SABIC CyberTrust Controls Guidelines

Version 1.0

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. DEFINITIONS

The following terms and abbreviations have been defined for use within this document:

Term	Definition
Access Management Policy	A policy that defines the required access control measures to all the information systems and applications to protect the privacy, security, and confidentiality of information technology resources.
Advanced Persistent Threat	An adversary with sophisticated levels of expertise and significant resources, allowing it through the use of multiple different attack vectors (e.g., cyber, physical, and deception) to generate opportunities to achieve its objectives. The advanced persistent threat pursues its objectives repeatedly over an extended period.
Anti-Malware	Software that is designed to detect, and remove, block, or contain various forms of malicious software.
Asset	Anything that has value to an organization, including but not limited to, another organization, person, computing device, information technology (IT) system, IT network, IT circuit, software, virtual computing platform, and related hardware.
Audit Log	Chronological record of information system activities providing an independently verifiable trail sufficient to permit reconstruction, review, and examination of sequence of environments and activities surrounding or leading to operation, procedure, or event in a transaction from inception to final results.
Backup	A backup, or data backup is a copy of computer data taken and stored elsewhere so that it may be used to restore the original after a data loss event.
Cloud computing	It is a model that enables convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Cloud models are composed of five Essential Characteristics: On-demand self-service, broad network access, Resource pooling, rapid elasticity, and measured service. There are three types of cloud computing services delivery models: • Cloud Software as a Service (SaaS). • Cloud Platform as a Service (PaaS). • Cloud Infrastructure as a Service (IaaS).
Consulting Services	Services provided by a professional advisory team where consultants review and analyze client business data and documents, which may contain sensitive and confidential data, and offer advice, benchmarks, and use their expertise to recommend best practice or help businesses based on their individual requirements.
Contract	An agreement between parties creating mutual obligations enforceable by law.
Cybersecurity	The information security requirements needed to support the protection of confidentiality, integrity, and availability of Assets.
Cybersecurity Acceptable Use	It is a policy stipulating constraints and practices that a System User must agree to for access to a corporate network, the internet or other resources. It states what a System User can and cannot do when using computers and computing resources.
Cybersecurity Assessment	Assessment conducted by SABIC to ensure that the Supplier is in full compliance with the Supplier Minimum Cybersecurity Requirements included in this document and any Contract.

Term	Definition
Firewall	Hardware and/or software technology that protects network resources from unauthorized access. A firewall permits or denies computer traffic between networks with different security levels based upon a set of rules and other criteria.
Industrial Control System (ICS)	An information system used to control industrial processes such as manufacturing, product handling, production, and distribution. Industrial control systems include supervisory control and data acquisition systems used to control geographically dispersed assets, as well as distributed control systems and smaller control systems using programmable logic controllers to control localized processes.
Logical access	Providing an authorized System User the ability to access one or more computer system resources such as a workstation, network, application, or database through automated tools. A Logical access control system requires validation of an individual's identity through some mechanism such as a personal identification number, smartcard, username and password, biometric, or other token.
Outsourcing	Business practice in which certain functions required by the business are performed by outside parties on a contract basis rather than the business's employees
Managed Services	Professional services that are provided on subscription basis to offload some professional IT and cybersecurity operations. This includes products, solutions, software, and hardware
Multi-Factor Authentication	Method of authenticating a system user whereby at least two factors are verified. These factors include something the System User has (such as a smart card or dongle), something the System User knows (such as a password, passphrase, or PIN), or something the System User has or does (such as fingerprints and other biometric elements).
Operational Technology (OT)	Programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems or devices detect or cause a direct change through the monitoring or control of devices, processes, and events. Examples include industrial control systems, building management systems, fire control systems, and physical access control mechanisms.
Patch	A piece of software designed to fix operating system or software programming errors and Vulnerabilities
Phishing	Phishing is a cybercrime in which a target or targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords.
Purchase Order	The document, including any attachments thereto, issued by Purchaser to order goods and/or services from Supplier.
Sanitize	The action of permanently removing all data and/or licensed software, through overwriting or degaussing methods, from an Asset before that Asset is disposed, loaned, destroyed, donated, transferred, or surpluses.
SAUDI BASIC INDUSTRIES CORPORATION (SABIC)	SAUDI BASIC INDUSTRIES CORPORATION, a joint stock company incorporated under the laws of the Kingdom of Saudi Arabia, having its head office located at P.O. Box 5101, Riyadh, 11422, Kingdom of Saudi Arabia, registered with the Commercial Register of Riyadh on 14 Muharram 1397H corresponding to 4 January 1977 under number 1010010813, and having a share capital of 30,000,000,000 Saudi Riyals fully paid.
Sender Policy Framework	Email-validation system that allows domain owners to publish a list of authorized IP addresses or subnets to detect and block email spoofing, and reduce the amount of spam, fraud and Phishing.

Term	Definition
Social Engineering	A manipulation technique that exploits human error to gain private information, access, or valuables. In cybercrime, these "human hacking" scams tend to lure unsuspecting System Users into exposing data, spreading malware infections, or giving access to restricted systems.
Staff Augmentation	The service provides people to augment the company staff with skill needed. The organization's augmented staff will be managed directly by the company, as if they are employees
Supplier	The legal entity specified in the relevant Purchase Contract as the supplying Party.
Supplier Environment	Supplier collection of computers, data storage devices, workstations, software applications, and networks that support the processing and exchange of electronic information.
System Integration	The service to support the creation a complex information system that may include designing or building a customized architecture or application, integrating it with new or existing hardware, packaged and custom software, and communications.
System Users	Supplier employees, contractors and others who have access to the Supplier information systems.
Telework System	Any technical system means or tools and its related components that are used by the organization to enable employees to perform their job duties in a place other than the official workplace. Examples include virtual meeting systems, collaboration systems, file sharing, virtual private network (VPN), remote access systems, and other systems used in the work environment.
Data Loss Prevention (DLP)	Set of tools and processes used to ensure that sensitive data is not lost, misused, or accessed by unauthorized users. DLP software classifies and monitors data to protect it both in transit and at rest, and can enforce data security policies to prevent unauthorized data transfers.

2. PURPOSE

SABIC CyberTrust Controls Guidelines provides guidance about how to fulfill the cybersecurity requirements set forth in the SABIC CyberTrust Standard. The scope and applicability of the controls is defined in the standard. These guidelines ensure that Suppliers are aware of the control requirements and supporting evidence, and that they are provided as part of the Supplier compliance package that will be submitted to the authorized audit firm.

3. SCOPE

This document provides guidance to all the requirements included in the SABIC CyberTrust Standard where the applicability of the requirements is defined. The applicability of the general requirements and specific requirements is based on the classifications defined in the standard that is show in the table below:

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.

4. CONFLICTS AND DEVIATIONS

In the event supplier's compliance with an applicable cybersecurity requirement included in the "SABIC CyberTrust Standard" is not technically possible, a waiver must be requested explaining the compensating control(s) applied. The waiver request will be analyzed by the auditor and raised to SABIC for approval.

The auditor must also highlight the waived/non-applicable control(s) within the report template and provide their assessment on any compensating controls and residual risks, if any, related to the control waiver request.

5. REVISION

This document will be reviewed, and updated annually or as required, by SABIC Cybersecurity department, to ensure that it continues to meet the business requirements. Updates to the cybersecurity requirements will be communicated to Suppliers where a significant change is made.

Before obtaining a new certification or renewing an existing one, it is advisable to download the required documents from SABIC's website.

6. SUPPLIER CYBERSECURITY REQUIREMENTS

6.1. GENERAL CYBERSECURITY REQUIREMENTS

The table below includes the General Cybersecurity requirements defined in the SABIC CyberTrust Standard. Column 'Control Guidelines' provides guidance on the control requirements and evidence requirements to show conformance with the standard.

Control ID	Requirement	Control Guidelines
GOVERN		
Policies, Processes, and Procedures (GV.PO)		
CT-01	**Information security management** Suppliers must have defined policies for information security, approved by their management, and communicated to the people with access to their information systems.	- Provide evidence of the supplier Cybersecurity Policies and Standards. - Provide evidence of communicating Cybersecurity Policies to employees. - Provide evidence where policies should be version-controlled
IDENTIFY		
Improvement (ID.IM)		
CT-02	**Self-assessments** Suppliers will perform, at minimum, a self-assessment of their operational resilience and Cybersecurity practices in order to identify and appropriately manage potential risks. The self-assessment must include, at minimum, all the requirements included in this document. The self-assessment must be repeated at yearly intervals (or when requested by SABIC).	- Provide a documented evidence of the self-assessment processes. - Provide the annual conducted self-assessments. - Provide evidence of the conducted risk assessment to identify potential vulnerabilities and threats to their operational resilience and cybersecurity practices. - Provide evidence of alignment of the self-assessment processes with relevant industry standards and best practices, such as NIST CSF, ISO 27001 for cybersecurity and ISO 22301 for business continuity.
CT-03	**Asset Management** SABIC Assets associated with information processing facilities managed by the Supplier must be identified and an inventory of these Assets must be drawn up and maintained by the Supplier.	- Provide evidence of the established and maintained comprehensive inventory of all identified assets. Include details such as asset name, description, unique identifier, location, owner, responsible party. - Provide a list of categorized assets based on their criticality, sensitivity, and importance to the organization. - Provide evidence of Implemented tagging for physical assets to facilitate easier tracking.

Control ID	Requirement	Control Guidelines
PROTECT		
Identity Management, Authentication, and Access Control (PR. AA)		
CT-04	**Access control management** Supplier must have a defined, documented and enforced Access Management Policy for physical and Logical access to networks, systems, and applications in Supplier Environment that processes, accesses, or stores SABIC 's data. • At least the Access control management must include: • the access rights granting, changing, and disabling based on documented and authorized approvals. • a process implemented to ensure the disabling of account of personnel no longer on employment or contracted. • the periodical review of access rights to ensure that access is fit for purpose. • In addition, it is recommended to implement the following password security requirements. • password minimum length of 8 characters and complexity rules. • password expiry set not less than 90 days. • Account lockout threshold set to 10 attempts (or less). • No password sharing allowed.	- Provide evidence of a document for developing a comprehensive Access Management Policy that outlines the procedures, guidelines, and requirements for granting, revoking, and managing access to physical and logical resources within the supplier environment. - Provide the established access control framework that defines roles, responsibilities, and privileges for different user groups. - Provide evidence of the Implemented access controls to ensure that users have the minimum level of privileges necessary to perform their job functions (principle of least privilege). - Provide evidence of the Implemented formal access request and approval process, these requests should be approved by authorized personnel before access is granted. - Provide evidence of the password configuration on Active Directory or LDAP to ensure that default settings are not used. If active directory does not exist, provide evidence from the local password policy on sample systems. - Provide evidence of password policy that should comply with the control requirements and technical check findings. - Provide evidence of enforcing the use of Multi-factor authentication on all privileged accounts access.
Platform Security (PR.PS)		
CT-05	**Physical security perimeter** Supplier must define and implement the security perimeters of their Environment to protect key systems/services and physical assets.	- Provide evidence that demonstrating the framework to protect key systems/services and assets physically - Provide evidence of appropriate physical security controls are commensurate with risk, including the following: a. Alarms and intruder detection systems with keyholder response (e.g. CCTV, motion sensors,...). b. Electronic Access Control Systems? c. Environmental controls (e.g. fire and smoke detectors). d. Physical barriers, locks, doors or walls.
CT-06	**Media protection** Supplier must protect both paper and electronic information or any other media storing SABIC's data, by limiting access to information on those media to the authorized System Users and Sanitize or destroy information system media before disposal or release for reuse.	- Provide evidence of implementation of security measures to ensure that only authorized System Users can access SABIC information/data stored in electronic form, paper or any other media. - Provide evidence of protect data at rest with measures like encryption. - Provide evidence of implementation of security measures to ensure the secure removal of data in media before disposal or reuse.

Control ID	Requirement	Control Guidelines
CT-07	**Personnel security** Suppliers must apply preventive measures confirming the adequacy and integrity of their System Users involved in the provision of services to SABIC. These measures must, at minimum, include the verification of their references and identity and the employee's agreement for proper use of information systems. The Supplier must report all changes related to System Users with access to SABIC's information systems so that their access authorization can be updated by SABIC accordingly. The Supplier must have formal procedures for off-boarding employees and contractors. Off-boarding procedures must include the return of Assets, and removal of all associated access rights.	- Suppliers must apply preventive measures confirming the adequacy and integrity of their System Users involved in the provision of services to SABIC. These measures must, at minimum, include: a. Identity and legal right to work verification. b. Address verification c. Employment history and reference checks. d. Criminal background checks. e. Employee's agreement for proper use of information systems. - Provide evidence of the supplier termination procedures to determine whether accounts/access are revoked in a timely manner. - Provide evidence of the return of assets. - Provide a copy of off-boarding procedures that shows the removal of all access to Assets.
Awareness and Training (PR.AT)		
CT-08	**System Users training** Supplier must provide and require all System Users to take a yearly mandatory Cybersecurity awareness training that addresses acceptable use and good computing practices. Training must address at least the following topics: • Cybersecurity Acceptable Use. • Internet and social media security. • Social Engineering and Phishing emails. • Confidentiality and not sharing credentials (e.g., user/password). • Information security policies.	- Provide acceptable use policy and/or training materials to ensure content is adequate. - Provide user training reports and/or documentation to ensure users are trained in accordance with applicable policy, guidance, and/or requirement (e.g., annual cybersecurity training of all employees). - Provide evidences of updating the training materials based on changes in cyber threat environment.
Technology Infrastructure Resilience (PR.IR)		
CT-09	**Email service protection** The Supplier must protect its email service with at least the following: • Analyzing and filtering email messages (specifically regarding Phishing and spam) using up-to-date email protection techniques. • Multi-Factor Authentication for remote and webmail access to email service • Email archiving and Backup. • Secure management and protection against Advanced Persistent Threats. • validation of the Supplier email service domains (e.g., using Sender Policy Framework).	- Provide evidence of SPF and DKIM enforcement on SABIC email domains: sabic.com - Provide evidence of policies enforcing the use of Multi-factor authentication on remote access to information systems and applications that including webmail access to email service. - Provide evidence of Multi-factor authentication page and configuration console. - Provide evidence of the email filtering technologies in place, in particular related to phishing and spam.

Control ID	Requirement	Control Guidelines
CT-10	**Patching** Supplier technology Assets and systems must be regularly updated with the operating system (OS), software and applications Patches provided by their manufacturer according with industry best practices.	- Provide evidence of the developed and maintained Patch Management Policy that outlines the procedures for identifying, testing, approving, and deploying OS, software, and application patches. - Provide evidence of regularly conducted vulnerability assessments to identify vulnerabilities in operating systems, software, and applications. - Provide evidence of deployed critical security patches promptly after testing, especially those addressing known vulnerabilities that are actively exploited or pose significant risks. - Provide evidence of established rollback procedures in case a patch causes unexpected issues or disruptions.
CT-11	**Anti-Malware** Supplier technology Assets must be protected with Anti-Malware software. Updates must be applied daily, and full system scans must be performed at least every two weeks. In case of virus/malware detection, the virus/malware must be eradicated promptly, and the affected systems restored to a clean status.	- Provide evidence of the anti-malware installed on endpoint devices. - Provide evidence of configuration console of the installed anti-malware software to determine the last updates and full system scan that were performed every two weeks. - Provide evidence of the history of updates.
CT-12	**Network controls** Networks in the Supplier Environment shall be managed and controlled to protect information in systems and applications. Network controls shall be deployed by means of Firewalls and other network security technologies that includes Intrusion Detection Systems (IPS) or Intrusion Detection Systems (IDS) and acting as network policy enforcement points.	- Provide evidence of the network security devices such as firewall setting for all third-party endpoint devices including related policies for enabling firewalls. - Provide evidence of the firewall being enabled on domain, public and private firewall settings on sample of third-party endpoint devices. - Provide evidence of network diagram for firewalls and IPS/IDS placement.
DETECT		
Continuous Monitoring (DE.CM)		
CT-13	**Audit and accountability** Supplier must create and maintain information system Audit Logs needed to allow the analysis, investigation, and reporting of unauthorized, or inappropriate information system activity in the Supplier Environment and ensure that the actions of individual information System Users can be attributed to those System Users.	- Provide evidence of audit logs (e.g., security, activity) are maintained and reviewed in a timely manner. - Provide evidence of Log files are sized such that logs are not deleted prior to review and/or being backed up. - Provide evidence of the supplier policy of logs handling. - Provide evidence of Audit logs and log management & analysis tools that are protected from unauthorized access, modification, and deletion. - Provide evidence of Audit records contain appropriate content (e.g., type of event, when the event occurred, where the event occurred, source of the event, and outcome of the event, identity of any individuals or subjects associated with the event).

Control ID	Requirement	Control Guidelines
RESPOND		
Incident Management (RS.MA)		
CT-14	**Incident response** Supplier must have an incident handling process for information systems in the Supplier Environment, which includes the preparation to detect, analyze, contain, recover and response to incidents.	- Provide evidence of the incident response plan to determine if appropriate steps are taken consider the following: a. Obtain evidence of event notifications (e.g., detection alerts, reports) from different systems. b. Determine who receives alerts or reports from detection systems and what actions are taken once reports are received. c. Review the incident response plan to determine if actions taken follow the plan. d. Steps to contain and control the incident to prevent further harm. e. Procedures to notify potentially affected Parties. f. Strategies to control different types of incidents (e.g., distributed denial-of-service [DDoS], malware, etc.). g. Steps to mitigate the incident to prevent further harm. h. Review any documented incidents to determine whether mitigation efforts were implemented and effective. - Provide evidence of reviewal organization's incident handling reports and incident testing documentation for action items and lessons learned.
Incident Analysis (RS.AN)		
CT-15	**Incident categorization** The supplier must define a clear process of how incidents are categorized based on the impact it could leave.	- Provide evidence of the incident response plan to determine if there is a process to formally analyze and classify incidents based on their potential impact. - Provide incident response plan to determine if it is designed to prioritize incidents, enabling a rapid response for significant incidents or vulnerabilities.
RECOVER		
Incident Recovery Communication (RC.CO)		

Control ID	Requirement	Control Guidelines
CT-16	**Supplier incident reporting** The Supplier must notify and report to SABIC any adverse situation or Cybersecurity incident that occurs in the Supplier Environment, affecting any networks, systems or applications that process, access, or store SABIC's data. The notification must be made as soon as practicable, but **no later than twenty-four (24) hours** after the Supplier becomes aware of it or should have become aware of it. The Supplier must make the notification to SABIC using the following channel: Email: CyberSecurityCenter@SABIC.COM	- Provide a clear and documented Incident Reporting Policy that outlines the procedures and guidelines for reporting adverse situations or cybersecurity incidents. - Implement procedures for promptly identifying adverse situations and cybersecurity incidents within the Supplier Environment. - Establish a protocol for immediate notification to SABIC in the event of a severe cybersecurity incident. For incidents requiring urgent attention, initiate immediate contact using predefined communication channels to inform SABIC stakeholders.

6.2. SPECIFIC CYBERSECURITY REQUIREMENTS

The table below includes the Specific Cybersecurity requirements defined in the SABIC CyberTrust Standard. Column 'Control Guidelines' provides guidance on the control requirements and evidence requirements to show conformance with the standard.

The code used to identify the classifications are as below:

Type of Service or Good	Code
Network Connectivity	NC
Cloud Computing Services (IaaS, PaaS, SaaS & FaaS)	CCS
Outsourcing and Managed Services	OMS
Consultancy Services	CS
Software management	SM
OT/ICS products and services	OT

Control ID	Requirement	Control Guidelines
GOVERN		
Risk Management Strategy (GV.RM)		
CT-17	The Supplier must maintain a Cybersecurity risk management and mitigation program, with clear roles & responsibilities, processes, risk appetite and tolerance, risk strategy, and Third Party Risk Management.	- Provide evidence of the framework or process used for risk management. Consider the following: a. Provide evidence of the organization's risk management plan showing the organization's response to risk levels. b. Provide evidence of risk register. c. Provide evidence of risk management plan that is designed to accept or reduce risk level in accordance with the organization's risk appetite/ tolerance.
Policies, Processes, and Procedures (GV.PO)		
CT-18	The Supplier must have policies and processes to classify information in terms of its value, sensitivity, criticality, confidentiality and regulatory requirements.	- Provide evidence of the third party data classification policy. - Provide implementation of data classification policy that categorizes data into different types based on value, sensitivity, criticality, confidentiality and regulatory requirements. - Provide evidence of the third party Data Classification program that cover all key resources (e.g., hardware, devices, data, software, and cloud) are classified based on risk.
Roles, Responsibilities, and Authorities (GV. RR)		

Control ID	Requirement	Control Guidelines
CT-19	The Supplier must have employee(s) whose primary responsibility is Cybersecurity. Responsibilities of those personnel must include maintaining the security of information systems and ensuring compliance with existing policies.	- Provide a copy of the organizational chart. - Provide evidence of job descriptions, agreements, RACI charts, service level agreements (SLAs) and/or contracts to determine if they include cybersecurity roles and responsibilities.
CT-20	The Supplier must conduct background check (screening/vetting) on Employees viewing or/and processing SABIC's confidential and strictly confidential.	- Provide evidence of hiring procedures to determine whether background checks/screenings are performed for all employees. - Provide evidence of HR screening policy.
IDENTIFY		
Asset Management (ID.AM)		
CT-21	The Supplier must follow an established Secure development Life Cycle (SDLC) for the Software and product development. The SDLC should comply with applicable best practice guidelines. SDLC should incorporate vendor-specific development best practices to ensure applications are built with the recommended security guidance from the vendor.	- Provide a documented SDLC policy outlining the secure development practices, including guidelines for coding standards, security testing, and vulnerability management. - Provide the SDLC followed by the supplier should adhere to recognized industry standards such as OWASP, CERT, or NIST, ensuring that the software development process meets established security benchmarks. - Provide evidence of enforcing the use of secure coding standards and best practices, ensuring that developers follow guidelines to prevent common security issues like SQL injection. - For OT/ICS, provide the Security Development Lifecycle Assurance (SDLA) Certification of compliance to the ISA/IEC 62443-4-1 standard.
CT-22	Supplier must use Secure-by-design principles as part of security architectural designs for OT/ICS products. Secure-by-design principles include establish secure defaults, minimize attack surface area, fail securely, defense in depth, least privilege, separation of duties, keeping security simple and avoid security by obscurity.	- Provide evidence of conducted comprehensive security architecture review for their OT/ICS products, ensuring they are designed with security in mind from the ground up. - Provide evidence of performed threat modeling exercises specific to the OT/ICS domain to identify potential threats and vulnerabilities early in the design phase. - Provide evidence of configuration OT/ICS products with secure defaults, ensuring that unnecessary services are disabled, and default passwords are changed before deployment.
CT-23	The Supplier must inventory all third-party software components (whether commercial, free, or open-source software) used in the Software development and provide such inventory to SABIC upon request. Supplier must assess whether any such components have any security defects or vulnerabilities that could lead to a Security Incident.	- Provide evidence of the created and maintained comprehensive inventory of all third-party software components used in their products, including libraries, frameworks, modules, and dependencies. - Provide evidence of the documented specific versions of third-party software components within the inventory to track potential vulnerabilities associated with specific versions. - Provide evidence of securely configuring third-party components based on industry best practices and security guidelines. Default configurations should be reviewed and adjusted to minimize security risks.
Risk Assessment (ID.RA)		

Control ID	Requirement	Control Guidelines
CT- 24	The supplier must conduct risk assessment to identify potential threats and mitigation plans of the identified risks should be well documented.	- Provide evidence of risk assessment performed and methodology used. - Provide evidence about who performs the assessments. - Provide evidence of the risk register as a result of the risk assessment.
CT-25	The Supplier must perform a regular vulnerability scanning using trusted vulnerability management technologies.	- Provide evidence of different security scans and vulnerability reports found on all developed applications. - Provide evidence of remediation of all security issues and findings discovered and closed prior the deployment in production. - Provide Application Vulnerability scanning policy.
CT-26	The Supplier must conduct at least annual Penetration Testing on its IT infrastructure systems and internet facing applications by reputed external party.	- Provide evidence of annual penetration testing reports conducted and analyzed on IT infrastructure considering all critical, internal and external systems, and internet facing applications. - Provide evidence of a policy tackling penetration test schedule, scope and requirements exist and communicated to stakeholders. - -Provide evidence of remediation and action plan related to penetration test results.
Improvement (ID.IM)		
CT-27	The personnel with access to OT/ICS assets, besides the general cybersecurity training and awareness, must go through an OT/ICS cybersecurity awareness and training program. The program must include, at a minimum, the following: customized training, qualifications, knowledge, and professional skillsets related to the OT/ICS assets cybersecurity.	- Provide user training reports and/or documentation to ensure users are trained in OT/ICS field, guidance, and/or requirement (e.g., annual cybersecurity training of all employees). - -Provide evidences of updating the training materials based on changes in cyber threat environment.
CT-28	The Supplier must have a process in place to guarantee that a non-disclosure agreement between contracted employees of the Supplier and the Supplier is signed before access to SABIC systems and/or premises is granted.	- Provide developed a comprehensive NDA policy document outlining the necessity of NDAs for all contracted employees before granting access to systems and premises. Clearly define the scope, terms, and obligations outlined in the NDAs. - Provide mandating document that all contracted employees, consultants, and third-party vendors sign the NDA before being granted access to systems, premises, or any sensitive information. Also, extend the requirement for NDAs to third-party vendors, subcontractors, and any external entities working on behalf of the Supplier.
PROTECT		
Identity Management, Authentication, and Access Control (PR. AA)		
CT-29	System Users must have unique user logins and passwords for applications and systems. Generic accounts must not be allowed, unless explicitly approved, restricted, and controlled.	- Provide evidence of access management policy that shows the requirement of using unique accounts. - Test sample of servers/ systems to determine if unique account is used for on-site assessment.

Control ID	Requirement	Control Guidelines
CT-30	All privileged accounts must be limited, justified, and reviewed on regular basis.	- Provide evidence of a policy that shows the procedure of obtaining and revoking the admin privileges based on the job requirements/ function. - Provide evidence of the third party process to identify privileged users. - Provide evidence of privileged accounts reviewed regularly.
CT-31	Multi-factor authentication must be enforced on all privileged accounts access including remote access to information systems and applications.	- Provide evidence of policies enforcing the use of Multi-factor authentication on all privileged accounts access including remote access to information systems and applications. - Provide evidence of Multi-factor authentication page and configuration console of all privileged accounts access including remote access to information systems and applications.
CT-32	The Supplier must support identity federation services.	- Provide evidence which ensures the Supplier supports widely recognized federation protocols such as Security Assertion Markup Language (SAML), OAuth and OIDC for seamless integration with identity federation services. - Provide a document to implement Single Sign-On functionality, allowing users to authenticate once with their identity provider and access multiple services and applications without needing to log in separately for each one. - Provide a document for establish a process for registering and verifying identity providers before allowing federation services. Ensure that authorized and trusted identity providers are integrated to prevent unauthorized access attempts.
Platform Security (PR.PS)		
CT-33	The Software must have the capability to segregate different data typology processed.	- Provide evidence for the software with built-in mechanisms to segregate different data typologies processed. Implement logical and physical separation of data, ensuring that sensitive data is isolated from less sensitive or public data. - Provide policy of enforce access controls and role-based permissions within the software.
CT-34	The Software must have the capability to provide authorization based on roles.	- Provide a document that emphasizes a Role-Based Access Control (RBAC) policy that defines roles and associated permissions within the software. - Provide a document that ensure that each user is assigned a specific role based on their job responsibilities and requirements. - Provide a document that emphasizes a role hierarchy if applicable, where higher-level roles inherit permissions from lower-level roles.
CT-35	The Software must support multi-factor authentication for users.	- Provide evidence of policies enforcing the use of Multi-factor authentication on all users. - Provide evidence of Multi-factor authentication page and configuration console of all users.

Control ID	Requirement	Control Guidelines
CT-36	The Software must have the capability to segregate users' accessible data.	- Provide a document for developing and implementing a data segregation policy that defines the criteria and rules for segregating users' accessible data. Clearly outline the segregation requirements based on user roles, departments, projects, or any other relevant factors. - Provide a document for design the software with built-in mechanisms to segregate users' accessible data logically and physically. Implement strong access controls to ensure that users can only access data relevant to their roles and responsibilities. - If the software supports multi-tenancy, provide a document for ensuring that users' accessible data is segregated at the tenancy level.
CT-37	Network connections to information systems and applications at the Supplier location must be authorized and monitored.	- Provide evidence of policies and procedures related to remote users' access capabilities are formalized. Consider that remote users (e.g., employees, contractors, third parties) with access to critical systems are approved and documented and remote connections are logged and monitored.
CT-38	The cryptographic technologies used by the product must be aligned with the applicable national regulations.	- Provide a document demonstrating that cryptographic technologies used in the product are regularly assessed to ensure alignment with applicable national regulations and standards. Stay updated with changes in regulations to adapt cryptographic implementations accordingly. - Provide a document for how to select cryptographic algorithms and protocols approved by the national regulatory authorities. - Provide evidence that demonstrating the conducted comprehensive review of national regulations related to cryptography.
CT-39	The Supplier must implement sufficient mechanisms to protect data-in-transit. Data-in-transit should be encrypted with strong, approved algorithms. End-to-end encryption should be enforced where applicable using VPN and/or TLS capable connectivity solutions with secure key exchange and forward-secrecy capability.	- Provide a document for how to use industry-standard and secure communication protocols such as HTTPS (SSL/TLS), SFTP, SSH, or IPsec to encrypt data transmitted over networks. - Provide a document that explains using digital certificates and PKI to establish secure connections between systems. - Provide a document for when transferring files, use secure file transfer protocols such as SFTP (SSH File Transfer Protocol) or SCP (Secure Copy Protocol) that provide encryption and authentication features,
CT-40	Encryption keys and certificates must be managed in a secure manner.	- Provide evidence of encryption key management procedure and policy. - Provide evidence of key management configurations.
CT-41	The Supplier must implement data-at-rest encryption mechanisms, using at least AES-128 encryption algorithm, on all devices or storage media hosting sensitive data.	- Provide evidence of encryption mechanisms applied on all devices, including disk drives. - Provide evidence of a policy ensuring mobile devices (e.g., laptops, tablets, and removable media) that are used to store confidential data are encrypted.
CT-42	Wireless networks accessing information systems must use strong encryption for authentication and transmission, such as WPA2 or WPA2 Enterprise.	- Provide evidence of access point configuration. - Provide evidence of Wireless baseline details.

Control ID	Requirement	Control Guidelines
CT-43	Creation of tunnels must be based on certificates with automation of tunnel creation and key rotation for each tunnel.	- Provide a document for sharing that tunnels must be created using certificates for authentication, ensuring a strong cryptographic mechanism to establish secure connections. - Provide a document for automate the process of key rotation for each tunnel to enhance security. Keys should be rotated regularly, following industry best practices and organizational policies. - Provide a document for maintaining a secure and trusted Certificate Authority for issuing and managing certificates used in the tunnel creation process. - Provide a document for Implementing secure key management practices, including secure storage, access control, and encryption of keys at rest, to prevent unauthorized access.
CT-44	The Supplier must provide secure session management including session authenticity, lockout, and timeout termination.	- Provide evidence of applied configurations from the available security appliance, showing the use of secure transmission protocols. - Provide evidence of configurations for session authentication enforcement, lockout, and timeout.
CT-45	The Supplier must have network controls deployed such as firewalls, network segmentation, network access control, Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS) and DoS filtering.	- Provide evidence of IPS/IDS configurations and enablement. - Provide evidence of the DoS defense deployed. - Provide evidence of network segmentation. - Provide evidence of network access controls - Provide evidence of complementary network controls in place.
CT-46	The Supplier must implement a device control mechanism (Endpoint Security) on Assets that are used to receive, store, process or transmit SABIC data.	- Provide a document for developing and documenting clear endpoint security policies specifying the requirements for devices used to handle and process data. - Provide a document for deploying endpoint security software solutions, including antivirus, anti-malware, and firewall programs, on all devices that handle and process data. - Provide a document for Implementing full disk encryption on endpoints to protect data at rest.
CT-47	The Supplier must have and apply a secure baseline configuration which should be established following applicable best practice guidelines (e.g., CIS) for all underlying assets used to provide the agreed service.	- Provide evidence of the baseline configurations for systems (e.g., servers, desktops, routers). - Provide evidence of samples against the third party's baseline configurations to ensure standards are followed and enforced, for the following: a. Resetting default usernames/passwords. b. Disabling unneeded software. c. Disabling unneeded services. d. Removing administrative access of users on workstations.

Control ID	Requirement	Control Guidelines
CT-48	The Supplier must conduct periodic vulnerability scans to evaluate configuration, Patches, and services for known Vulnerabilities.	- Provide evidence of the third party vulnerability management plan and ensure it includes the following: e. Frequency of vulnerability scanning. f. Method for measuring the impact of vulnerabilities identified (e.g., Common Vulnerability Scoring System. g. Incorporation of vulnerabilities identified in other security control assessments (e.g., external audits, penetration tests) h. Procedures for developing remediation of identified vulnerabilities. - Provide evidence of samples of vulnerability scan reports. - Provide Vulnerability scanning policy.
CT-49	The Supplier must implement a sanitization process before any Assets are loaned, donated, destroyed, transferred, or surpluses. The process must be aligned to industry best practices such as NIST 800-88.	- Provide a policy and procedure document outlining the sanitization process for assets before they are loaned, donated, destroyed, transferred, or surplused. - Provide evidence of classification of data based on sensitivity (e.g., public, internal, confidential, restricted) to determine the level of sanitization required for different types of information. - Provide evidence that the sanitization methods used comply with industry standards and regulations (e.g., NIST guidelines, ISO/IEC 27040 Standard). - Provide evidence of restricted access to the sanitization process to authorized and trained personnel only.
CT-50	The Supplier must retain all audit logs from information systems and applications storing, processing, or transmitting SABIC data for one (1) year, as per local and international laws and regulations (whichever is greater) depending upon the type of data being collected.	- Provide evidence of audit logs (e.g., security, activity) are maintained and reviewed in a timely manner. - Provide evidence of Log files are sized such that logs are not deleted prior to review and/or being backed up. - Provide evidence of the supplier policy of logs handling. - Provide evidence of Audit logs and log management & analysis tools that are protected from unauthorized access, modification, and deletion. - Provide evidence of Audit records contain appropriate content (e.g., type of event, when the event occurred, where the event occurred, source of the event, and outcome of the event, identity of any individuals or subjects associated with the event).

Control ID	Requirement	Control Guidelines
CT-51	The Supplier must ensure the isolation of tenants. The SABIC's environments/data (specifically virtual server if applicable) must be separated from other customer environments/data hosted at the cloud services provider.	- Provide a document for Implementing network segmentation to isolate tenant environments. Use firewalls, VLANs, or other network security measures to prevent unauthorized access between tenant networks. - Provide a document for isolating computing resources, such as servers, databases, and storage, for each tenant. Ensure that tenants do not share physical or virtual resources to prevent resource contention and unauthorized access. - Provide a document for configuring tenant-specific settings and policies to ensure that each tenant's environment is customized according to their requirements while maintaining isolation from other tenants. - Provide a document for Implementing tenant-specific logging and monitoring to detect and respond to any suspicious activities within each tenant's environment.
CT-52	The Supplier must have the capability to restrict the storage of the customer data to specific countries or geographical locations in compliance with applicable laws and regulations.	- Provide a document for develop clear and documented policies outlining the procedures and criteria for storing customer data in specific countries or regions. Include details on legal requirements, customer consent, and data transfer mechanisms. - The supplier must be aware of and comply with applicable data protection laws, regulations, and international data transfer agreements (such as GDPR in Europe) governing the storage and processing of customer data. - Provide a document for Maintaining a comprehensive data inventory and map customer data to specific countries or geographical locations. Understand the legal requirements associated with data storage in each jurisdiction.
CT-53	The supplier must ensure the implementation of a data loss prevention (DLP) technology.	- Provide evidence of implementation of data loss prevention technology (DLP).
Technology Infrastructure Resilience (PR.IR)		

Control ID	Requirement	Control Guidelines
CT-54	The Supplier must ensure that physical assets are adequately secured and that access to the physical assets as well as SABIC's data is restricted to authorized personnel only. Access in such cases must be documented, and compliant with any applicable legal requirements.	- Provide a document for establishing and enforce access control policies specifying who is authorized to access physical assets and SABIC's data. - Provide a document for implementing physical security measures such as access control systems, security cameras, intrusion detection systems, and secure entry points to safeguard physical assets. - Provide evidence of access is restricted to authorized people. - Provide evidence of control and monitor access points to physical assets, ensuring that entry is limited to authorized personnel only. - Provide evidence of implementation of visitor management system to log and track the entry of external individuals into areas containing physical assets or sensitive data.
CT-55	The Supplier must implement data validation on all input fields for applications or Cloud Services used by SABIC to only accept input with valid data type, syntax, length range, sanitized, accurate, well-formed, and adheres to defined constraints.	- Provide evidence of Test sample input fields for accepting valid data types, syntax and length range part of the user accepting testing. - Provide evidence of Data Validation policy. - Provide evidence of applied configuration.
CT-56	Access to the Internet must be restricted by Content-filtering technologies to block: • malicious and suspicious websites. • personal and non-company email services. • personal and non-company approved public cloud services.	- Provide evidence of the technology used for content filtering. - Provide evidence of no related business site like malicious websites, personal, non-company email Services, non-company approved public cloud services being blocked. - Provide evidence of appropriate configuration for accessing web-based email, cloud Storage services.
CT-57	Physical security procedures defined and followed that address the control of physical access, environmental protection, equipment maintenance, equipment siting, visitor management etc.	- Provide a document for developing access control policies that clearly define who has authorized physical access to facilities and equipment. - Provide documented evidence that demonstrating the implementation of access control mechanisms such as card readers, biometric systems, or access badges to restrict entry to authorized personnel. Use multi-factor authentication where applicable to enhance security. - Provide evidence of the visitor management system that includes check-in and check-out procedures for all visitors. - Provide a document for Implementing environmental controls to safeguard equipment from environmental hazards, including temperature fluctuations, humidity, fire, water leaks, and power surges.

Control ID	Requirement	Control Guidelines
CT-58	Access to sensitive areas (server location, tape library, computer room, etc.) must be physically restricted to authorized personnel only; wherever applicable physical access control must be implemented.	- Provide evidence that physical access to key assets (e.g., server rooms, network closets, zones) are physically restricted: a. Locked doors. b. Surveillance. c. Fences or walls. d. Logs. e. Visitor escorts. - Provide evidence of policies and procedures allow only authorized personnel access to sensitive areas. - Provide evidence of termination /off-boarding procedures to ensure physical access is removed once an employee leaves.
CT-59	The facilities must be protected against fire, water damage, vandalism, and other threats known or likely to occur at their geographical locations.	- Provide documented evidence for conducting a thorough risk assessment to identify potential threats and vulnerabilities specific to the geographical location of the facilities. Consider factors such as natural disasters, criminal activities, and local threats when assessing risks. - Provide documented evidence for Installing fire detection systems, including smoke detectors and fire alarms, throughout the facilities. Implement automatic fire suppression systems such as sprinklers or gas-based suppression systems to contain and extinguish fires promptly. - Provide documented evidence for Implementing measures to prevent water damage, such as waterproofing basements, installing sump pumps, and maintaining drainage systems. Store critical equipment and documents above potential flood levels. - Provide evidence of employing security personnel to monitor the facilities and conduct regular patrols. - Provide evidence of securing the facility perimeter with fencing, gates, and barriers.
CT-60	Facilities and server rooms must be monitored via a Closed-Circuit Television (CCTV) system on a 24/7 basis. All video surveillance data must be protected from unauthorized disclosure and modification and maintained for at least ninety (90) days or otherwise in accordance with the local/regional regulations.	- Provide evidence of an inventory of critical facilities (e.g., data centers, network closets, operations centers, critical control centers). - Provide evidence of physical security monitoring controls are implemented and appropriate to detect potential cybersecurity events (e.g., sign in/out logs, motion detectors, security cameras, security lighting, security guards, door/window locks, automatic system lock when idle, restricted physical access to servers, workstations, network devices, network ports).
CT-61	Uninterruptible Power Supplies (UPS) and surge protector must be used to provide short-term and long-term power when the power fails and to protect information systems from voltage spikes and reductions.	- Provide a document for deploying UPS systems for critical information systems and devices to provide short-term power backup during outages. - Provide evidence of Implementation of redundant UPS units to ensure failover capability in case of UPS failure. - Provide evidence of conducted regular testing and maintenance of UPS units to ensure they are operational. - Provide evidence of configured UPS systems to automatically switch to battery power when a power outage occurs.

Control ID	Requirement	Control Guidelines
CT-62	The Cloud service provider must establish mechanisms to automatically identify equipment using connection authentication (cryptographic based mechanisms that get verified after establishing a connection between the communicating services).	- Provide evidence of Implementation of cryptographic-based authentication mechanisms, such as mutual TLS (Transport Layer Security) or mutual SSL (Secure Sockets Layer), to authenticate equipment and services communicating within the cloud environment. - Provide evidence of utilization of digital certificates to authenticate equipment and services. Ensure that certificates are issued by trusted Certificate Authorities (CAs) and are regularly updated and renewed as needed. - Provide evidence of strong and up-to-date encryption algorithms used to protect authentication mechanisms. - Provide evidence of Implementation of mechanisms for certificate revocation to promptly invalidate compromised or expired certificates.
CT-63	The Supplier must return the SABIC data in a usable format upon service completion.	- Provide a document for defining the acceptable data formats for the return of data, ensuring compatibility with the systems and applications used by the customer. Common formats include CSV, JSON, XML, or database dumps. - Provide a document for Implementing mechanisms to verify the integrity of the returned data to ensure that it has not been tampered with or corrupted during the transfer process. - Provide documented evidence that include comprehensive documentation and metadata with the returned data, explaining the structure, meaning, and context of the data elements. Proper documentation enhances the usability of the data.
CT-64	The Supplier must provide security documentation for any equipment or services under request by SABIC.	- Provide a document for establishing a formal process for requesting security documentation from suppliers. Define the specific types of documentation required, such as security policies, configurations, vulnerability assessments, and incident response plans. - Provide a document for clearly outlining in the supplier contracts and agreements that the supplier must provide relevant security documentation upon request by the organization. Include specific clauses detailing the types of documentation, format, and timeline for submission.
CT-65	The Supplier must use a source code control system that authenticates and logs the team member associated with all changes to the software baseline and all related configuration and build files.	- Provide evidence of different security scans and vulnerability reports found on all developed applications. - Provide evidence of remediation of all security issues and findings discovered and closed prior the deployment in production. - Provide Application Vulnerability scanning policy.

Control ID	Requirement	Control Guidelines
CT-66	Supplier system development environments, including testing environment and integration platforms, must be protected.	- Provide a document for Implementing a strict access controls, ensuring that only authorized personnel have access to development environments. Use role-based access control (RBAC) to restrict permissions based on job roles and responsibilities. - Provide a document that mention securely configure development servers, databases, and other components, following industry best practices and security guidelines. - Provide a document for segment development networks from production and other critical networks. Use firewalls and network security measures to prevent unauthorized access between different environments.
CT-67	The Supplier must use a build process that reliably builds a complete distribution from source. This process must include a method for verifying the integrity of the software delivered to Client, such as signing with a certificate from an industry recognized Certificate Authority.	- Provide a document for Implementing an automated build process that can reliably build a complete distribution from the source code. Automation reduces the risk of human error and ensures consistency in the build output. - Provide evidence that version control system (e.g., Git, SVN) is used to track changes in the source code. Ensure that the build process pulls code from a secure and up-to-date repository to avoid version conflicts and ensure the use of the latest codebase. - Provide evidence of the inclusion of verification steps in the build process to check the integrity of the software. This may involve checksum verification, digital signatures, or other cryptographic methods to ensure that the built software matches the expected output. - Provide evidence of the signed software artifacts using a digital certificate from an industry-recognized Certificate Authority (CA).
CT-68	The Supplier must apply, test, and validate the appropriate patches and updates and/or workarounds on a test version of the application before distribution.	- Provide evidence of patch management policy and procedures. - Provide evidence of on sample of workstations to ensure that OS and software are up to date. - Provide evidence of scheduling and technology used for patch and updates deployment.
CT-69	The Supplier must provide periodic security patches certified by it and upgrades and implementation guidance or recommendations with respect to cybersecurity.	- Provide a document for establishing a regular patch management process to identify, develop, and release security patches for their products and services. Patches should address known vulnerabilities and security weaknesses. - Provide evidence that security patches provided by the supplier must be certified by the supplier itself, indicating that they have been thoroughly tested and validated for effectiveness. - Provide evidence of security patches are compatible with the current version of the product or service.

Control ID	Requirement	Control Guidelines
CT-70	All media must be inventoried and labelled as per the classification level. Inventory audit should be used to avoid unknown or unresolved discrepancies in tape inventories in order to find the information needed to get up and running in the event of a disaster.	- Provide a document for Maintaining a comprehensive inventory of all media, including tapes, disks, and other storage devices used for data backup and recovery purposes. Record details such as serial numbers, date of creation, classification level, and contents. - Provide evidence of labelling all media clearly and visibly with the appropriate classification level (e.g., confidential, restricted, public). - Provide evidence of implementation of strict access controls for media storage areas. Limit access to authorized personnel only and maintain an access log to track who accesses the media and when. - Provide a document for establishing procedures to resolve any unknown or unresolved discrepancies in tape inventories immediately. Investigate the cause of discrepancies, update the inventory records, and take corrective actions to prevent future discrepancies. - Provide evidence of integrated media inventory information into the disaster recovery plan. Include details on where media is stored, how to access it, and the process for recovering data from different types of media.
CT-71	Backup media must be secured to block/inhibit unauthorized physical access.	- Provide evidence of backup media physical security controls implemented. - Provide evidence of backup media related policy and configuration.
CT-72	Supplier must establish and follow regular procedures for backup of critical systems and SABIC's data, software, and websites.	- Provide a document for developing a comprehensive backup policy outlining the frequency of backups, types of data to be backed up, retention periods, and the backup methods to be employed. - Provide evidence of Identification and prioritization of critical systems, applications, databases, and websites. Ensure that backups are performed for all critical components necessary for business operations. - Provide a document for establishing a regular backup schedule based on the criticality of the systems and data. Conduct backups daily, weekly, or as per business requirements to minimize data loss in the event of a disaster. - Provide evidence that utilize a combination of full, incremental, and differential backup methods based on the data volume and recovery time objectives (RTO). Implement offsite or cloud-based backups for redundancy and disaster recovery purposes.
CT-73	Backup stored at an off-site location must be encrypted using at least AES encryption algorithm, and 128 bits key.	- Provide evidence of supplier backup policy, process and procedures. - Provide evidence of the backup tapes are encrypted for off-site location. - Provide evidences of the type of encryption applied.

Control ID	Requirement	Control Guidelines
CT-74	Clear desk and clear screen policy must be enforced in the organization.	- Provide training and awareness programs to educate employees about the clear desk and clear screen policy. Ensure that employees understand the importance of the policy in safeguarding sensitive data. - Encourage employees to store sensitive documents and materials in secure cabinets or lockable drawers when not in use. Avoid leaving confidential information exposed on desks or in open areas. - Require employees to enable automatic screen locking mechanisms on their computers. Screens should lock after a specified period of inactivity, requiring a password or authentication to access the system again.
CT-75	The Supplier must monitor Technology Assets, Systems, and applications to identify unauthorized access, or unauthorized activity.	- Provide evidence of policies and procedures regarding system and network monitoring. - Provide evidence of detected events (e.g., alerts from IDS) and the organization's response to them. - Provide evidence of reviews for the events and responses to ensure thorough analysis of detected events is performed.
CT-76	The Supplier must conduct an analysis of software errors, most common programming errors, vulnerabilities, risks a threat as early as possible during the software lifecycle. The Supplier must share with SABIC all security-relevant information regarding the vulnerabilities, risks, threats, and mitigated steps taken.	- Provide evidence of error messages handling part of the application design document. - Provide evidence of samples of error messages generated by the application. - Provide evidence of the login failure for username and password. The error messages. - Provide evidence of Secure Programming Policy.
CT-77	The Supplier must ensure that errors and events within the application that may be the result of failures, crashes, unauthorized access attempts or other indicators of potential compromise, are appropriately recorded in a log file conforming to industry standards.	- Provide evidence of Test sample input fields for accepting valid data types, syntax and length range part of the user accepting testing. - Provide evidence of Data Validation policy. - Provide evidence of applied configuration.
CT-78	The Supplier must perform security scans (with the most current signature files) to verify that the system has not been compromised during the testing phase or it has open vulnerabilities. The Supplier must provide to SABIC written documentation of the results of the scans and tests it has performed along with a mitigation plan. These vulnerabilities must be mitigated within a pre-negotiated period.	- Provide a document for conducting regular security scans using the most current signature files to identify vulnerabilities and security weaknesses in the system. Scans should be performed at defined intervals or after significant system changes. - Provide evidence that security scans cover all components of the system, including applications, operating systems, databases, network devices, and configurations. Perform scans on both internal and external network segments. - Provide evidence of conducted authentication testing during security scans to identify vulnerabilities related to weak or default credentials, improper access controls, or authentication bypass issues. - Provide a document for sharing regular reports summarizing the findings of security scans, including identified vulnerabilities, their severity levels, and actions taken for remediation. Reports should be detailed and easy to understand.

Control ID	Requirement	Control Guidelines
CT-79	All physical access control logs periodically reviewed and retained as per retention requirements.	- Provide evidence of an inventory of critical facilities (e.g., data centers, network closets, operations centers, critical control centers). - Provide evidence of physical security monitoring controls are implemented and appropriate to detect potential cybersecurity events (e.g., sign in/out logs, motion detectors, security cameras, security lighting, security guards, door/window locks, automatic system lock when idle, restricted physical access to servers, workstations, network devices, network ports).
CT-80	Systems' logs and critical files must be protected from unauthorized access, tampering, illegitimate modification and/or deletion.	- Provide evidence of implementing secure measures to protect systems' logs and critical files from unauthorized access, tampering, illegitimate modification and/or deletion.
CT-81	Records kept of all suspected or actual faults and all maintenance activities performed on equipment's Is the maintenance must be carried out by authorized personnel only.	- Provide a document for maintaining detailed records of all suspected or actual faults, issues, and maintenance activities performed on equipment. Records should include the nature of the fault, actions taken for resolution, date and time of maintenance, and the personnel involved. - Provide evidence that maintenance activities are carried out exclusively by authorized and trained personnel. Define clear roles and responsibilities for authorized maintenance staff and restrict access to equipment to prevent unauthorized tampering.
DETECT		
Continuous Monitoring (DE.CM)		
CT-82	The remediation of newly discovered critical vulnerabilities presenting significant risks must be performed in a timely manner: • Critical Risk: immediate correction up to fourteen (14) calendar days of critical vendor patch release, notification from SABIC, or discovered security breach whichever is earlier. • High Risk: within one (1) month of vendor patch release or discovered security breach whichever is earlier. • Medium and Low Risk: within three (3) months of discovery.	- Provide evidence of the remediated critical vulnerabilities presenting significant risks immediately, within fourteen (14) calendar days of any of the following events, whichever occurs earlier: a. Receipt of a critical vendor patch release. b. Notification from SABIC regarding the vulnerability. c. Discovery of a security breach related to the vulnerability. - Provide evidence of the remediated high-risk vulnerabilities within one (1) month of any of the following events, whichever occurs earlier: a. Vendor patch release addressing the high-risk vulnerability. b. Discovery of a security breach related to the vulnerability. - Provide evidence of the remediated medium and low-risk vulnerabilities within three (3) months of their discovery. This provides a reasonable timeframe to address less critical vulnerabilities while ensuring they are resolved in a timely manner. - Provide evidence of the established communication protocol to receive notifications about critical and high-risk vulnerabilities from vendors, security researchers, or internal sources promptly.

Control ID	Requirement	Control Guidelines
CT-83	The supplier must be continuously monitoring cybersecurity events through a security incident and event management process.	- Provide evidence of implementation of robust Security Incident and Event Management (SIEM) solution capable of aggregating, correlating, and analyzing security events and logs from various sources within their environment. - Provide evidence of configured SIEM to provide real-time monitoring of security events, enabling immediate detection of suspicious activities, unauthorized access attempts, and potential security breaches. - Provide evidence of logs from network devices, servers, applications, and security appliances are collected and analyzed by the SIEM solution. Logs should include relevant information for security analysis and incident response. - Provide evidence of Implementation of anomaly detection mechanisms within the SIEM to identify deviations from normal network and user behavior patterns. Unusual activities, such as large data transfers or multiple failed login attempts should trigger alerts.
Adverse Event Analysis (DE.AE)		
CT-84	Suppliers must periodically aggregate and correlate data from multiple systems and critical applications such as Firewalls, IDS/IPS, and anti-virus in a central repository for event monitoring and analysis purposes.	- Provide evidence of listing of event aggregation and monitoring systems in use at the organization (e.g., SIEMs, event log correlation systems). - Provide evidence of list of sources that provide data to each event aggregation and monitoring system (e.g. firewalls, routers, servers).
CT-85	The Supplier must have a Disaster Recovery Plan (DR Plan) which is documented, maintained, tested, and communicated to appropriate parties. The DR Plan should address the recovery of Assets and communications following a major disruption to business operations.	- Provide evidence of Disaster Recovery plans addressing the control requirements. - Provide evidence of samples of communicating DR to responsible parties and stakeholders. - Provide evidence the DR plan is tested regularly.
RESPOND		
Incident Management (RS.MA)		
CT-86	The Supplier must have security mechanisms in place to achieve resilience requirements in normal and adverse situations and ensure high availability of its services. This includes having sufficient capacity available.	- Provide evidence of data center tier rating. - Provide evidence of and high-availability of service fail over. - Provide evidence that the third party is deploying Distributed Denial of Service (DDOS) protection appliance that sit in front of network firewalls. - Provide evidence that the third party is deploying web application firewalls, and use load balancers.

Control ID	Requirement	Control Guidelines
CT-87	Procedures for the backups of the provisioned solution and SABIC's data must be established, conducted, maintained, and tested on a regular basis. SABIC can define more specific requirements for backup in the Scope of Work.	- Provide a document for developing a comprehensive backup policy that outlines the procedures, frequency, and methodologies for backing up the provisioned solution and SABIC's data. - Ensure that backup procedures comply with any specific requirements defined by SABIC in the Scope of Work (SOW). - Define backup frequency based on the criticality of data and the acceptable level of data loss. - Provide a document for establishing a data retention policy specifying the duration for which backups will be retained. - Provide evidence of periodic backup testing is performed to verify data are accessible and readable.
Incident Response Reporting and Communication (RS.CO)		
CT-88	Supplier must have an Incident Response capability that includes preparation, detection and analysis, containment, eradication, recovery, documentation and preservation of evidence, communication protocols and lessons learned.	- Provide evidence of the incident response plan to determine if appropriate steps are taken consider the following: a. Obtain evidence of event notifications (e.g., detection alerts, reports) from different systems. b. Determine who receives alerts or reports from detection systems and what actions are taken once reports are received. c. Review the incident response plan to determine if actions taken follow the plan. d. Steps to contain and control the incident to prevent further harm. e. Procedures to notify potentially impacted Suppliers. f. Strategies to control different types of incidents (e.g., distributed denial-of-service [DDoS], malware, etc.) g. Steps to mitigate the incident to prevent further harm. h. Review any documented incidents to determine whether mitigation efforts were implemented and effective. - Provide evidence of reviewal the organization's incident handling reports and incident testing documentation for action items and lessons learned.
CT-89	Documented Security Incident Response process covering physical security incidents	- Provide evidence of the incident response plan to determine if there is a process to formally analyze and classify incidents based on their potential impact. - Provide incident response plan to determine if it is designed to prioritize incidents, enabling a rapid response for significant incidents or vulnerabilities.

To be certified to provide cloud services or outsourcing and manage services to SABIC Saudi-Based departments or Affiliates the Supplier shall comply with the additional requirements included in the below table."

Control ID	Requirement	Controls Requirements
CT-90	The Cloud Services provider must host and storage SABIC´s information originated or owned by Saudi-Based departments or affiliates inside the Kingdom of Saudi Arabia.	- Provide a document for establishing a data localization policy specifying that all information originated or owned by Saudi-Based departments or affiliates must be hosted and stored within the Kingdom of Saudi Arabia. - Provide evidence that the data localization policy aligns with relevant laws, regulations, and data protection requirements in Saudi Arabia. - Provide evidence of the inclusion of explicit clauses in the service level agreements (SLAs) and contracts with the cloud service provider stating the requirement to host and store data within the Kingdom of Saudi Arabia. - Provide evidence of physical location of the data centers used by the cloud service provider is inside the Kingdom of Saudi Arabia.
CT-91	The Cloud Services provider must fulfill NCA's requests to remove software or services, provided by third-party providers that may be considered a cybersecurity threat to national organizations, from the marketplace provided to SABIC.	- Provide a document for developing a clear policy outlining the procedures for responding to requests from NCAs to remove software or services. Define the criteria for identifying cybersecurity threats and the escalation process for handling such requests. - Provide a document for Implementing a robust threat assessment mechanism to evaluate software or services flagged as potential cybersecurity threats. This mechanism should involve cybersecurity experts and threat intelligence analysis to assess the validity of the NCA's concerns.
CT-92	**If SABIC´s information originated or owned by Saudi-Based classified by SABIC as critical** is involved in the cloud service: The Cloud services provider must be following NCA's Cloud Cybersecurity Controls (CCC).	- Provide evidence of alignment of internal policies, procedures, and security practices with NCA's Cloud Cybersecurity Controls to ensure compliance with the specified security standards and requirements. - Provide evidence of design and architecture of cloud services adhere to the specifications outlined in NCA's Cloud Cybersecurity Controls. - Provide evidence of Implementation of the necessary technical configurations and security features recommended by the NCA.
CT-93	**If SABIC data or systems classified by SABIC as critical** is involved in the service: Outsourcing services must rely on Saudi companies and organizations, in accordance with the relevant legislative and regulatory requirements.	- Provide evidence of compliance with all relevant legislative and regulatory requirements related to outsourcing services to Saudi companies and organizations. - Provide a document for establishing vendor selection criteria that prioritize Saudi companies and organizations. - Provide evidence that specify the preference for sourcing goods, services, and labor locally within contracts and procurement agreements. Encourage and support the use of local suppliers and service providers.

Control ID	Requirement	Controls Requirements
CT-94	Cybersecurity managed services centers for monitoring and operations must be completely present inside the Kingdom of Saudi Arabia.	- Provide evidence that the cybersecurity managed services centers for monitoring and operations are physically located within the Kingdom of Saudi Arabia. This information should be clearly stated in contracts and agreements. - Provide evidence that the physical presence of the centers complies with data sovereignty regulations in Saudi Arabia, ensuring that sensitive data and information remain within the country's borders as required by law.
CT-95	**If a hosted telework system is provided to Saudi-Based SABIC systems,** it must be inside the Kingdom of Saudi Arabia.	- Provide evidence that the hosted telework system is physically located within the Kingdom of Saudi Arabia. This information should be clearly stated in contracts and agreements. - Provide a document for ensuring that the physical presence of the telework system complies with data sovereignty regulations in Saudi Arabia, ensuring that sensitive data and information remain within the country's borders as required by law. - Provide evidence of upholding strict data privacy and confidentiality standards within the hosted telework system. Ensure that user data is handled with the utmost care and in compliance with applicable privacy regulations.

7. REFERENCE

- National Institute of Standards and Technology Cybersecurity Framework (NIST CSF 2.0)
- National Cybersecurity Authority (Cloud Cybersecurity Controls (CCC) – 1: 2020)

8. APPENDIX A - CYBERSECURITY INCIDENT RESPONSE INSTRUCTIONS

The Supplier, in case of suffering any adverse situation or Cybersecurity incident in its environment, affecting any networks, systems or applications that process, access, or store SABIC's data, shall follow these basic instructions:.

Verify and identify :

- Supplier will verify received Incident alert and determine impact.
- If the incident affects any networks, systems or applications that process, access, or store SABIC's data, the Supplier must notify and report the incident to SABIC.
- The notification must be made as soon as practicable, but no later than twenty-four (24) hours.
- The Supplier must make the notification to SABIC using the following channel:
    - Email: CyberSecurityCenter@SABIC.COM
- Supplier can notify the incident additionally via a call through the following hotline number [+966556900971 OR +966133455080].
- SABIC will evaluate received notification and perform protection actions to protect SABIC, if required.
- SABIC will provide Supplier with details of protection action taken by SABIC.

Contain, Eradicate and Recover

- Supplier will build containment, eradication and recovery plan to mitigate incident.
- In case the incident is impacting SABIC data or services, the Supplier will provide plan progress report every 24 hours to SABIC/SOC.

Post-incident

- Supplier will provide final report to SABIC include RCA (root cause analysis) and remediation plan.
- SABIC will review and evaluate provided reports from third party to get back to normal operation.