Platforms i	Location/Facilities i	Assessment Domains i
SOC 2	<input type="text" value="Enter Organization..."/>	<input type="text" value="Select One"/>		Reliance	<input type="button" value="PLATFORMS"/>	<input type="button" value="FACILITIES"/>	11 Access Control, 18 Physical & Environmental Security

Instructions: How to complete the Audits & Assessments Utilized Webform when relying on third-party audits and assessments

Step 3 – Enter the name of the name of the organization that was assessed for the assessment being added to the repository.

Step 4 – Select the Report Type from the options:

- Point-in-time assessment report (e.g., PCI DSS ROC, HITRUST Validated Report without Certification)
- Period-of-time assessment report (e.g., SOC 2 Type II)
- Future-looking assessment report (e.g., HITRUST Validated Report with Certification, ISO 27001/2 Certification Report)



The screenshot displays a webform with several input fields. The 'Report Type' field is currently set to 'Select One' and is open, showing a dropdown menu with three options: 'Point-in-time assessment report (e.g. PCI DSS ROC, HITRUST CSF Validated Report without Certification)', 'Period-of-time assessment report (e.g. SOC 2 Type II)', and 'Future-looking assessment report (e.g. HITRUST CSF Validated Report with Certification, ISO 27001/2 Certification Report)'. Other fields include 'Assessment Utilized' (SOC 2), 'Assessed Organization' (XYZ Colocations), 'Report Date', 'Utilization Approach' (Reliance), 'Platforms' (PLATFORMS), 'Location/Facilities' (FACILITIES), and 'Assessment Domains' (11 Access Control, 18 Physical & Environmental Security). A green 'SAVE' button is located at the bottom left of the form.

Instructions: How to complete the Audits & Assessments Utilized Webform when relying on third-party audits and assessments

Step 5 – Enter the relevant report dates depending on the Report Type selected in Step 4.

SOC 2 XYZ Colocations Point-in-time a: ▾ The assessment report's issuance date Reliance PLATFORMS ▾ FACILITIES ▾ 11 Access Control, 18 Physical & Environmental Security

mm/dd/yyyy 📅

Date of the assessment's report * mm/dd/yyyy 📅

SOC 2 XYZ Colocations Period-of-time ▾ The assessment report's issuance date Reliance PLATFORMS ▾ FACILITIES ▾ 11 Access Control, 18 Physical & Environmental Security

mm/dd/yyyy 📅

The assessment report's audit period start date * mm/dd/yyyy 📅

The assessment report's audit period end date * mm/dd/yyyy 📅

SOC 2 XYZ Colocations Future-looking ▾ The assessment report's issuance date Reliance PLATFORMS ▾ FACILITIES ▾ 11 Access Control, 18 Physical & Environmental Security

mm/dd/yyyy 📅

Date of the assessment's report * mm/dd/yyyy 📅

The assessment report's validity end date * mm/dd/yyyy 📅

Instructions: How to complete the Audits & Assessments Utilized Webform when relying on third-party audits and assessments

Step 6 – After a document has been identified as an attestation report issued by a third party and has been linked to at least one requirement statement, the External Assessor or Assessed Entity should return to the Audits and Assessments Utilized webform to select the relevant Platforms and Facilities.

Step 6a – The External Assessor or Assessed Entity should select the platforms that are relevant to the assessment utilized. The options listed will be the platforms/systems that were entered on the Scope of the Assessment page.

SOC 2 XYZ Colocations Period-of-time ▾ The assessment report's issuance date: 06/03/2021 Reliance **PLATFORMS ▾** FACILITIES ▾ 11 Access Control, 18 Physical & Environmental Security

Platform ABC

The assessment report's

Step 6b – The External Assessor or Assessed Entity should select the facilities that are relevant to the assessment utilized. The options listed will be the facilities that were entered on the Scope of the Assessment page.

SOC 2 XYZ Colocations Period-of-time ▾ The assessment report's issuance date: 06/03/2021 Reliance PLATFORMS ▾ **FACILITIES ▾** 11 Access Control, 18 Physical & Environmental Security

Data Center 123

The assessment report's