



Cybersecurity Compliance Certification (CCC)

Third Party Manual

July 2021

Table of Contents

How to Get Certified?.....	2
Appendix A - Related Documents	5

How to Get Certified?

Perform the following steps to obtain Saudi Aramco Cybersecurity Compliance Certificate (CCC):

1. Certification Requirements Preparation

- 1.1. For companies that aims to conduct business and register with Saudi Aramco: The company must comply with all controls under “A. General Requirements” section in Third Party Cybersecurity Standard (SACS-002).
- 1.2. For companies that have an active procurement agreement with Saudi Aramco:
 - 1.2.1. Initiate a request to all proponent organizations within Saudi Aramco that your company has ongoing business with to fill the *Third Party Classification Template*, please see [Appendix -A](#).
 - 1.2.2. Fill the *Third Party Classification Confirmation Letter*, please see [Appendix-A](#).
 - 1.2.3. If the company falls under more than one classification, then all the cybersecurity controls under the determined classifications are required.
- 1.3. Identify applicable certificate type and assessment requirements:

Company Classification	Certificate Type	Assessment Approach
<ul style="list-style-type: none"> > General Requirements > Outsourced Infrastructure > Customized Software 	Cybersecurity Compliance Certificate- CCC	A self-compliance assessment against SACS-002 completed by the company and verified remotely by the Authorized Audit Firm.
<ul style="list-style-type: none"> > Network Connectivity > Critical Data Processor 	Cybersecurity Compliance Certificate Plus- CCC+	An on-site compliance assessment against SACS-002 conducted by the Authorized Audit Firm.

- 1.4. If CCC & CCC+ are both applicable, based on your company classification, then only CCC+ will be accepted.
- 1.5. Implement all applicable cybersecurity controls specified in SACS-002.

2. Conduct Self-Compliance Assessment

- 2.1. For CCC+ certification, please skip this step and move to step # 4 (This section is applicable for CCC only)
- 2.2. Fill all of the fields in the *Third Party Cybersecurity Compliance Report*.

- 2.3. Ensure the answers are comprehensive, clearly described, and attach supporting documents.
- 2.4. Ensure evidences
 - Are clear, readable, and time stamped
 - Shows proof of its relation to the Third Party
 - Are clearly pointed out/highlighted in the screenshots

3. Select an Authorized Audit Firm

- 3.1. Select an Audit Firm from the Authorized Audit Firms list, available on <https://www.aramco.com/ccc>
- 3.2. Establish a contract with the Authorized Audit Firm prior to assessment verification.

4. Compliance Verification & Issuance

4.1. CCC

- 4.1.1. Submit the filled *Third Party Cybersecurity Compliance Report*, *Third Party Classification Template*, and *Third Party Classification Confirmation Letter* to the Authorized Audit Firm, prior to assessment verification.
- 4.1.2. The Authorized Audit Firm will verify the submitted documents and generate the *Third Party Cybersecurity Compliance Report*.

4.2. CCC+

- 4.2.1. Submit the *Third Party Classification Template* and *Third Party Classification Confirmation Letter* to the Authorized Audit Firm, prior to assessment verification.
 - 4.2.2. Arrange with an Authorized Audit Firm to conduct the compliance on-site-assessment.
 - 4.2.3. The Authorized Audit Firm will conduct the on-site assessment and generate the *Cybersecurity Compliance Report*.
- 4.3. If the company is 100% compliant against all applicable SACS-002 requirements, the Authorized Audit firm will issue *Third Party Cybersecurity Compliance Certificate*.
 - 4.4. In case your company didn't obtain 100% compliance, the Authorized Audit Firm will share Noncompliance Controls that you need to implement, to obtain the 100% compliance assessment result.

4.5. Implement the findings and submit the updated *Third Party Cybersecurity Compliance Report* to the Authorized Audit Firm, to verify the assessment.

5. Submit issued CCC



5.1. Submit both issued *Third Party Cybersecurity Compliance Certificate* and the *Cybersecurity Compliance Report* by the Authorized Audit Firm to Saudi Aramco, through the e-marketplace System.

6. CCC Validity & Renewal

- 6.1. CCC is valid for two years from the issuance date.
- 6.2. If your company is awarded with a new contract that involves a cybersecurity classification type not covered in the current valid certificate, then a new certificate needs to be obtained and submitted.
- 6.3. Prior to the end of the two years, your company needs to submit a new CCC.

Appendix A - Related Documents

To open the attachment, please right click on  and select “Open Hyperlink”.

Document Name	Attachment
Third Party Classification Template	
Third Party Classification Confirmation Letter	
Third Party Cybersecurity Compliance Report Template	