SABIC CyberTrust Manual

Supplier

Version 1.1

Disclaimer
This is a controlled document for business use by SABIC and its' business partners only. This document cannot be changed or distributed with any modification unless SABIC approves a new version.

Contents

1. PURPOSE 3
2. SCOPE 3
3. CERTIFICATION REQUIREMENTS 4
3.1 Determine supplier Classification 4
3.2 Implement Applicable Supplier Cybersecurity Certification Requirements 4
3.3 Complete CyberTrust Report 5
3.4 Select an Authorized Audit Firm 5
4. HOW TO GET CERTIFIED? 6
4.1 Assessment Process 6
4.2 Certificate Validity and Renewal 6
5. RELATED DOCUMENTS 7

1. PURPOSE

The purpose of this document is to assist SABIC's suppliers in complying with the cyber security requirements of the **SABIC CyberTrust Standard**. This manual will provide the suppliers with the required guidance to obtain the CyberTrust cybersecurity certificate.

2. SCOPE

The SABIC CyberTrust certification program applies to new or existing suppliers falling under the classifications in the table below and to suppliers that have access to SABIC data. Other suppliers can volunteer to comply with CyberTrust Standard.

Additional to the general requirements, specific cybersecurity requirements are defined for suppliers classified under the below classifications:

Type of Service	Code	Description
Network Connectivity	**NC**	Suppliers who require network connectivity to SABIC to provide its services including telecom-based services.
Cloud Computing Services (IaaS, PaaS, SaaS & Faas)	**CCS**	The Supplier provides cloud computing services: • Cloud Infrastructure as a Service (IaaS). • Cloud Platform as a Service (PaaS). • Cloud Software as a Service (SaaS). • Function as a service (Faas).
Outsourcing and Managed Services	**OMS**	Suppliers providing outsourcing and/or managed services including services and infrastructure such as data centers, co-location centers, and offline backup centers.
Consultancy Services	**CS**	Suppliers providing consultancy services with access to SABIC's classified data (i.e., financial data, strategic projects, confidential and strictly confidential data).
Software Management	**SM**	Suppliers providing custom software development and/or maintenance or packaged solutions.
OT/ICS products and services	**OT**	Suppliers providing OT product and/or services.

3. CERTIFICATION REQUIREMENTS

In order to obtain the CyberTrust certificate, the supplier must ensure the below requirements are followed:

3.1 Determine Supplier Classification

SABIC CyberTrust comprises specific cybersecurity requirements defined in **SABIC CyberTrust Standard**. These requirements are applicable based on the supplier's classification determined by the activity of work.

Additionally, the supplier's classification will be indicated by the UNSPSC Code shown on SAP Ariba.

3.2 Implement Applicable Supplier Cybersecurity Certification Requirements

- The supplier should refer to **SABIC CyberTrust Standard** to identify the applicable cybersecurity requirements based on their classification. The applicable registered suppliers that are aiming to conduct business with SABIC must implement all applicable cybersecurity controls in **SABIC CyberTrust Standard** prior to starting project execution. Moreover, contract awarded suppliers that are awarded to conduct business with SABIC must implement all cybersecurity controls in **SABIC CyberTrust Standard**, which are applicable based on the supplier classification.
- Classified suppliers are required to obtain the CyberTrust Certificate, while unclassified suppliers may choose to obtain it voluntarily.
- The supplier should refer to the **CyberTrust Guidelines** in order to understand the control implementation requirements.
- Existing supplier must obtain the certificate within 120 days after receiving notification by SABIC.

3.3 Complete CyberTrust Report

- The supplier must fill all of the fields in the **SABIC CyberTrust Report.**
- The supplier must ensure the answers are comprehensive, clearly described, and attach supporting documents.
- The supplier should ensure evidences are clear, readable, and time stamped.
- The supplier should ensure evidences show a proof of its relation to the supplier.
- The supplier should ensure a clear point out/highlight of the evidences in the screenshots.
- The supplier should provide valid justification for non-applicable controls which this justification must be added to the **CyberTrust Report,** and signed by the supplier.
- The supplier must implement all applicable cybersecurity controls specified in the **SABIC CyberTrust Standard** on:
  - All supplier information systems and/or assets used to connect to SABIC's network.
  - All supplier assets hosting, receiving, storing, processing, or transmitting SABIC data. These assets must be secured and stored in keeping with the **SABIC CyberTrust Standard** and must be made available to authorized users on a need-to-know basis.

3.4 Select an Authorized Audit Firm

- The certificate assessment and issuance will be performed by an independent audit firm authorized by SABIC.

4. HOW TO GET CERTIFIED?

4.1 Assessment Process

- The Supplier should conduct a self-assessment based on The Supplier classification that defines the assessment scope and the required cybersecurity controls as detailed in the **SABIC CyberTrust Standard**.
- The Supplier should refer to the **SABIC CyberTrust Guidelines** in order to understand the control implementation requirements.
- The Supplier should select one of the authorized audit firms from the CyberTrust authorized audit firms list published in SABIC supplier portal.
- The Supplier should establish a contract with the audit firm prior to conducting the assessment validation by the audit firm.
- The Supplier should submit the **CyberTrust Report** to the audit firm prior to conducting the assessment validation by the audit firm.
- The audit firm shall verify the submitted documents and generate the **CyberTrust Report**.
- The Supplier should obtain 100% compliance against all applicable SABIC CyberTrust requirements to attain the certificate from the audit firm.
- In case The Supplier did not obtain 100% compliance, the audit firm will share the non-compliance controls that The Supplier need to implement to obtain 100% compliance assessment result.
- The Supplier should implement the non-compliance controls and submit the updated report to the audit firm to re-validate the assessment.
- The Supplier should submit the **CyberTrust Certificate** and report to SABIC through the SABIC portal.

4.2 Certificate Validity and Renewal

The certificate will be valid for 2 years from the issue date, unless the supplier is awarded a contract with a classification type that is not covered in the current certificate then a new certificate should be obtained.

Classification: General Business Use

5. RELATED DOCUMENTS

In order to understand the CyberTrust program requirements to facilitate audit and certification journey, the supplier should refer to below documents:

1. SABIC CyberTrust Standard.
2. SABIC CyberTrust Guidelines.