CYBERSECURITY
COMPLIANCE
CERTIFICATION

Third-Party Cybersecurity Standard SACS-210

February 2026

Table of Contents

1. Purpose

The Third Party Cybersecurity Standard (TPCS) sets forth the minimum requirements for third parties to protect confidentiality, Integrity and availability of data and Information systems. TPCS aims to effectively protect corporate Assets and Critical Facilities that are accessed, processed, communicated to, or managed by third parties through providing the required cybersecurity controls. It is the responsibility of the Third Party to meet the requirements of this Standard as applicable. The Third Party must ensure any subcontractors supporting the contracted work adhere to the applicable cybersecurity and data privacy requirements within this Standard.

2. Scope

This Standard applies to all third parties engaging with the corporation where the Third Party:

- Processes, transmits or stores corporate information and personal data.
- Has access to a corporate information endpoint (computer or server).
- Provides off-the-shelf / customized technical products (applications/software) for the corporation's use.
- Has a connection to the corporate network.
- Provides consultancy services for high-sensitivity strategic projects at the national level.

3. Third Party Classification

- General Requirement:

Includes the minimum cybersecurity controls that third parties must implement, regardless of their services or access levels, to ensure basic protection of the company data and systems. Covers governance, access management, password policies, multi factor authentication, data security (antivirus, system updates), user training, and CCC certification.

- Network Connectivity:

The Third Party's computing infrastructure is provided with network connectivity to proponent network to access intranet services via leased lines or VPN solutions (e.g., SSL VPN, site-to-site VPN).

- Outsourced & Managed Services:

The Third Party is providing, managing, maintaining and/or supporting outsourced infrastructure and/or managed services, that is owned by the corporation. (e.g., data centers, co-location centers, and backup centers).

- Critical Data Processor:

The Third Party is developing, accessing, and/or processing confidential data with access to the company.

- Software Services:

The Third Party is developing and/or hosting a customized software, application, website, or solution.

- Cloud Computing:

The Third Party provides cloud computing services:

- IaaS (Infrastructure),
- PaaS (Platform),
- SaaS (Software).

- Operation Technology:

The Third Party is involved in the design, development, supply, integration, operation, and maintenance of Operational Technology (OT) products and systems play a critical role in supporting essential industrial processes. These entities provide a wide range of services and solutions, including the engineering, testing, and ongoing support of OT infrastructure. This includes:

- Key systems and components:

  - Distributed Control Systems (DCS)
  - Supervisory Control and Data Acquisition (SCADA) systems
  - Safety Instrumented Systems (SIS)
  - Controllers, Remote Terminal Units (RTUs)
  - Programmable Logic Controllers (PLCs)
  - Human-Machine Interfaces (HMIs)
  - Communication modules
  - Embedded software and firmware

- Lifecycle Services:

The Third Party is involved in providing lifecycle services such as:

- System engineering and configuration
- Commissioning
- Factory Acceptance Testing (FAT)
- Site Acceptance Testing (SAT)
- Operations and Maintenance (O&M)

4. Change Control

Changes made to the standard documentation will be highlighted using the following labeling scheme.

Status	Name	Description
	Modified	An existing requirement which has been modified.
	New	A new requirement introduced in this release.
	Regulatory requirement	A requirement mandated by a regulatory body in the Kingdom of Saudi Arabia.

5. Policy Deviation

In the event of a conflict between this document and that of higher priority (e.g., national regulations, corporate policies, general instructions), the document with higher priority must take precedence. In the event compliance with security requirements is not feasible, policy waiver must be requested and processed by their local governing entities.

6. The Third Party Cybersecurity Requirements

- General Requirements:

Third parties must comply with all controls specified in this section.

GOVERN	
Organizational Context	
TPC1.1 	The Third Party must ensure legislative and regulatory compliance, which should include, as a minimum, continuous compliance with all laws, regulations, instructions, decisions, regulatory frameworks and controls, and mandates regarding cybersecurity and data privacy in KSA and/or other applicable national regulations.
Policy	
TPC1.2 	The Third Party must develop, approve and communicate an Acceptable Use Policy (AUP).
TPC1.3 	Third Party must establish, maintain, and communicate Cybersecurity Policies and Standards that include, at minimum, the following: a) asset management; b) access management; c) physical security; d) secure disposal of media/sanitization of data; e) classification and handling of assets and data; f) incident management; g) vulnerability and patch management; h) business continuity and disaster recovery.

TPC1.4	The Third Party must have formal documented process for onboarding employees (i.e., conducting background checks) and offboarding employees (i.e. return of assets and removal of access rights).
Cybersecurity Supply Chain Risk Management	
TPC1.5	The Third Party must obtain a Cybersecurity Compliance Certificate (CCC), or approved certificate, from authorized audit firms in accordance with the requirements set forth in this Standard. Third Parties must submit the CCC to proponent through the established process.
TPC1.6	The Third Party must renew the CCC (or approved certificate) before it expires.
TPC1.7	Proponent data must only be shared with individuals who are part of the work specified in the contract.
IDENTIFY	
Asset Management	
TPC1.8	Third Party must have an effective mechanism to maintain an inventory of all information and technology assets, ensuring visibility and accuracy across all technical assets.
PROTECT	
Identity Management, Authentication, and Access Control	
TPC1.9	User authorizations to information technology systems and applications must be managed via a centralized corporate identity and access management solution. Authorizations must be based on: a) identity; b) access control principal — need-to-know and need-to-use basis; c) least privilege and segregations of duties.
TPC1.10	User authentication must be granted based on unique authentication credentials.
TPC1.11	The following rules must be used for password and authentication code management (where feasible): a) using long passwords or passphrases that are 8 – 64 characters in length; b) containing lower case characters a-z; c) containing upper case characters A-Z; d) containing digits 0-9; e) containing special characters (e.g.! @ # $ % ^ & *, etc.); f) using multi-factor authentication (MFA) mechanism; g) not providing password hints.
TPC1.12	Multi-factor authentication must be enforced on: a) remote access (including access from the Internet); b) access to cloud services; c) access to company email through web/mobile devices; d) access to internet facing applications; e) users with privileged accounts.

TPC1.13	Single sign-on can be used but must be coupled with MFA upon initial login to a system.
TPC1.14	Third Party must review user accounts and access rights at least annually.
TPC1.15	All Third Party technology assets must be authenticated using secure authentication mechanisms.
Data Security	
TPC1.16	All proponent data must be securely returned to the proponent and then deleted from all technology assets at the end of the data life cycle or designated retention period (including backups).
TPC1.17	Technology assets must be securely disposed at the end of their lifecycle (e.g., loaned, donated, destroyed, transferred or surplused) in accordance with applicable legislative requirements and industry best practices.
TPC1.18	The Third Party must encrypt data at rest and in transit using technical mechanisms and cryptographic primitives for strong encryption, in accordance with the advanced level in the KSA National Cryptographic Standards (NCS-1:2020) and industry-approved encryption algorithms.
TPC1.19	The Third Party must restrict and secure the use of external storage media.
TPC1.20	The Third Party must implement Sender Policy Framework (SPF), Domain Message Authentication Reporting (DMARC) and DomainKeys Identified Mail (DKIM) technology on the mail server.
TPC1.21	The Third Party must inspect all incoming emails originating from the Internet using anti-spam protection.
TPC1.22	The Third Party must inspect all email attachments with signature analysis before allowing the attachments.
TPC1.23	The Third Party must use a private email domain. Generic public domains, such as Gmail and Hotmail, must not be used.
TPC1.24	The Third Party must ensure that Microsoft Office macros in any files originating from external sources (such as internet downloads and email attachments) are automatically blocked.
TPC1.25	The Third Party must synchronize all technology assets with an authorized time source e.g., NTP server.
TPC1.26	Event logs must be protected from alteration, disclosure, destruction, and unauthorized access and unauthorized release.
Platform Security	
TPC1.27	Firewalls must be configured and enabled on all endpoint devices.
TPC1.28	The Third Party must inspect all HTTP and HTTPS traffic from Internet facing (External) applications using Web Application Firewall (WAF).

TPC1.29	Third Party technology assets must be protected with signature-based up-to-date virus and malware protection software.
TPC1.30	Before implementation to the production environment, security patches must be tested or have measures implemented to ensure back-out or recovery is possible.
DETECT	
Continuous Monitoring	
TPC1.31	Audit and cybersecurity event logs must be activated on information systems and applications. Logs must capture at minimum the events stated in Appendix C.
RESPOND	
Incident Management	
TPC1.32	If the Third Party discovers a Cybersecurity Incident, The Third Party must (besides its continuous efforts to resolve and mitigate the Incident): a) Notify proponent within 24 hours of discovering the Incident; b) Follow the Cybersecurity Incident Response Process set forth in Appendix A.
TPC1.33	Third party must notify proponent when the Third Party's employees provided with proponent user credentials no longer requires access. This includes employees being transferred, re-assigned, retired, or no longer associated with the Third Party.

- Specific Requirements

Third parties that fall under one or multiple classes, need to comply with the applicable requirements.

CNTL No.	Control Name	Network Connectivity	Outsourced & Managed Services	Critical Data Processor	Customized Software	Cloud Computing Service	Operational Technology
GOVERN							
Risk Management Strategy							
TPC-2.1	Cybersecurity risk management methodology and procedures must be defined, documented and approved.	✓	✓	✓	✓	✓	✓
TPC-2.2	Cybersecurity risk management methodology and procedures must be implemented.	✓	✓	✓	✓	✓	✓
TPC-2.3	Cybersecurity risk management methodology and procedures must be reviewed periodically according to planned intervals or upon changes to related laws and regulations. Changes and reviews must be approved and documented.	✓	✓	✓	✓	✓	✓

CNTL No.	Control Name	Network Connectivity	Outsourced & Managed Services	Critical Data Processor	Customized Software	Cloud Computing Service	Operational Technology
TPC-2.4	Cybersecurity risk management methodology must include: a) Defining acceptable risk levels for the cloud services, and communicating them to the CST if they are related to the CST; b) Considering data and information classification, as part of Risk management methodology; c) Developing cybersecurity risk register for cloud services, and monitoring it periodically according to the risks.					✓	
Oversight							
TPC-2.5	The Third Party must measure and monitor cybersecurity incident metrics and ensure compliance with contracts and legislative requirements.	✓	✓	✓	✓	✓	✓
Roles, Responsibilities, and Authorities							
TPC-2.6	The Third Party must ensure well-defined ownership for cryptographic keys.	✓	✓	✓	✓	✓	✓
TPC-2.7	The Third Party must have employee(s) whose primary responsibility is Cybersecurity. Responsibilities must include maintaining the security of information systems and ensuring compliance with existing policies.	✓	✓	✓	✓	✓	✓
TPC-2.8	Prior and during the professional relationship of personnel, the Third Party must cover: a) Positions of cybersecurity functions in CSP's data centers within the KSA must be filled with qualified and suitable Saudi nationals; b) Screening or vetting candidates of personnel working inside KSA who have access to Cloud Technology Stack, periodically; c) Cybersecurity policies as a prerequisite to access to Cloud Technology Stack, signed and appropriately approved.					✓	
Cybersecurity Supply Chain Risk Management							
TPC-2.9	The Third Party must integrate third-party cybersecurity risks into its overall risk management and governance framework.	✓	✓	✓	✓	✓	✓
TPC-2.10	Cloud Service Provider's data center must be certified and/or have an audit report against industry recognized standard / authority.					✓	

CNTL No.	Control Name	Network Connectivity	Outsourced & Managed Services	Critical Data Processor	Customized Software	Cloud Computing Service	Operational Technology
TPC-2.11	The Third Party's cloud service providers must provide proponent evidence of secure data storage processes, procedures, and technologies to comply with related legal and regulatory requirements.					✓	
TPC-2.12	The Third Party must have a process in place to guarantee that a nondisclosure agreement between the Third Party and its contracted employees is signed before access to proponent systems and/or premises is granted.	✓	✓	✓	✓	✓	✓
IDENTIFY							
Asset Management							
TPC-2.13	The Third Party must identify assets owners and involve them in the asset management lifecycle.	✓	✓	✓	✓	✓	
TPC-2.14	The Third Party must have an inventory of all end users and mobile devices.			✓		✓	✓
Risk Assessment							
TPC-2.15	The Third Party must have a process to conduct cybersecurity risk assessments on regular basis, to identify, assess and remediate Risks to data and information systems.	✓	✓	✓	✓	✓	✓
TPC-2.16	The Third Party must be subscribed in authorized and specialized organizations and groups to stay up-to-date on cybersecurity threats, common practices and key know-how.					✓	✓
PROTECT							
Identity Management, Authentication, and Access Control							
TPC-2.17	Users with remote access to systems must be documented and approved.	✓	✓	✓	✓	✓	✓
TPC-2.18	Remote access from the internet must not be allowed unless it's explicitly approved, restricted, and controlled.	✓	✓	✓	✓	✓	✓
TPC-2.19	The Third Party must be capable to immediately interrupt a remote access session and prevent any future access for a user.	✓	✓	✓	✓	✓	✓
TPC-2.20	Identity and access management of generic accounts credentials for accountability must not be assigned for a specific individual.	✓	✓	✓	✓	✓	✓

CNTL No.	Control Name	Network Connectivity	Outsourced & Managed Services	Critical Data Processor	Customized Software	Cloud Computing Service	Operational Technology
TPC-2.21	The Third Party must mask displayed authentication inputs, especially passwords, to prevent shoulder surfing.					✓	
TPC-2.22	The Third Party must restrict and control access to storage systems (such as Storage Area Network (SAN)).					✓	
TPC-2.23	The Third Party must implement access control between different network segments.					✓	
TPC-2.24	Access to the Internet must be restricted by content-filtering technologies to block: a) Malicious and suspicious websites; b) Personal and non-company approved public cloud services.	✓	✓	✓	✓	✓	✓
TPC-2.25	Access to critical areas within the organization (e.g., data center, Cloud Technology Stack, disaster recovery center, sensitive information processing facilities, security surveillance center, network cabinets) must be restricted and limited to authorized personnel only.	✓	✓	✓	✓	✓	✓
Awareness and Training							
TPC-2.26	The Third Party must require all information system users to take a yearly mandatory cybersecurity training that covers the following, including but not limited to: a) Acceptable use and good computing practices; b) Responding to cybersecurity incidents, in line with their roles and responsibilities; c) Mobile device security; d) Data classification and handling requirements.	✓	✓	✓	✓	✓	✓
TPC-2.27	The Third Party must support identity federation services.	✓			✓	✓	
Data Security							
TPC-2.28	Encryption key management capability, including preservation and retrieval, must be defined, applied, and reviewed.	✓		✓		✓	✓
TPC-2.29	The Third Party must logically (e.g., partitioning a physical drive) and/or physically segregate proponent data-at-rest from the data of other clients or customers.	✓	✓	✓	✓	✓	
TPC-2.30	The Third Party 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.			✓		✓	

CNTL No.	Control Name	Network Connectivity	Outsourced & Managed Services	Critical Data Processor	Customized Software	Cloud Computing Service	Operational Technology
TPC-2.31	The Third Party must implement data validation on all input fields for applications or Cloud Computing Services used by the proponent to only accept input with valid data type, syntax, and length range.				✓	✓	
TPC-2.32	The Third Party must securely handle proponent data found in the audit trails and cybersecurity event logs.					✓	
TPC-2.33	Data Leakage Prevention (DLP) policies must be established, and DLP solutions must be configured to monitor and control the exfiltration of sensitive data from the network.	✓	✓	✓	✓	✓	✓
TPC-2.34	The Third Party must prohibit the use of Cloud Technology Stack's data in any environment other than production environment, except after applying strict controls for protecting that data, such as: data masking or data scrambling techniques.					✓	
TPC-2.35	The Third Party must utilize secure methods and algorithms for saving and processing passwords, such as secure hashing functions.	✓	✓	✓	✓	✓	✓
TPC-2.36	The Third Party must regularly backup corporate data.	✓	✓	✓	✓	✓	
TPC-2.37	Backup data stored at an off-site location must be encrypted.	✓	✓	✓	✓	✓	
TPC-2.38	The Third Party must fulfill NCA's requests to remove software or services, that may be considered a cybersecurity threat to national organizations, from the marketplace provided to CSTs.					✓	
TPC-2.39	The Third Party must secure access, storage and transfer of the following: a) Proponent data; b) Cloud Technology Stack backups and their mediums, and protect them against damage, amendment or unauthorized access.					✓	
TPC-2.40	The Third Party must provide proponent with secure means to export and transfer data and virtual infrastructure.			✓		✓	✓
TPC-2.41	The Third Party must ensure that the security functions within the cloud technology stack is fully isolated from other operations within the stack.					✓	

CNTL No.	Control Name	Network Connectivity	Outsourced & Managed Services	Critical Data Processor	Customized Software	Cloud Computing Service	Operational Technology
TPC-2.42	The Third Party must ensure community cloud services provided to proponent are fully isolated from cloud services offered to external entities.					✓	
TPC-2.43	The Third Party must protect data transmitted through the network; from and to the Cloud Technology Stack network using cryptography primitives; for management and administrative access.					✓	
TPC-2.44	The Third Party must use certificates that are securely issued by an approved certification authority.				✓	✓	✓
TPC-2.45	The Third Party must have data sanitation and secure disposal for end-user devices.	✓	✓	✓		✓	✓
Platform Security							
TPC-2.46	Firewalls must be implemented at the network perimeter, and only required services must be allowed.	✓	✓	✓	✓	✓	✓
TPC-2.47	Intrusion Prevention Systems (IPS) must be implemented at the network perimeter.	✓	✓	✓	✓	✓	✓
TPC-2.48	Intrusion Prevention Systems (IPS) must be updated to the latest signature.	✓	✓	✓	✓	✓	✓
TPC-2.49	Servers and workstations subnets must be segmented and access between them restricted and monitored.	✓	✓	✓	✓	✓	✓
TPC-2.50	Servers accessible from the internet must be placed in a DMZ (i.e., perimeter network) with restricted access to internal subnets.	✓	✓	✓	✓		✓
TPC-2.51	Denial of service protection must be implemented on all internet-facing services. This should include Distributed Denial of Service (DDoS).				✓	✓	✓
TPC-2.52	The Third Party must protect the Cloud Technology Stack network and isolate the network from other internal and external networks.					✓	
TPC-2.53	The Third Party must isolate cloud service delivery network, cloud management network and CSP enterprise network.					✓	

CNTL No.	Control Name	Network Connectivity	Outsourced & Managed Services	Critical Data Processor	Customized Software	Cloud Computing Service	Operational Technology
TPC-2.54	The Third Party must detect and prevent unauthorized changes to software and systems, and employ modern technologies such as Endpoint Detection and Response (EDR) to ensure information processing systems are ready for rapid incident response.			✓	✓	✓	✓
TPC-2.55	The Third Party must consider cybersecurity requirements of the Cloud Technology Stack and relevant systems in the design and implementation of the cloud computing services.					✓	
TPC-2.56	Audit logs and cybersecurity event logs from information systems and applications storing, processing, or transmitting client organization data must be retained for a minimum of one (1) year.	✓	✓	✓	✓	✓	✓
TPC-2.57	Sessions must be encrypted (e.g., using HTTPS), and session authentication, lockout, and timeout must be enforced.	✓	✓	✓	✓	✓	✓
TPC-2.58	IPsec tunnels must utilize IKEv2 with certificate-based authentication.	✓	✓	✓	✓	✓	
TPC-2.59	The Third Party cybersecurity requirements must include at least the following: a) Logical or physical segregation and segmentation of network segments using firewalls and defense-in-depth principles; b) Secure browsing and Internet connectivity including restrictions on the use of file storage/sharing and remote access websites, and protection against suspicious websites; c) A comprehensive risk assessment and management exercise must be conducted to assess and manage the cyber risks prior to connecting any wireless networks to the organization's internal network; d) Management and restrictions on network services, protocols and ports; e) Security of Domain Name Service (DNS); f) Secure management and protection of Internet browsing channel against Advanced Persistent Threats (APT), which normally utilize zero-day viruses and malware.	✓	✓	✓	✓	✓	✓

CNTL No.	Control Name	Network Connectivity	Outsourced & Managed Services	Critical Data Processor	Customized Software	Cloud Computing Service	Operational Technology
TPC-2.60	The Third Party must apply network segregation between production, test and development environments.	✓			✓		
TPC-2.61	The Third Party must protect system development environments, testing environments (including data used in testing environment), and integration platforms.				✓	✓	✓
TPC-2.62	The Third Party must create and manage baseline configurations to harden information systems based on vendor recommendation and best practices.	✓	✓	✓	✓	✓	✓
TPC-2.63	The Third Party must adopt the multi-tier architecture principle.	✓	✓		✓	✓	
TPC-2.64	Backup media must be secured to prevent unauthorized physical access.	✓	✓	✓	✓	✓	
TPC-2.65	Multiple physical security measures must be implemented to prevent unauthorized access to facilities.	✓	✓	✓	✓	✓	✓
TPC-2.66	Visitors' management process must be defined and implemented.	✓	✓	✓	✓	✓	✓
TPC-2.67	All visitors accessing critical facilities must be escorted.	✓	✓	✓	✓	✓	✓
TPC-2.68	All systems (routers, switches, servers, and firewalls) must be housed in a secure area (e.g., communication room) with controlled access.	✓	✓	✓	✓	✓	✓
TPC-2.69	If the Third Party works on high-sensitivity projects at the national level and if the project contains sensitive data, the Third Party must: a) Have a dedicated closed room for employees to perform their work; b) Only allows individuals with authorized access into the closed room mentioned; c) Prevent the entry of non-authorized electronic devices; d) Prevent the carrying out of devices, storage media and documents outside of the room.		✓	✓			✓
TPC-2.70	Third Party must have: a) Centralized mobile device security management (MDM); b) Screen locking for end user devices.			✓		✓	✓

CNTL No.	Control Name	Network Connectivity	Outsourced & Managed Services	Critical Data Processor	Customized Software	Cloud Computing Service	Operational Technology
TPC-2.71	The Third Party must follow OWASP best practices when developing software/applications for proponent.	✓	✓	✓	✓	✓	✓
TPC-2.72	The Third Party must regularly provide certified security patches, system upgrades, and implementation guidance or recommendations related to cybersecurity.				✓		✓
TPC-2.73	Application Programming Interface (API) must be secured using the steps below. a) input validation; b) use tokens; c) use encryption and signatures; d) use quotas and throttling (where applicable); e) be behind an API gateway (if accessed remotely).				✓	✓	
TPC-2.74	APIs must be inventoried to include API name and description, Endpoint URLs, owner and authentication methods used (e.g., OAuth 2.0, API keys).				✓	✓	
TPC-2.75	API access tokens must be validated with every request.				✓	✓	
TPC-2.76	A timeframe must be defined and enforced for access token expiry to reduce the risk of unauthorized access.				✓	✓	
TPC-2.77	The Third Party must protect information involved in application service transactions against possible risks (e.g.: incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure….).					✓	✓
TPC-2.78	Cybersecurity requirements for usage of information and data media within Third Party must be identified, documented and approved.					✓	
TPC-2.79	Cybersecurity requirements for usage of information and data media within Third Party must be applied.					✓	
TPC-2.80	The Third Party must use secure means when disposing of media.					✓	
TPC-2.81	The Third Party must ensure that media is labeled in human-readable format to explain its classification and the sensitivity of the information it contains.	✓	✓	✓		✓	
TPC-2.82	The Third Party must ensure controlled and physically secure storage of removable media.			✓		✓	

CNTL No.	Control Name	Network Connectivity	Outsourced & Managed Services	Critical Data Processor	Customized Software	Cloud Computing Service	Operational Technology
TPC-2.83	The Third Party must restrict and control the usage of portable media inside the Cloud Technology Stack.					✓	
TPC-2.84	The Third Party must periodically apply and review the cybersecurity requirements for usage of information and data media.					✓	
TPC-2.85	The Third Party must perform a monthly internal vulnerability scan on all internal computing resources to identify and remediate any vulnerability.	✓	✓	✓	✓	✓	✓
TPC-2.86	The Third Party must conduct periodic penetration testing and close all identified vulnerabilities. The Third Party must ensure the scope of penetration tests covers Internet-facing services and its technical components including infrastructure, websites, web applications, mobile apps, email and remote access.	✓	✓	✓	✓	✓	✓
TPC-2.87	The scope of penetration tests must cover Cloud Technology Stack and must be conducted at least once every six months.					✓	
TPC-2.88	The Third Party must remediate vulnerabilities on systems, network infrastructure, software or other computer equipment. a) Internet facing devices must be handled within the following timeframes: i. Critical Risk: Immediately; ii. High Risk: within seven (7) days of vendor patch release or discovered security breach whichever is earlier; iii. Medium Risk/Low Risk: within one (1) month of discovery. b) Internal devices must be handled within the following timeframes: i. Critical Risk: Immediately; ii. High Risk: within two (2) weeks of vendor patch release or discovered security breach whichever is earlier; iii. Medium and Low Risk: within one (1) month of discovery.	✓	✓	✓	✓	✓	✓
TPC-2.89	The Third Party must assess and remediate vulnerabilities on external components of Cloud Technology Stack at least once every month, and at least once every three					✓	

CNTL No.	Control Name	Network Connectivity	Outsourced & Managed Services	Critical Data Processor	Customized Software	Cloud Computing Service	Operational Technology
	months for internal components of Cloud Technology Stack.						
TPC-2.90	The Third Party must notify proponent of identified vulnerabilities that may affect the proponent.	✓	✓	✓	✓	✓	✓
TPC-2.91	The Third Party must: a) Identify the vulnerabilities classification based on criticality level; b) Patch management; c) Subscribe an authorized and trusted cybersecurity resources for up-to-date information and notifications on technical vulnerabilities.	✓	✓	✓	✓	✓	✓
TPC-2.92	Cybersecurity requirements for change management within the Third Party must be identified, documented and approved.	✓	✓	✓	✓	✓	✓
TPC-2.93	Cybersecurity requirements for change management within third party must be implemented.	✓	✓	✓	✓	✓	✓
TPC-2.94	Cybersecurity requirements for change management must be reviewed periodically.	✓	✓	✓	✓	✓	✓
TPC-2.95	Cybersecurity for change management in Third Party must cover: a) Processes and procedures to securely implement changes (planned works) in production systems, with priority given to cybersecurity observations; b) Process for the implementation of cybersecurity exceptional changes (e.g., changes during incident restoration).					✓	
TPC-2.96	The Third Party must ensure secure management of cryptographic keys during their lifecycles.	✓	✓	✓	✓	✓	✓
TPC-2.97	Cybersecurity requirements for key management process within the Third Party must be identified, documented and approved.			✓		✓	✓
TPC-2.98	Cybersecurity requirements for key management process within the Third Party must be implemented.			✓		✓	✓
TPC-2.99	The Third Party must periodically review cybersecurity requirements for key management.			✓		✓	✓

CNTL No.	Control Name	Network Connectivity	Outsourced & Managed Services	Critical Data Processor	Customized Software	Cloud Computing Service	Operational Technology
TPC-2.100	The Third Party must implement a secure cryptographic key retrieval mechanism in case of cryptographic key lost (such as backup of keys and enforcement of trusted key storage, strictly external to cloud).			✓		✓	✓
DETECT							
Continuous Monitoring							
TPC-2.101	Privileged accounts activity must be logged and monitored.	✓	✓	✓	✓	✓	✓
TPC-2.102	The Third Party must perform continuous monitoring of Technology Assets, and applications using a central logging solution and a Security Information and Event Management System (SIEM).	✓	✓	✓	✓	✓	✓
TPC-2.103	The Third Party must implement an automated monitoring and logging of remote access sessions event logs.	✓	✓	✓	✓	✓	✓
TPC-2.104	Third Party must activate and monitor all audit trails of keys.			✓		✓	✓
TPC-2.105	Physical access (e.g., entry, exit) to sensitive sites and buildings must be continuously monitored through surveillance camera. Surveillance records must be protected from authorized access/tamper.	✓	✓	✓	✓	✓	✓
Adverse Event Analysis							
TPC-2.106	The Third Party must have cyber threat intelligence (including vulnerability intelligence) processes in place to be swiftly alerted for cyber threats exploiting relevant vulnerabilities and monitor/apply evolving mitigations to such vulnerabilities.	✓	✓	✓	✓	✓	✓
RECOVER							
Incident Recovery Plan Execution							
TPC-2.107	The Third Party must conduct business continuity drills at least once a year.	✓	✓	✓		✓	
TPC-2.108	The Third Party must ensure resilience and continuity of cybersecurity systems dedicated to the protection of Cloud Technology Stack.					✓	

CNTL No.	Control Name	Network Connectivity	Outsourced & Managed Services	Critical Data Processor	Customized Software	Cloud Computing Service	Operational Technology
TPC-2.109	The Third Party must: a) cover critical technology and information assets during the development and implementation of backup and recovery scope; b) Maintain the ability to perform quick recovery of data and systems following cybersecurity incidents by implementing reliable backup mechanisms and conducting periodic tests to verify the effectiveness of recovery procedures.	✓	✓	✓	✓	✓	
RESPOND							
Incident Management							
TPC-2.110	The Third Party **must** test incident response capability periodically.	✓	✓	✓	✓	✓	
Incident Analysis							
TPC-2.111	The Third Party **must** perform a root cause analysis of cybersecurity incidents and develop plans to address them.	✓	✓	✓	✓	✓	✓
Additional OT Requirements							
TPC-2.112	The Third Party personnel with access to OT assets must complete an OT-specific cybersecurity awareness and training program, in addition to general cybersecurity training. The awareness and training program must include the following but not limited to: a) Account & Access Control Hygiene; b) Portable Media & Malware Control; c) Incident & Event Reporting; d) Security Maintenance Discipline (Patching, Hardening, System Integrity).						✓
TPC-2.113	The Third Party must implement and demonstrate Secure-by-Design principles as part of the security architecture and development lifecycle of OT products and systems delivered.						

CNTL No.	Control Name	Network Connectivity	Outsourced & Managed Services	Critical Data Processor	Customized Software	Cloud Computing Service	Operational Technology
TPC-2.114	Sub-Category 1: OT Systems • All third parties providing and delivering integrated Operational Technology (OT) systems, including but not limited to Distributed Control Systems (DCS), Supervisory Control and Data Acquisition (SCADA), and Safety Instrumented Systems (SIS), must provide valid certification demonstrating compliance with IEC 62443-4-1 and IEC 62443-3-3 (refer to Appendix D for the certification requirements).						✓
TPC-2.115	Sub-Category 2: OT Components • All third parties providing individual Operational Technology (OT) components, including but not limited to controllers, remote terminal units (RTUs), programmable logic controllers (PLCs), human-machine interfaces (HMIs), communication modules, and embedded software or firmware, must provide valid certification demonstrating compliance with IEC 62443-4-1 and IEC 62443-4-2 (refer to Appendix D for the certification requirements).						✓
TPC-2.116	Sub-Category 3: OT System Integration • All third-party service providers responsible for any stage of system integration and lifecycle support—including but not limited to system design and engineering, configuration and commissioning, Factory Acceptance Testing (FAT), Site Acceptance Testing (SAT), and post-deployment operations and maintenance (O&M)—must maintain a valid organizational-level certification demonstrating compliance with IEC 62443-2-4 (refer to Appendix D for the certification requirements).						✓

7. Cloud Service Model Applicability

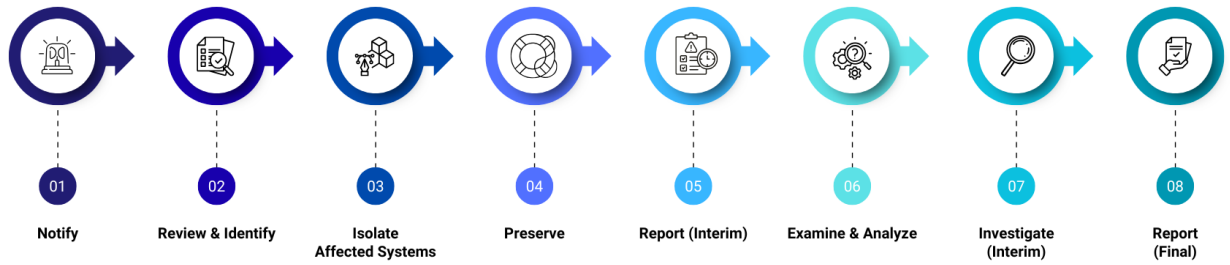
Control #	IAAS	PAAS	SAAS
TPC-2.1	✓	✓	✓
TPC-2.2	✓	✓	✓
TPC-2.3	✓	✓	✓
TPC-2.4	✓	✓	✓
TPC-2.5	✓	✓	✓
TPC-2.6	✓ (Cloud Technology Stack)	✓ (Cloud Technology Stack)	✓ (Cloud Technology Stack)
TPC-2.7	✓	✓	✓
TPC-2.8	a) ✓ b) ✓ c) ✓	a) ✓(Resources and Cloud Technology Stack) b) ✓ (Resources and Cloud Technology Stack) c) ✓ (Resources and Cloud Technology Stack)	a) ✓ (Resources and Cloud Technology Stack) b) ✓ (Resources and Cloud Technology Stack) c) ✓ (Resources and Cloud Technology Stack)
TPC-2.9	✓	✓	✓
TPC-2.10	✓	✓	✓
TPC-2.11	✓	✓ (Cloud Technology Stack)	✓ (Cloud Technology Stack)
TPC-2.12	✓	✓	✓
TPC-2.13	✓ (Cloud Technology Stack)	✓ (Cloud Technology Stack)	✓ (Cloud Technology Stack)
TPC-2.14	✓	✓	✓
TPC-2.15	✓	✓	✓
TPC-2.16	✓	✓	✓
TPC-2.17	✓	✓	✓
TPC-2.18	✓ (Offerings and Cloud Technology Stack)	✓ (Offerings and Cloud Technology Stack)	✓ (Offerings and Cloud Technology Stack)
TPC-2.19	✓ (Offerings and Cloud Technology Stack)	✓ (Offerings and Cloud Technology Stack)	✓ (Offerings and Cloud Technology Stack)
TPC-2.20	✓ (Offerings and Cloud Technology Stack)	✓ (Offerings and Cloud Technology Stack)	✓ (Offerings and Cloud Technology Stack)
TPC-2.21	✓ (Offerings and Cloud Technology Stack)	✓ (Offerings and Cloud Technology Stack)	✓ (Offerings and Cloud Technology Stack)
TPC-2.22	✓ (Cloud Technology Stack)	✓ (Cloud Technology Stack)	✓ (Cloud Technology Stack)
TPC-2.23	✓	✓	✓

Control #	IAAS	PAAS	SAAS
TPC-2.24	✓ (Physical Security)	✓ (Physical Security)	✓ (Physical Security)
TPC-2.25	✓	✓	✓
TPC-2.26	✓	✓	✓
TPC-2.27	✓	✓	✓
TPC-2.28	✓ (Cloud Technology Stack)	✓ (Cloud Technology Stack)	✓ (Cloud Technology Stack)
TPC-2.29			✓
TPC-2.30	✓ (Resources and Cloud Technology Stack)	✓ (Resources and Cloud Technology Stack)	✓ (Resources and Cloud Technology Stack)
TPC-2.31	✓	✓	✓
TPC-2.33	✓ (Cloud Technology Stack)	✓ (Cloud Technology Stack)	✓ (Cloud Technology Stack)
TPC-2.34	✓ (Offerings and Cloud Technology Stack)	✓ (Offerings and Cloud Technology Stack)	✓ (Offerings and Cloud Technology Stack)
TPC-2.35	✓	✓	✓
TPC-2.36	✓	✓	✓
TPC-2.37	✓	✓	✓
TPC-2.38	✓ (Cloud Technology Stack)	✓ (Cloud Technology Stack)	✓ (Cloud Technology Stack)
TPC-2.39	✓	✓	✓
TPC-2.40	✓ (Cloud Technology Stack)	✓ (Cloud Technology Stack)	✓ (Cloud Technology Stack)
TPC-2.41	✓	✓	✓
TPC-2.42	✓ (Cloud Technology Stack)	✓ (Cloud Technology Stack)	✓ (Cloud Technology Stack)
TPC-2.43	✓ (Cloud Technology Stack)	✓ (Cloud Technology Stack)	✓ (Cloud Technology Stack)
TPC-2.44	✓ (Cloud Technology Stack)	✓ (Cloud Technology Stack)	✓ (Cloud Technology Stack)
TPC-2.45	✓	✓	✓
TPC-2.46	✓	✓	✓
TPC-2.47	✓	✓	✓
TPC-2.48	✓	✓	✓
TPC-2.50	✓ (Cloud Technology Stack)	✓ (Cloud Technology Stack)	✓ (Cloud Technology Stack)
TPC-2.51	✓ (Cloud Technology Stack)	✓ (Cloud Technology Stack)	✓ (Cloud Technology Stack)
TPC-2.52	✓ (Cloud Technology Stack)	✓ (Cloud Technology Stack)	✓ (Cloud Technology Stack)
TPC-2.53	✓	✓	✓

Control #	IAAS	PAAS	SAAS
TPC-2.54	✓ (System Development and Cloud Technology Stack)	✓ (System Development and Cloud Technology Stack)	✓ (System Development and Cloud Technology Stack)
TPC-2.55	✓	✓	✓
TPC-2.56	✓ (Cloud Technology Stack)	✓ (Cloud Technology Stack)	✓ (Cloud Technology Stack)
TPC-2.57	✓ (Cloud Technology Stack)	✓ (Cloud Technology Stack)	✓ (Cloud Technology Stack)
TPC-2.58	✓ (Cloud Technology Stack)	✓ (Cloud Technology Stack)	✓ (Cloud Technology Stack)
TPC-2.59	✓ (System Development and Cloud Technology Stack)	✓ (System Development and Cloud Technology Stack)	✓ (System Development and Cloud Technology Stack)
TPC-2.60	✓	✓	✓
TPC-2.61	✓ (Cloud Technology Stack)	✓ (Cloud Technology Stack)	✓ (Cloud Technology Stack)
TPC-2.62	✓	✓	✓
TPC-2.63	✓	✓	✓
TPC-2.64	✓	✓	✓
TPC-2.65	✓	✓	✓
TPC-2.66	✓	✓	✓
TPC-2.68	✓ (Cloud Technology Stack)	✓ (Cloud Technology Stack)	✓ (Cloud Technology Stack)
TPC-2.69	✓	✓	✓
TPC-2.70	✓	✓	✓
TPC-2.71	✓	✓	✓
TPC-2.72	✓	✓	✓
TPC-2.73	P (Cloud Technology Stack)	P (Cloud Technology Stack)	✓ (Cloud Technology Stack)
TPC-2.74	✓	✓	✓
TPC-2.75	✓	✓	✓
TPC-2.76	✓ (Cloud Technology Stack)	✓ (Cloud Technology Stack)	✓ (Cloud Technology Stack)
TPC-2.77	✓ (Cloud Technology Stack)	✓ (Cloud Technology Stack)	✓ (Cloud Technology Stack)
TPC-2.78	✓ (Cloud Technology Stack)	✓ (Cloud Technology Stack)	✓ (Cloud Technology Stack)
TPC-2.79	✓ (Cloud Technology Stack)	✓ (Cloud Technology Stack)	✓ (Cloud Technology Stack)
TPC-2.80	✓	✓	✓
TPC-2.81	✓	✓	✓
TPC-2.82	✓ (Cloud Technology Stack)	✓ (Cloud Technology Stack)	✓ (Cloud Technology Stack)

Control #	IAAS	PAAS	SAAS
TPC-2.83	✓ (Cloud Technology Stack)	✓ (Cloud Technology Stack)	✓ (Cloud Technology Stack)
TPC-2.84	✓	✓	✓
TPC-2.85	✓ (Cloud Technology Stack)	✓ (Cloud Technology Stack)	✓ (Cloud Technology Stack)
TPC-2.86	✓ (Cloud Technology Stack)	✓ (Cloud Technology Stack)	✓ (Cloud Technology Stack)
TPC-2.87	✓ (Cloud Technology Stack)	✓ (Cloud Technology Stack)	✓ (Cloud Technology Stack)
TPC-2.88	✓	✓	✓
TPC-2.89	✓	✓	✓
TPC-2.90	✓	✓	✓
TPC-2.91	✓ (Resources and Cloud Technology Stack)	✓ (Resources and Cloud Technology Stack)	✓ (Resources and Cloud Technology Stack)
TPC-2.92	✓ (Cloud Technology Stack)	✓ (Cloud Technology Stack)	✓ (Cloud Technology Stack)
TPC-2.93	✓	✓	✓
TPC-2.94	✓	✓	✓
TPC-2.95	✓	✓	✓
TPC-2.96	✓ (Cloud Technology Stack)	✓ (Cloud Technology Stack)	✓ (Cloud Technology Stack)
TPC-2.97	✓	✓	✓
TPC-2.98	✓ (Resources and Cloud Technology Stack)	✓ (Resources and Cloud Technology Stack)	✓ (Resources and Cloud Technology Stack)
TPC-2.99	✓ (Resources and Cloud Technology Stack)	✓ (Resources and Cloud Technology Stack)	✓ (Resources and Cloud Technology Stack)
TPC-2.100	✓ (Cloud Technology Stack)	✓ (Cloud Technology Stack)	✓ (Cloud Technology Stack)
TPC-2.101	✓ (Physical Security)	✓ (Physical Security)	✓ (Physical Security)
TPC-2.102	✓	✓	✓
TPC-2.103	✓ (Cloud Technology Stack and business continuity management)	✓ (Cloud Technology Stack and business continuity management)	✓ (Cloud Technology Stack and business continuity management)
TPC-2.104	**a)** ⦸ **b)** ✓	a) ✓ (Cloud Technology Stack) b) ✓ (Cloud Technology Stack)	c) ✓ (Cloud Technology Stack) **a)** ✓ (Cloud Technology Stack)
TPC-2.105	✓	✓	✓
TPC-2.106	✓	✓	✓
TPC-2.107	✓	✓	✓

8. **Appendix A:** Cybersecurity Incident Response Process



Notify

- Notify Proponent (SOC) via the Security Hotline below:

Entity	Security Hot Line
Saudi Aramco (SAO)	+966 (13)-880-0000
SABIC	+966 556900971

- Subsequent notification should be communicated via the communication method agreed by SOC during the initial notification.

Review and Identify

- Immediately review all recent changes and modifications to information system users and access privileges for unauthorized modifications.
- Conduct a thorough review of the Third Party's information systems for evidence of compromise.

Isolate Affected Systems

Isolate affected systems from the network to prevent the spread of the incident.

Preserve

Preserve images of all known affected information systems and all associated logs for at least ninety (90) days from the submission of the Final Report.

Report (Interim)

Provide Proponent with reports detailing the Incident. The Third Party must communicate its ongoing efforts to mitigate and resolve the Incident every 24 hours until the time of Incident resolution. Please refer to Appendix B.1 for details of the report template. The Incident must be classified according to the below classification:

Severity	Description
Low	An incident that: • Adversely impacts a very small number of systems or individuals. • Disrupts a very small number of network devices or segments. • Has little or no risk of propagation or causes only minimal disruption or damage.
Medium	An incident that: • Adversely impacts a moderate number of systems and/or people. • Adversely impacts a non-critical organization system or service. • Adversely impacts a business unit system or service. • Disrupts a business unit network.
High	An incident that: • Threatens to have a significant adverse impact on a large number of systems and/ or people. • Poses a potential large financial risk or legal liability to the organization • Threatens the confidentiality of data. • Adversely impacts an organization system or service critical to the operation of a major portion of Proponent. • Has a high probability of propagating to many systems and causing significant damage or disruption?.

Examine and Analyze

Upon request by proponent, the Third Party must provide access to information or equipment associated with the reported Incident for the purpose of conducting a forensic analysis. This includes but not limited to hard disk drives, volatile memory dumps and logs.

Investigate

The Third Party must submit (or provide access) to proponent SOC, any malicious software/program, supporting binaries and files associated with the Incident for forensic analysis purpose. The suitable submission method will be defined by proponent upon receiving the first Interim Status Report.

Report (Final)

Provide proponent with two Final Reports of the Incident:

a) ***Business Report***: High-level report for proponent Management within three (3) business days of resolution or a determination that the problem cannot be resolved within such time period. Please refer to Appendix B.2-1 for details of the reports template.

b) ***Technical Report:*** detailed report for proponent cybersecurity team within ten (10) business days of resolution or a determination that the problem cannot be resolved within such time period. Please refer to Appendix B.2-2 for details of the reports template.

Appendix B: Cybersecurity Incident Subsequent Reports and Notifications

B-1 Interim Status Reports

The Third Party must provide the proponent's SOC with an interim written status report of each cybersecurity incident within 24 hours from initial incident notification. The subsequent Interim Status Reports must be provided to proponent SOC every 24 hours until the Cybersecurity Incident is resolved. The following report must be used:

Third Party Cyber Incident Interim Status Report			Report Number:
Date:	MM/DD/YYYY	Third Party Incident Coordinator Information	
Affiliate Name:		Name:	
		Email:	
		Phone/Mobile:	
Incident Classification:			
Type of information affected:			
Incident Impact:			
Known/Suspected cause:			
Incident Description:			
Incident Response Activities			
Actions taken:			
Future actions that will be taken:			
Current incident status:			
Expected timeframe for full-service restoration:			

B-2 Final Report

1. Business Report

The Third Party must provide proponent SOC with a final written report of any cybersecurity incident within three (3) business days of resolution or a determination that the problem cannot be resolved within such time period, such report must include:

- Third Party's Name;
- Third Party's Incident Coordinator and contact information;
- The proponent's Incident Coordinator;
- Date and Time of the Incident;
- Incident Classification (according to proponent classification provided in this document);
- Length of Outage and Impact (i.e., Reputational, operational, customer, financial and legal);
- Incident Executive Overview.

2. Technical Report

The Third Party must provide proponent SOC with a final written report of any Cybersecurity Incident within ten (10) business days of resolution or a determination that the problem cannot be resolved within such time period, such report must include:

- Third Party's Name;
- Third Party's Incident Coordinator and contact information;
- The proponent's Incident Coordinator;
- Date and time of the incident;
- Incident classification (according to proponent classification provided in this document);
- Impact and length of outage;
- Incident Executive Overview including incident impact (i.e., Reputational, operational, customer, financial and legal);
- Incident details:
  a) List of individuals and other Third Parties that were involved with any aspect of the Incident handling;
  b) How/when the Incident was initially detected;
  c) How/when the Incident was initially reported to proponent;
  d) Description of what resources/services were impacted;
  e) Description of incident's impact to proponent (volume and type where applicable);
  f) Containment — how the incident was contained;
  g) Root Cause — the cause for disruption;
  h) Corrective action during the Incident — steps taken to reduce exposure during the incident (in most cases, there are interim steps taken to reduce exposure, e.g., Filtering, rerouting services, etc);
  i) Permanent corrective actions/preventative measures — permanent corrective actions that have been put in place as a result of the incident;
  j) Conclusion.

Appendix C: Auditing Events

Information Systems must be capable of auditing the events listed below.

No.	Event Type
1	Availability state changes for systems includes start, shutdown, restart
2	Successful login attempts during a short period when the attempts are geographically separated (e.g., a successful login from Saudi Arabia and Germany within an hour of each other)
3	Failed login attempts
4	Addition and deletion of user accounts
5	Escalation/Modification of account privileges
6	Modification of security configuration/policies
7	Activities of privileged accounts
8	Logs cleared or paused

No.	Event Attributes
1	Timestamp
2	User ID
3	Event name
4	Event category
5	Event severity
6	Host name
7	Source IP address
8	Destination IP address
9	Source Port
10	Destination Port

Appendix D: OT Certifications Requirements

Certification	Accepted by	Certificate scope
IEC 62443-4-1	Any certifying body that is accredited by ISO/IEC 17011 AB to perform SSA certification or IECEE to perform IEC 62443-4-1 certification.	The certificate must clearly define the scope of the system, the Security Level Capability (SL-C) achieved, and the validity period of the certification.
IEC 62443-3-3	Any certifying body that is accredited by ISO/IEC 17011 AB to perform SSA certification or IECEE to IEC 62443-3-3 certification.	
IEC 62443-4-1	Any certifying body that is accredited by ISO/IEC 17011 AB to perform CSA certification or IECEE to perform IEC 62443-4-1 certification.	The certificate must clearly define the product or component name and model/version, the security functionality covered, and the validity period of the certification.
IEC 62443-4-2	Any certifying body that is accredited by ISO/IEC 17011 AB to perform CSA certification or IECEE to perform IEC 62443-4-2 certification.	
IEC 62443-2-4	Any certifying body that is accredited by IECEE to perform IEC 62443-2-4 certification.	• The certification must explicitly demonstrate that the organization meets security requirements applicable to each of the covered services, including FAT, SAT, and O&M. • The certification scope must clearly identify the regional offices, FAT/SAT facilities, engineering teams, and O&M support centers responsible for delivering the services. • A copy of the certification scope statement or audit summary must be provided, indicating the certified entities, services covered, and the validity period.

Appendix E: Terms and Definitions

Term	Definition
Information Technology	
Assets	Anything that has value to corporate created (intellectual and personal data) or procured data, proposed or executed contracts, agreements, devices, systems, hardware, software, research information, training manuals, operational or support procedures, continuity plans and any facilities that enable the organization to achieve business purposes.
Audit log	A chronological record of system activities. Includes records of system accesses and operations performed in a given period. Examples of auditable events are included in Appendix C.
Compliance Assessment	The practice and activities conducted on processes and systems to evaluate and verify their adherence to the enforced cybersecurity controls in the Standard and the contract.
Critical Data	Corporate confidential data that if leaked or lost would result in high risk and adverse impact to Proponent including but not limited to brand reputational damage, financial loss, operational impact, loss of proprietary information, or loss of competitive advantage.
Content-filtering	The use of a program to screen and exclude users from accessing web pages and services that contain hate-based, pornographic, extremist/militancy, gambling, illegal substances or other objectionable material.
Corporate Network	The corporate computing resources and infrastructure, excluding plant networks and international offices networks.
Critical Facilities	A physical location housing information processing Systems such as data centers, communications closets, or cabling (power, network etc.).
Cybersecurity	The mandatory minimum information security requirements to support the protection of confidentiality, integrity, and availability of Assets.
Cybersecurity Assessment	Cybersecurity assessments include risk assessments, compliance assessments, vulnerability assessments and forensic analysis. A cybersecurity assessment is conducted by corporate using corporate resources to ensure that the Third Party is compliant with cybersecurity controls in the Standard and the contract.
Cybersecurity Incident	Unauthorized access, disclosure, modification or disruption of information, systems and services. Physical incidents include but not limited to: • Unauthorized physical access to restricted areas or communication rooms; • Theft of assets.
Cybersecurity Policy	The set of laws, rules, directives and practices that governs how an organization protects information systems and information.
Cloud Technology Stack	Layered architecture of technologies that are essential to implement cloud computing services, including but not limited to: • Data center infrastructure, LAN, storage/compute/hyper convergence hardware, hypervisor, cloud management platform, virtual appliances, operating systemss, application software, O&M platforms, cloud security technologies.
Data Life Cycle	The process of managing the flow of data. The cycle includes the management of data from creation and storage to the time when the data becomes obsolete and is deleted.

Term	Definition
DMZ	Demilitarized Zone or a perimeter network is an additional layer of security to separate an organization's Local Area Network (LAN) from other untrusted networks such as the Internet and has additional cybersecurity controls to restrict access to other layers in the network.
Incident Response	A process detailing the steps required to minimize or eradicate a cybersecurity incident that threatens the confidentiality, integrity or availability of the Third Party's or corporate Assets. A critical component of this process is highlighting the guidelines and procedures for defining the criticality of the cybersecurity incident, reporting and escalation process, and recovery procedures.
Patch	A piece of software designed to fix operating system or software programming errors and vulnerabilities.
Penetration Testing	A live test of the effectiveness of security defenses through mimicking the actions of real-life attackers to uncover vulnerabilities. This includes testing a computer system, network or Web application.
Physical Security	Physical security describes security measures designed to prevent unauthorized access to the organization's facilities, equipment and resources, and to protect individuals and property from damage or harm (such as espionage, theft or terrorist attacks). Physical security involves the use of multiple-tier of interconnected systems, including CCTV, security guards, security limits, locks, access control systems and many other technologies.
Public Cloud Computing	A model for enabling on-demand network access to a shared pool of configurable IT capabilities/resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal operation management effort or service provider interaction. It allows users to access technology-based services from the cloud without knowledge of, expertise with, or control over the technology infrastructure that supports them.
Remote Access	Act of utilizing a remote access service, hardware or process to connect to the corporate network or corporate Systems.
Risk	The measurement and articulation of the potential adverse impact on the operation of information systems, which is affected by threat occurrences on organizational operations, assets, and people.
Risk Assessment	The overall process of calculating the potential impact of an event using metrics-based risk identification, analysis and evaluation.
Risk Management	The process of recognizing Risk; assessing the impact and likelihood of that Risk; and developing strategies to manage it, such as avoiding the Risk, reducing the negative effect of the Risk and/or transferring the risk.
Sanitization	The process of permanently removing all data and/or licensed software, through overwriting or degaussing methods, from an asset before it is disposed, loaned, destroyed, donated, transferred, or surplused.
Sender Policy Framework (SPF)	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.
Standard	Provides information security requirements that support the implementation of the policy.
Suspicious Activities	Any observed user, system or network traffic behavior that could indicate or lead to a cyberattack on Assets that are used to receive, access, store, process or transmit corporate data.

Term	Definition
Systems	A collection of communication and computing hardware, software, firmware, database and applications organized to accomplish a specific function or set of functions.
System Development	Any application, platform, middleware, operating system, hypervisor, network stack and any other software that is part of the Cloud Technology Stack.
Technology Asset(s)	Any information technology or operational technology system, network, or device that is owned, operated, leased, or controlled by the company or that stores or processes data to include any hardware or software.
Third Party	Any external party; individual, business or organization that generates, acquires, compiles, transmits or stores data on behalf of corporate.
Threat	An activity, event or circumstance with the potential for causing harm to information system resources.
Vulnerability	Any known or unknown deficiency in an information system, application or network that is subject to exploitation or misuse by threat agents.
Vulnerability Assessment	A process that defines, identifies, and classifies the security weaknesses/exposures (Vulnerabilities) in a computer, network, or communications infrastructure in order to apply a patch or fix to prevent a compromise and ensure adherence with the Standard.
Waiver	An exception or exemption to any written information security policy, standard, procedure, or practice that has been approved by the appropriate governing body and published for use.
Network Connectivity third-party	The Third Party's computing infrastructure is provided with network connectivity (e.g., SSL VPN, Leased line) to the Corporate Network.
Outsourcing & Managed Services	The Third Party is providing, managing, maintaining and/or supporting outsourcing infrastructure and/or managed services, that is owned by the corporation on behalf of it (e.g., data centers, co-location centers, and backup centers).
Critical Data Storage/Systems third-party	The Third Party is processing or storing Corporate Critical Data or maintaining Critical Systems.
Customized Software third-party	The Third Party is developing software for the corporation.
Cloud Computing Service third-party	The Third Party is providing Public Cloud Computing service to host, store and/or process Corporate data. This includes any cloud computing service model; such as Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS))