CYBERSECURITY
COMPLIANCE
CERTIFICATION

SACS-210 Third-Party Cybersecurity Standard Control Guidelines

Table of Contents

1. Purpose

Third Party Cybersecurity Standard (TPCS) Control Guideline provides guidance on fullfilling the cybersecurity requirements set forth in the Third Party Cybersecurity Standard (TPCS). The scope and applicability of the controls is defined in the standard. These guidelines ensure that third parties are aware of the control requirements and supporting evidence, and that they are provided as part of the Third Party Compliance Package that will be submitted to the authorized audit firm.

2. Scope

This document provides guidance on all the requirements included in the Third Party Cybersecurity Standard (TPCS) where the certification applicability is defined. The applicability of the certification is based on the standard scope below covering 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.
- Provides OT products and/or services.

3. Third Party Classification

The applicability of the general requirements and specific requirements is based on the classifications defined in the standard as shown below:

- ## General Requirement:

This standard applies to all third parties interacting with corporate data or assets, establishing minimum cybersecurity controls to ensure the fundamental protection of company data and systems. The general requirement classification encompasses controls related to governance, access management, password policies, multi-factor authentication, data security measures such as antivirus and 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:

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

- ## Critical Data Processor:

Third Party is developing, accessing, and/or processing confidential data. This includes Third Parties that provides consultancy services for high-sensitivity strategic projects that is deemed to be sensitive/critical to corporate and/or at the national level.

- ## Software Services:

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

- ## Cloud Computing:

Third Party provides cloud computing services:

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

- ## Operation Technology:

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:

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 controls 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. Third Party Cybersecurity Requirements

• General Requirements:

The following section details the evidence expectations for each cybersecurity control within the General Requirements classification of the Third Party Cybersecurity Standard (TPCS).

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

CNTL No.	Control Name	Control Guidelines
GOVERN		
Organizational Context		
TPC1.1	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.	• A document (such as a policy, procedure, or/and letter approved by the authorization official) indicating the identification and documentation of the requirements related to this control. • An updated list that clarifies the national cybersecurity laws and regulations that are relevant to the organization's operations and issued by the National Cybersecurity Authority (NCA). • A report that cybersecurity laws and regulations applicable to the organization.
Policy		
TPC1.2	Third Party must develop, approve and communicate an Acceptable Use Policy (AUP).	• Approved policy that covers the requirements for acceptable use of the organization's information and technology assets. • Acceptable use policy of the organization's information and technology assets must be communicated to all employees and stakeholders in the organization through, including but not limited to the official email or through the organization's website. • Evidence that all employees and stakeholders are aware and informed must be provided.

		• Formal approval by the head of the organization or his/her deputy on the policy.
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.	• Cybersecurity policies and/or standards, approved by the head of the organization or his/her deputy, that explicitly address the following control areas: ○ asset management; ○ access management; ○ physical security; ○ secure disposal of media/data sanitization; ○ classification and handling of assets and data; ○ incident management; ○ vulnerability and patch management; and ○ business continuity and disaster recovery. • A mapping or cross-reference identifying the policy/standard and the corresponding section that addresses each of the above control areas.
TPC1.4 	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).	• Evidence of hiring procedures to determine whether background checks/screenings are performed for all employees. • Evidence of HR screening policy. • Evidence of the third-party termination procedures to determine whether accounts/access are disabled in a timely manner. • Evidence of the return of assets. • Samples of the removal of all access to asset's as part of the third party offboarding procedures.
Cybersecurity Supply Chain Risk Management		
TPC1.5 	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.	• A Copy of approved and stamped Cybersecurity Compliance Certificate (CCC) by a CCC authorized audit firm.

TPC1.6	Third Party must renew the CCC (or approved certificate) before it expires.	• A Copy of approved and stamped Cybersecurity Compliance Certificate (CCC) by a CCC authorized audit firm.
TPC1.7	Proponent data must only be shared with individuals who are part of the work specified in the contract.	• A document (such as approved policy or procedure) indicating the identification and documentation of the requirements related to this control.
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.	• A documented and up-to-date record of all information and technology assets (e.g., Excel spreadsheet or displayed through automated means using solutions such as CMDB) must be provided. • Specific procedures for dealing with assets based on their classification and in accordance with the relevant laws and regulations.
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.	• Cybersecurity policy that covers Identity and Access Management. • Evidence that outlines the implementation of User authorization management requirements, including but not limited to a screenshot showing the configuration of systems to ensure the implementation of user authorization management based on a Need to Know and Need to Use basis and least privilege and Segregation of Duties.
TPC1.10	User authentication must be granted based on unique authentication credentials.	• Cybersecurity policy that covers Identity and Access Management. • Evidence demonstrating that user authentication is based on unique authentication credentials, such as a user account listing, identity management system records, or equivalent evidence showing that individual users are assigned unique user accounts and shared or duplicate credentials are not used.

TPC1.11	The following rules must be used for password and authentication code management (where feasible): a) using long passwords or passphrases between 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.	• Cybersecurity policy that covers Identity and Access Management, including password management. • Evidence demonstrating the enforcement of password complexity requirements, including: ○ password/passphrase length between 8–64 characters; ○ lowercase characters; ○ uppercase characters; ○ numeric characters; ○ special characters; and ○ password hints are disabled or not permitted. • Evidence of Multi-Factor Authentication (MFA) implementation. • Evidnence that no password hints are provided duing loging.
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.	• Evidence of activation of multi-factor authentication for remote access, cloud services, organization's webmail access, internet facing applications, privileged accounts by, but not limited to, one of the following methods: ○ Text messages linked to the email user's number must be used. ○ Advanced and reliable applications for multi-factor authentication. ○ Mobile device management applications must be used to allow users' devices (as another element of access) to email for protocols (such as EWS, outlook anywhere protocols) that do not support text messages or applications that provide verification code.
TPC1.13	Single sign-on can be used but must be coupled with MFA upon initial login to a system.	• Evidence of MFA implementation with single sign-on systems.
TPC1.14	Third-Party must review user accounts and access rights at least annually.	• Evidence of user accounts and access rights review at least annually, and for revoked accounts that are invalid (e.g., retired, resigned or no longer associated with the Third Party).

TPC1.15	All Third Party technology assets must be authenticated using secure authentication mechanisms.	• Cybersecurity policy that covers Identity and Access Management, including secure authentication requirements. • Evidence demonstrating the implementation of secure authentication mechanisms for third-party technology assets such as certificate-based authentication, or other approved secure authentication methods, where applicable.
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).	• Provide evidence of the third-party sanitization (data destruction) policies. • Provide evidence of sanitization techniques and procedures are commensurate with the security category or classification of the information or asset and in accordance with organizational standards and policies. • Provide evidence (e.g., destruction certificates) that media sanitization is occurring according to policy.
TPC1.17	Technology assets must be securely disposed at the end of their lifecycle (e.g., loaned, donated, destroyed, transferred or surplussed) in accordance with applicable legislative requirements and industry best practices.	• Provide evidence of the third-party sanitization policies. • Provide evidence of sanitization techniques and procedures are commensurate with the security category or classification of the information or asset and in accordance with organizational standards and policies. • Provide proof (e.g., destruction certificates) that media sanitization is occurring according to policy.
TPC1.18	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.	• Cryptography policy, approved by the head of the organization or his/her deputy, that covers encryption requirements for data at rest and data in transit in accordance with the advanced level of the KSA National Cryptographic Standards (NCS-1:2020) and industry-approved encryption algorithms. • Evidence demonstrating the implementation of encryption for data at rest in accordance with the organization's cryptography policy.

		• Evidence demonstrating the implementation of encryption for data in transit in accordance with the organization's cryptography policy. • Evidence demonstrating the implementation of encryption for data in transit, including data transmitted over VSAT communication links, in accordance with the organization's cryptography policy and approved encryption standards.
TPC1.19	Third Party must restrict and secure the use of external storage media.	• Documentation approved by the head of the organization or his/her deputy that defines the requirements for restricting and securing the use of external storage media. • Evidence demonstrating that the use of external storage media is restricted and secured, including: o Restricted access to removable media (e.g., USB device restrictions) o Evidence of approval of enabled external storage media. o Encryption of removable media, where applicable.
TPC1.20	Third Party must implement Sender Policy Framework (SPF), Domain Message Authentication Reporting (DMARC) and DomainKeys Identified Mail (DKIM) technology on the mail server.	• Provide evidence of implementation on the third-party mail server: o SPF o DMARC o DKIM
TPC1.21	Third Party must inspect all incoming emails originating from the Internet using anti-spam protection.	• Evidence of using an anti-spam protection for all incoming emails on the email security appliance.
TPC1.22	Third Party must inspect all email attachments with signature analysis before allowing the attachments.	• Evidence of relevant configuration for scanning email attachment. • Evidence of blocked malicious email attachment.
TPC1.23	Third Party must use a private email domain. Generic public domains, such as Gmail and Hotmail, must not be used.	• Evidence of the third-party acceptable use policy (AUP) that highlights the use of the third-party private email domain only and prohibit the use of generic domains. • Verify that the third-party has a private email domain.

TPC1.24	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.	• Evidence of relevant group policy configuration.
TPC1.25	Third Party must synchronize all technology assets with an authorized time source e.g., NTP server.	• A document (such as approved policy or procedure) indicating the identification and documentation of the requirements related to this control. • Evidence that the organization uses a central server to synchronize timing (including but not limited to: a screenshot or direct example of the presence of this server in the network with all server details). • Evidence that technology assets are synchronized with the authorized time source.
TPC1.26	Event logs must be protected from alteration, disclosure, destruction, and unauthorized access and unauthorized release.	• Evidence of relevant group policy configuration to protect log event from alteration. • Evidence of securing access into the log data to be limited to authorized individuals.
Platform Security		
TPC1.27	Firewalls must be configured and enabled on all endpoint devices.	• Evidence of firewall configuration and enablement on third-party endpoint devices. • Sample configuration or screenshots demonstrating that host-based firewalls are enabled on endpoint devices (e.g., Windows Firewall domain, private, and public profiles, or equivalent firewall settings for the operating system in use).
TPC1.28	Third Party must inspect all HTTP and HTTPS traffic from Internet facing (External) applications using Web Application Firewall (WAF).	• Evidence of implementing Web Application Firewall (WAF). • Evidence of the WAF configuration and activation.
TPC1.29	Third Party Technology Assets must be protected with signature based up-to-date virus and malware protection software.	• Provide evidence of the anti-virus/malware installed on endpoint devices. • Provide evidence of configuration console of the installed anti-virus/malware software to determine the last updates and full system scan that were performed.

		• Provide evidence of the history of updates.
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.	• Patch management policy and procedures covering patch testing deployment, back up, and rollback before implementation into production enviorment. • Evidence that patch testing was performed before implementation to production environment. • Evidence demonstrating the ability to restore systems in the event of patch failure.
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.	• Cybersecurity policy that covers Event Logging and Monitoring Management. • Evidence demonstrating that audit and cybersecurity event logs are enabled on information systems and applications. • Evidence demonstrating that the required security events are collected and monitored in accordance with Appendix C. • Where monitoring is performed by a managed service provider, a copy of the service agreement or equivalent documentation demonstrating the monitoring service. • Evidence that all event types and event attributes are covered.
RESPOND		
Incident Management		
TPC1.32	If Third Party discovers a Cybersecurity Incident, Third Party must (besides its continuous efforts to resolve and mitigate the Incident): a) Notify proponent within 24 hours of discovering the Incident;	• Third-party cybersecurity incident management policy and procedures that require notification of the proponent within 24 hours of discovering a cybersecurity incident. • Sample incident notification records or communication demonstrating

	b) Follow the Cybersecurity Incident Response Process set forth in Appendix A.	notification to the proponent within the required 24-hour timeframe. • Evidence demonstrating the implementation of the Cybersecurity Incident Response Process defined in Appendix A.
TPC1.33	Third party must notify proponent when 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.	• Third-party policy or contractual requirements defining the process for notifying the proponent when user credentials are no longer required. • Sample communication notifying the proponent to revoke user credentials that are no longer required. • Evidence demonstrating that proponent user credentials are revoked for third-party personnel who are transferred, reassigned, retired, or no longer associated with the third party.

Specific Requirements

The following section details the evidence expectations for each cybersecurity control within the Specific Requirements classification of the Third Party Cybersecurity Standard (TPCS).Third Parties that fall under one or multiple classifications, must comply with all applicable requirements in the specific classification(s), in addition to the general requirments.

CNTL No.	Control Name	Control Guidelines
GOVERN		
Risk Management Strategy		
TPC-2.1 	Cybersecurity risk management methodology and procedures must be defined, documented and approved.	• The approved cybersecurity risk management methodology. • Approved cybersecurity risk management procedures.
TPC-2.2 	Cybersecurity risk management methodology and procedures must be implemented.	• Cybersecurity Risk Register of the organization. • Cybersecurity Risk Treatment Plan of the organization. • A report that outlines the cybersecurity risk assessment and monitoring.
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.	• An approved document that defines the review schedule for the cybersecurity risk management methodology and procedures. • Cybersecurity risk methodology and procedures indicating that they have been reviewed and updated, and that changes have been documented and approved by the representative.
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	• Defined acceptable risk levels of cloud services documented and communicated with the concerned and relevant stakeholders, including the CSTs. • Cybersecurity risk management methodology includes clear procedure to handle data based on its classification levels. • Cybersecurity Cloud Services Risk Register. • Cybersecurity Cloud Services Risk Register review plan.

CNTL No.	Control Name	Control Guidelines
	monitoring it periodically according to the risks.	• Cybersecurity Cloud Services Risk Register review reports.
Oversight		
TPC-2.5 	Third Party must measure and monitor cybersecurity incident metrics and ensure compliance with contracts and legislative requirements	• Contractual and legislative requirements register. • Formally approved and tested cybersecurity incident metrics (KPI, KCI). • Metrics dashboards and compliance reports. • Sample of dashboard and compliance report.
Roles, Responsibilities, and Authorities		
TPC-2.6 	Third Party must ensure well-defined ownership for cryptographic keys.	• Document approved by the head of the organization or his/her deputy that defines the ownership and responsibilities for cryptographic keys. • Evidence demonstrating the formal assignment of cryptographic key ownership, including the designated key owners and their responsibilities.
TPC-2.7 	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.	• Organizational structure identifying the cybersecurity function. • Job descriptions or documented roles and responsibilities for cybersecurity personnel demonstrating responsibility for maintaining the security of information systems and ensuring compliance with organizational policies.
TPC-2.8 	Prior and during the professional relationship of personnel, 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;	• List of cybersecurity positions related to the Cloud Technology Stack within KSA data centers and the requirements for each position. • List of personnel assigned to these positions and their qualifications. • Cybersecurity training program and training records demonstrating completion. • Screening/vetting process for personnel with access to the Cloud Technology

CNTL No.	Control Name	Control Guidelines
	c) Cybersecurity policies as a prerequisite to access to Cloud Technology Stack, signed and appropriately approved.	Stack, including evidence of implementation. • Evidence demonstrating that screening/vetting has been completed for applicable personnel, with sensitive personal information redacted where appropriate. • Cybersecurity policy acknowledgment and compliance records demonstrating that personnel working on the Cloud Technology Stack acknowledged the applicable cybersecurity policies before being granted access.
Cybersecurity Supply Chain Risk Management		
TPC-2.9	Third Party must integrate third-party cybersecurity risks into its overall risk management and governance framework.	• Cybersecurity policy that covers the requirements of contracts and agreements with third parties. • A report that outlines the identification, assessment, and remediation of third party cybersecurity risks that provide outsourcing services to IT or managed services.
TPC-2.10	Cloud Service Provider's data center must be certified and/or have an audit report against industry recognized standard / authority.	• Valid certification document. • Certification scope statement indicating the relevant services and locations. • Audit reports from third-party certifiers
TPC-2.11	Third Party cloud service providers must provide proponent evidence of securely data storage processes, procedures, and technologies to comply with related legal and regulatory requirements.	• Data storage and protection policy. • Evidence of implemented secure data storage technologies and controls.
TPC-2.12	Third Party must have a process in place to guarantee that a nondisclosure agreement between contracted employees of the Third Party and the Third party is signed before access to proponent systems and/or premises is granted.	• Cybersecurity policy that covers the requirements of contracts and agreements with third- parties. • Signed sample of a contract or agreement with third parties indicating the inclusion of confidentiality clauses and secure removal of data.

CNTL No.	Control Name	Control Guidelines
IDENTIFY		
Asset Management		
TPC-2.13	Third Party must identify assets owners and involve them in the asset management lifecycle.	• Information asset management cybersecurity requirements (in form of policy or standard) approved by the organization. • Evidence of assets inventory showing asset owners. • Evidence demonstrating the involvement of assesset owners in the asset management lifcycle (commisisoing, decomissioing, upgrades, etc.).
TPC-2.14	Third Party must have an inventory of all end users and mobile devices.	• Information asset management cybersecurity requirements (in form of policy or standard) approved by the organization. • Maintained inventory of end-user and mobile devices.
Risk Assessment		
TPC-2.15	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.	• Documented risk assessment procedure. • Risk registers. • Risk assessment reports. • Mitigation or remediation action plans. • Schedule of periodic risk assessments. • Evidence demosntating reviews and updates on the risk register.
TPC-2.16	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.	• A document (such as approved policy or procedure) indicating the identification and documentation of the requirements related to this control. • Screenshot or direct example showing the organization's subscription in a platform.
PROTECT		
Identity Management, Authentication, and Access Control		
TPC-2.17	Users with remote access to systems must be documented and approved.	• Access approval forms and records fro system access from another location or device (Site-to-Site VPN, jump server, etc.)

CNTL No.	Control Name	Control Guidelines
		• Evidence of remote access logs.
TPC-2.18 	Remote access from the Internet must not be allowed unless it's explicitly approved, restricted, and controlled.	• Access control policy explicitly restricting remote access from the internet. • Approved exception request forms (if any). • Network architecture diagram showing restricted pathways Firewall and access control logs or configuration screenshots.
TPC-2.19 	Third Party must be capable to immediately interrupt a remote access session and prevent any future access for a user.	• Establish controlled remote access sessions. • Sample of system/proxy configurations.
TPC-2.20 	Identity and access management of generic accounts credentials for accountability must not be assigned for a specific individual.	• Document outlining the list if users of generic accounts (service accounts, technical accounts, etc.). • Technical restrictions applied to the use and management of generic accounts.
TPC-2.21 	Third Party must mask displayed authentication inputs, especially passwords, to prevent shoulder surfing.	• Evidence that demonstrates the implementation of obfuscation and masking of sensitive and personal information. • Evidence demontraing the masking of user password during login.
TPC-2.22 	Third Party must restrict and control access to storage systems (such as Storage Area Network (SAN)).	• Access Policy for storage systems. • Evidence of the asset register containing storage systems. • Sample of access policy for storage implementation. • Sample of architecture design of storage systems. • Sample access requests for storage systems.
TPC-2.23 	Third Party must implement access control between different network segments.	• Evidence of Network connection assigned to authenticated users/identities. • Access control list.
TPC-2.24 	Access to the Internet must be restricted by content-filtering technologies to block:	• Content filtering policy. • Firewall or proxy configuration screenshots.

CNTL No.	Control Name	Control Guidelines
	a) Malicious and suspicious websites; b) Personal and non-company approved public cloud services.	• Web filtering logs or reports. • Blocked domains list.
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.	• A document (such as approved policy or procedure) indicating the identification and documentation of the requirements related to this control. • An approved user access request form. • Schedule of visit to a critical area (data center but not limited to) to assess Access. • Evidence of revoking access authorities after the expiry of the period documented on the approved application form (e.g., by email).
Awareness and Training		
TPC-2.26	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.	• A document (such as an approved policy or procedure) identifying the requirements related to this control. • Cybersecurity awareness program approved by the head of the organization or his/her deputy. • Cybersecurity awareness training content demonstrating coverage of: ○ acceptable use and good computing practices; ○ responding to cybersecurity incidents; ○ mobile device security; and ○ data classification and handling requirements. • Action plan for implementing the cybersecurity awareness program. • Awareness materials and training records demonstrating that the cybersecurity awareness program has been delivered to employees.

CNTL No.	Control Name	Control Guidelines
		• List of beneficiaries of the cybersecurity awareness program.
TPC-2.27	Third Party must support identity federation services.	• Identity and access management policy or procedures covering identity federation requirements and access authentication mechanisms. • Evidence of implemented federation services.
Data Security		
TPC-2.28	Encryption key management capability, including preservation and retrieval, must be defined, applied, and reviewed.	• Key Management Policy (KMP) document. • Records of key creation, distribution, and retirement. • Access control logs to key management system. • Periodic review reports of key lifecycle management.
TPC-2.29	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.	• Evidence of system architecture showing logical/physical data segregation. • Configuration of tenant isolation in cloud environment. • Data classification and isolation policy. • Audit logs proving no cross-tenant access.
TPC-2.30	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.	• Data classification policy or procedures covering requirments fo restricting data storage to approved geographical locations. • Configuration evidence or system settings demonstration of restricting data storage locations by country or region. • Evidence of compliance with applicable legal, regulatory, or contractual data residency requirments.
TPC-2.31	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.	• Evidence of secure coding standards including input validation. • Source code excerpts showing implementation of data type and length checks.

CNTL No.	Control Name	Control Guidelines
		• Application security testing reports with validation findings.
TPC-2.32 	Third Party must securely handle proponent data found in the audit trails and the cybersecurity event logs.	• Data handling and protection policy covering the secure handling of proponent data in audit trails and cybersecurity event logs. • Evidence that appropriate technical and administrative controls are implemented to protect proponent data within audit trails and cybersecurity event logs. • Evidence of Personally Identifiable Information (PII) anonymization or masking in logs, where applicable. • Sample audit trails or cybersecurity event logs demonstrating secure handling of proponent data.
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.	• Cybersecurity policy that covers the requirements of Data and Information Protection in the organization. • Evidence of DLP system configuration and logs. • A sample of incident reports on DLP violations.
TPC-2.34 	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.	• Evidence of segregated production, development, and test envrioments. • Architecture design documentation. • Evidence that only non-production data is used in development and test envrioments.
TPC-2.35 	Third Party must utilize secure methods and algorithms for saving and processing passwords, such as secure hashing functions.	• Evidence that demonstrates a sample of stored passwords. • Document outlining the applied standard to the storage of passwords.
TPC-2.36 	Third Party must regularly backup corporate data.	• Backup policy and schedule documentation. • Logs of automated or manual backups.

CNTL No.	Control Name	Control Guidelines
		• Screenshot from backup system or console. • Reports showing successful backup jobs. • Evidence that backups are performred regurarly.
TPC-2.37	Backup data stored at an off-site location must be encrypted.	• Backup architecture or solution design indicating off-site encryption. • Encryption policy or encryption key management document. • Sample backup logs showing encryption status. • Certification of encryption algorithm used.
TPC-2.38	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.	• Review the catalogue of third-party software providers and their software. • A document outlining procedures for removing specific programs from the market based on legislative requests.
TPC-2.39	Third Party must secure access, storage and transfer of the following: a) Proponent data; b) Cloud Technology Stack backups and its mediums, and protect it against damage, amendment or unauthorized access.	• Data protection policy covering the secure storage, transfer, and protection of proponent data. • Backup and media protection policy covering Cloud Technology Stack backups and backup media. • Evidence of implemented security measures protecting proponent data against damage, amendment, or unauthorized access. • Evidence of implemented security measures protecting Cloud Technology Stack backups and backup media against damage, amendment, or unauthorized access. • Regular review or monitoring reports demonstrating the effectiveness of the implemented security measures.
TPC-2.40	Third Party must provide proponent with secure means to export and transfer data and virtual infrastructure.	• Secure data/assets export functionalities over an encrypted and secure channel or connection.

CNTL No.	Control Name	Control Guidelines
TPC-2.41	Third Party must ensure that the security functions within the cloud technology stack is fully isolated from other operations within the stack.	• Document demonstrating that security functions and applications are isolated from other functions and applications in the Cloud Technology Stack. • Architecture design documentation.
TPC-2.42	Third Party must ensure community cloud services provided to proponent are fully isolated from cloud services offered to external entities.	• Sample of the Isolation mechanisms implemented between cloud services.
TPC-2.43	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.	• Evidence illustrating that Cloud Technology management networks are encrypted using strng encryption methods.
TPC-2.44	Third Party must use certificates that are securely issued by an approved certification authority.	• Installation and activation of a trusted source/authority for accreditation. • Sample of trusted and certified certificates.
TPC-2.45	Third Party must have data sanitation and secure disposal for end-user devices.	• Approved and implemented data sanitation and device disposal tools and methods for Cloud Technology Stack – related end-user devices.
Platform Security		
TPC-2.46	Firewalls must be implemented at the network perimeter, and only required services must be allowed.	• Network architecture diagrams. • Firewall configuration files showing permitted services. • Firewall change request forms. • Firewall ruleset audit logs.
TPC-2.47	Intrusion Prevention Systems (IPS) must be implemented at the network perimeter.	• Cybersecurity policy that covers all the requirements of network security management in the organization • Sample showing the implementation of requirements related to IPS, including but not limited to: ○ Sample showing the implementation of IPS (e.g., a screenshot showing evidence of subscription and use of modern and advanced technologies to implement IPS, as well as access

CNTL No.	Control Name	Control Guidelines
		to technical infrastructure, demonstrating the use of IPS and the comprehensiveness of all the organization's information and technology assets within IPS. ○ Periodic review report on IPS configuration and development of all technical controls and standard controls must be reviewed and verified in relation to the configuration of IPS within an advanced automation program or through Excel Sheet, as well as supporting the review by obtaining prior approval for review and update of the configuration if required.
TPC-2.48	Intrusion Prevention Systems (IPS) must be updated to the latest signature.	• Evidence of up-to-date IPS signature. • Evidnece that IPS signatures are updated regurarly.
TPC-2.49	Servers and workstations subnets must be segmented and access between them restricted and monitored.	• Network segmentation plan. • ACLs or VLAN configuration screenshots. • Logs showing access controls between segments. • Penetration test or network audit reports.
TPC-2.50	Servers accessible from the internet must be placed in a DMZ (i.e., perimeter network) with restricted access to internal subnets.	• DMZ network architecture documentation. • Firewall rules limiting access from DMZ to internal network. • DMZ asset inventory. • Evidence of access control enforcement.
TPC-2.51	Denial of service protection must be implemented on all internet-facing services. This should include Distributed Denial of Service (DDoS).	• A document or report demonstrating that Denial of Service threats are analyzed, detected and mitigated.
TPC-2.52	Third Party must protect the Cloud Technology Stack network and isolate the network from other internal and external networks.	• Threat Model for Cloud Technology Stack network. • Network-level controls implementation. • Architecture design documentation.

CNTL No.	Control Name	Control Guidelines
TPC-2.53	Third Party must isolate cloud service delivery network, cloud management network and CSP enterprise network.	• Isolation mechanisms for networks. • Architecture design documentation.
TPC-2.54	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.	• EDR systems implemented across all devices and servers. • EDR systems configurations review plan and reports. • EDR systems updates plan and reports.
TPC-2.55	Third Party must consider cybersecurity requirements of the Cloud Technology Stack and relevant systems in the design and implementation of the cloud computing services.	• Secure design or secure architecture standard demonstrating that cybersecurity requirements are incorporated into the design and implementation of Cloud Technology Stack and related systems. • Secure design review or architecture review reports demonstrating that cybersecurity requirements were evaluated during the design and implementation process. • Evidence that identified cybersecurity requirements have been implemented and verified within the Cloud Technology Stack and related systems. • Risk assessment or threat modeling documentation, where applicable, demonstrating cybersecurity considerations during the design process.
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.	• Log retention policy • System configurations showing 1-year log retention • Archive samples or exports • Compliance audit reports

CNTL No.	Control Name	Control Guidelines
TPC-2.57	Sessions must be encrypted (e.g., using HTTPS), and session authentication, lockout, and timeout must be enforced.	• HTTPS/TLS configuration settings. • Application settings showing session timeout and lockout. • Authentication mechanism documentation. • Web vulnerability scan results confirming HTTPS usage.
TPC-2.58	IPsec tunnels must utilize IKEv2 with certificate-based authentication	• Certificate configuration or authentication evidence demonstrating the use of certificate-based authentication for IPsec connections.
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	• Cybersecurity policy that covers the requirements of network security management in the organization. • Sample showing the implementation of requirements related to the safe physical or logical isolation and segregation of network parts, including but not limited to: ○ Evidence showing the implementation of requirements related to the safe physical or logical isolation and segregation of network parts and defense in depth strategy (e.g., a screenshot showing evidence of the subscription and use of modern and advanced technologies to implement the physical or logical isolation and segregation of network parts in a secure manner) ○ Sample showing the implementation of the requirements of appropriate and advanced technologies for the safe physical or logical isolation and segregation of network parts and defense in depth (e.g., a screenshot showing evidence of the safe physical or logical isolation and segregation of network arts, as well as viewing and reviewing Network Diagram.

CNTL No.	Control Name	Control Guidelines

	normally utilize zero-day viruses and malware.	• List of server addresses in production environment and development and testing environment.
		• An up-to-date network diagram document that shows logical segregation and clarifies the isolation between the production environment network from the development and testing networks.
		• Sample showing the implementation of requirements related to browsing and internet connection security, including but not limited to:
		  ○ Sample showing the implementation of browsing and internet connection security requirements (e.g., screenshot showing evidence of use of modern and advanced technologies for browsing and internet connection security).
		  ○ Sample showing the implementation of the requirements of appropriate and advanced technologies for browsing and internet connection security (e.g., a screenshot showing evidence that the network settings and firewall systems are conducted and configured to ensure security of browsing and internet connection, evidence of restriction of suspicious websites, file sharing and storage sites, remote access sites).
		• Wireless Security Standard approved by the organization (e.g., electronic copy or official hard copy).
		• Sample showing the implementation of wireless network security and protection requirements, including but not limited to:
		  ○ Sample showing the implementation of wireless network security and protection requirements (e.g., a

CNTL No.	Control Name	Control Guidelines
		screenshot showing evidence of subscription and use of modern and advanced technologies to implement wireless network security and protection, including but not limited to wireless network connection cryptography, as well as configuration of network devices and firewall systems in line with the verification of the user's name before granting the access to connect to the organization's wireless network) • Sample of conducting a thorough study of the risks arising from connecting wireless networks to the organization's internal network in case there is a need to link them, and deal with them in a way that ensures the protection of the organization's technical assets. There must be evidence of risk analysis and study, including but not limited to, providing a thorough report that includes identifying and classifying risks, notes, and remediation plan (e.g., through an advanced automation program or an Excel sheet) • Sample of separating the internal network (LAN) from the wireless network by isolating the two networks from each other, as well as isolating the wireless visitor network from the wireless network of the organization. • Sample showing the implementation of requirements related to network ports, protocols, and services restrictions and management, including but not limited to: ○ Sample showing the implementation of network ports, protocols, and services restrictions and management requirements (e.g., screenshot showing evidence of subscription and use of modern and advanced technologies to apply restrictions and

CNTL No.	Control Name	Control Guidelines
		manage network ports, protocols, and services through firewall system) ○ Sample showing the periodic review of the protection systems' configuration and updates on an ongoing basis, including but not limited to periodic review at least on an annual basis, as well as the development of all technical controls and standard controls that are reviewed and verified with relation to the protection systems configuration within the advanced automation program or through Excel Sheet. This is in addition to supporting the review by obtaining prior approval for review and update of the configuration, if necessary. ○ Sample showing approval procedures form to update the Firewall Rules to ensure that no update or change is made without obtaining the approval of the representative. In addition, a sample showing what has been updated on the Firewall Rules. • Sample showing the implementation of requirements related to DNS including but limited to: ○ DNS security policy or configuration demonstrating the implementation of DNS security controls. ○ Screenshot showing DNS security configuration (e.g., DNSSEC, DNS filtering, DNS sinkhole, or equivalent DNS protection mechanisms). ○ Screenshot showing domain name configuration at the organization (DNS) indicating the use of a documented DNS address. ○ Screenshot of DNS Security that indicates IP range protection at the organization. • Sample showing the implementation of the requirements related to Internet

CNTL No.	Control Name	Control Guidelines
		browsing channel APT Protection, including but not limited to: ○ Sample showing the implementation of the requirements of Internet browsing channel APT Protection (e.g., a screenshot showing evidence of subscription and use of modern and advanced technologies to implement Internet browsing channel APT Protection and evidence of the APT Protection against zero-day malware.
TPC-2.60	Third Party must apply network segregation between production, test and development environments.	• Cybersecurity policy that covers all the requirements of network security management in the organization. • List of server addresses in production environment and development and testing environment. • An up-to-date network diagram document that shows logical segregation and clarifies the isolation between the production environment network from the development and testing networks.
TPC-2.61	Third Party must protect system development environments, testing environments (including data used in testing environment), and integration platforms.	• List of identified risks. • Evidence confirming the identification of preventative measures and ensuring the protection of data used in the testing environment.
TPC-2.62	Third Party must create and manage baseline configurations to harden information systems based on vendor recommendation and best practices.	• Baseline configuration documents. • Hardening checklists with vendor references. • System audit logs verifying compliance. • Configuration management tool screenshots.

CNTL No.	Control Name	Control Guidelines
TPC-2.63 	Third Party must adopt the multi-tier architecture principle.	• A document approved policy indicating the identification and documentation of the requirements related to this control. • Sample of application designs that demonstrate the use of a multi-tier architecture principle for the organization's application.
TPC-2.64	Backup media must be secured to prevent unauthorized physical access.	• Media handling and storage policy. • Physical access logs to media storage rooms. • Security controls (e.g., locked cabinets, safes). • Backup chain-of-custody records
TPC-2.65 	Multiple physical security measures must be implemented to prevent unauthorized access to facilities.	• Physical security policy. • Photos or diagrams of layered security (e.g., access card + biometric). • Maintenance records for physical barriers. • Physical security audit reports.
TPC-2.66 	Visitors' management process must be defined and implemented.	• Visitor management policy. • Visitor logbook or electronic system records. • Sample visitor badge issuance forms. • Sign-in/out procedures.
TPC-2.67 	All visitors accessing critical facilities must be escorted.	• Visitor escort policy. • Visitor sign-in/sign-out logs. • Staff instructions or duty roster showing escort responsibilities.
TPC-2.68 	All systems (routers, switches, servers, and firewalls) must be housed in a secure area (e.g., communication room) with controlled access.	• Physical security policy. • Access logs to server rooms. • Surveillance camera placement maps. • Visitor access approval forms.

CNTL No.	Control Name	Control Guidelines
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.	• Background screening or vetting logs. • Physical access control system reports. • Site photos or layout diagrams showing controlled room. • Policies banning devices and physical security check procedures.
TPC-2.70 	Third party must have: a) Centralized mobile device security management (MDM); b) Screen locking for end user devices.	• All mobile devices centrally managed in terms of security. • Sample of system configuration. • Screen lock policy enforced to user devices. • Documents illustrating user awareness methods for manually locking the screen when they are not in proximity to their devices.
TPC-2.71 	Third Party must follow OWASP best practices when developing software/applications for proponent.	• Secure Software Development Life Cycle (SSDLC) documentation. • References to OWASP Top 10 in developer guidelines. • Code reviews or static analysis scan reports. • Secure coding training completion logs.
TPC-2.72 	The Third Party must regularly provide certified security patches, system upgrades, and implementation guidance or recommendations related to cybersecurity.	• Patch management policy or procedures covering the provision of security patches, system upgrades, and cybersecurity guidance. • Records of notifications demonstrating communication of implementing guidance and recommendations.

CNTL No.	Control Name	Control Guidelines
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).	• API security policy. • API gateway configuration settings. • Sample code or architecture diagrams • Logs showing token issuance and rate limiting.
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).	• API inventory or registry screenshots. • API documentation. • Change management records for API updates. • Inventory review logs.
TPC-2.75 	API access tokens must be validated with every request.	• API gateway/token validation settings. • System logs showing token validation events. • Secure API design documentation. • Test cases showing token validation on calls.
TPC-2.76 	A timeframe must be defined and enforced for access token expiry to reduce the risk of unauthorized access.	• Token policy defining expiration rules. • Token issuance and expiry log samples. • API gateway or OAuth config showing token TTL. • Penetration test confirming token expiry enforcement.
TPC-2.77 	Third Party must protect information involved in application service transactions against possible risks (e.g.: incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure….)	• Web application firewalls appropriately configured. • Traffic inspection and behavioral monitoring established. • Access from known malicious or bad reputation sources denied. • Data transmission encryption and integrity protection layers (TLS/SSL) applied. • Evidence demonstrating message integrity protection mechanisms (e.g., digital signatures, message authentication

CNTL No.	Control Name	Control Guidelines
		codes (MAC), checksums, or equivalent controls). • Evidence demonstrating mechanisms to detect or prevent message mis-routing (e.g., routing validation, transaction verification, or secure routing configurations). • Regular application exposure to the internet review and unintentional data exposure detection established.
TPC-2.78	Cybersecurity requirements for usage of information and data media within the third party must be identified, documented and approved.	• Information and data media usage standard covering at minimum cybersecurity requirements TCP2.80 – TCP 2.84.
TPC-2.79	Cybersecurity requirements for usage of information and data media within the third party must be applied.	• Evidnece that cybersecurity requirmeents for Information and data are implemented (TCP2.80 – TCP 2.84)
TPC-2.80	Third Party must use secure means when disposing of media.	• Defined requirements and acceptable methods for disposal of media.
TPC-2.81	Third Party must ensure that media is labeled in human-readable format to explain its classification and the sensitivity of the information it contains.	• Evidence of stablished labelling rules. • Each media labeled according to established rules.
TPC-2.82	Third Party must ensure controlled and physically secure storage of removable media.	• List of identified risks for storing removable media. • Controls and requirements for secure storage of removable media.
TPC-2.83	Third Party must restrict and control the usage of portable media inside the Cloud Technology Stack.	• List of identified risks for using external storage media on the Cloud Technology Stack. • Approved restrictions and controls for using external storage media on the Cloud Technology Stack.
TPC-2.84	Third Party must periodically apply and review the cybersecurity requirements for usage of information and data media	• Cybersecurity requirements for usage of information and data media. • Periodical review logs.

CNTL No.	Control Name	Control Guidelines
TPC-2.85	Third Party must perform a monthly internal vulnerability scan on all internal computing resources to identify and remediate any vulnerability.	• Provide evidence of the third-party vulnerability management plan and ensure it includes the following: ○ Frequency of vulnerability scanning ○ Method for measuring the impact of vulnerabilities identified (e.g., Common Vulnerability Scoring System ○ Incorporation of vulnerabilities identified in other security control assessments (e.g., external audits, penetration tests) ○ Procedures for developing remediation of identified vulnerabilities ○ Provide evidence of samples of vulnerability scan reports. ○ Evindece of applying remediation of identified vulnerabilities.
TPC-2.86	Third Party must conduct periodic penetration testing and close all identified vulnerabilities. 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.	• Evidence of penetration testing reports conducted and analyzed covering Internet-facing services and technical components, including infrastructure, websites, web applications, mobile applications, email services, and remote access. • Penetration testing policy defining the testing schedule, scope, methodology, and reporting requirements. • Evidence of remediation plans and action plans addressing findings identified during penetration testing. • Evidence demonstrating closure or remediation of identified penetration testing vulnerabilities.
TPC-2.87	The scope of penetration tests must cover Cloud Technology Stack and must be conducted at least once every six months.	• Penetration tests conducted to the entire Cloud Technology Stack.

CNTL No.	Control Name	Control Guidelines
TPC-2.88	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.	• Vulnerability management policy with defined SLAs, • Patch management logs showing remediation timelines. • Vulnerability scan reports before and after remediation. • Exception handling records with documented mitigating controls, • Notifications and orrective action plans,
TPC-2.89	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 months for internal components of Cloud Technology Stack.	• Threat and Vulnerability Management Policy. • Sample of assessments. • Sample of remediation's plans and actions.
TPC-2.90	Third Party must notify proponent of identified vulnerabilities that may affect the proponent.	• Reports sent to proponent about detected vulnerabilities that impact them.
TPC-2.91	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	• Vulnerabilities management procedures that illustrate the classification mechanism. • Vulnerabilities detection and assessment reports indicating the classification of vulnerabilities.

CNTL No.	Control Name	Control Guidelines
	notifications on technical vulnerabilities.	• Policy and procedures that cover the security patch management requirements to address vulnerabilities. • Vulnerability assessment (before and after remedy) • List of communication channels subscribed in to receive alerts on new vulnerabilities.
TPC-2.92	Cybersecurity requirements for change management within the Third Party must be identified, documented and approved.	• Cybersecurity change management policy approved by the organization.
TPC-2.93	Cybersecurity requirements for change management within the third party must be implemented.	• Documents confirming the implementation of cybersecurity requirements for change management, as documented in the policy documented. • Document that clarifies an action plan for implementing cybersecurity requirements for change management.
TPC-2.94	Cybersecurity requirements for change management must be reviewed periodically.	• Log of updates and changes to the cybersecurity requirements for change management. • An approved document that sets the policy's review schedule. • Policy indicating that it has been reviewed and updated, and that changes have been documented and approved by the head of the organization.
TPC-2.95	Cybersecurity for change management in the 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).	• Change management procedures that include prioritizing the implementation of changes related to cybersecurity. • Evidence demonstrating verification of secure procedures during the execution of changes. • A document that contains procedures for implementing exceptional changes. • Evidence that shows technical capability for monitoring and control changes.

CNTL No.	Control Name	Control Guidelines
TPC-2.96 	Third Party must ensure secure management of cryptographic keys during their lifecycles.	• Cybersecurity policy that covers all the requirements of cryptography in the organization. • Cybersecurity procedure that covers all the requirements of cryptographic keys management in the organization. • Document that defines the technology effectiveness review cycle used for the secure management of cryptographic keys during their lifecycle. • Evidence that the secure management requirements for cryptographic keys are implemented throughout their lifecycle (e.g., a screenshot showing evidence to ensure that cryptographic key settings are configured to the best standard controls for the secure management of cryptographic keys during their lifecycle).
TPC-2.97 	Cybersecurity requirements for key management process within the Third Party must be identified, documented and approved.	• Key management standard that is formally approved and periodically reviewed. • Regular review reports.
TPC-2.98 	Cybersecurity requirements for key management process within the Third Party must be implemented.	• Cybersecurity requirements for key management process are implemented and followed as per defined policy and related documentations.
TPC-2.99 	Third Party must periodically review cybersecurity requirements for key management.	• Evidence of periodic review reports.
TPC-2.100 	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).	• Cryptographic key retrieval plan.
DETECT		
Continuous Monitoring		

CNTL No.	Control Name	Control Guidelines
TPC-2.101	Privileged accounts activity must be logged and monitored.	• Audit logs of privileged user actions. • Access control policy. • SIEM reports highlighting privileged activity.
TPC-2.102	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).	• 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).
TPC-2.103	Third Party must implement an automated monitoring and logging of remote access sessions event logs.	• Evidence of Remote sessions automatically monitored.
TPC-2.104	Third party must activate and monitor all audit trails of keys.	• Evidence demonstrating that audit trails for cryptographic keys are enabled and continuously monitored. • Sample audit logs capturing cryptographic key lifecycle events (e.g., key creation, activation, rotation, usage, modification, revocation, and deletion). • SIEM reports, alerts, or monitoring records demonstrating monitoring of cryptographic key audit trails. • Cryptographic key management policy or procedure defining logging and monitoring requirements for key-related events.
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.	• A document (such as approved policy or procedure) indicating the identification and documentation of the requirements related to this control. • Schedule of visit to the organization's buildings that contain surveillance cameras to assess their effectiveness, locations and monitoring.
Adverse Event Analysis		

CNTL No.	Control Name	Control Guidelines
TPC-2.106	Third Party must have cyber threat intelligence (incl. vulnerability intelligence) processes in place to be swiftly alerted for cyber threats exploiting relevant vulnerabilities and monitor/apply evolving mitigations to such vulnerabilities.	• Subscriptions to CTI feeds. • CTI integration evidence (dashboards, alerts). • Incident response records showing CTI inputs. • Patch and mitigation documentation linked to threat intelligence.
RECOVER		
Incident Recovery Plan Execution		
TPC-2.107	Third Party must conduct business continuity drills at least annually.	• Business Continuity Plan (BCP) document. • Drill execution reports or test results. • Attendance sheets or calendar invitations for the drill. • Post-drill lessons learned or improvement plans.
TPC-2.108	Third Party must ensure resilience and continuity of cybersecurity systems dedicated to the protection of Cloud Technology Stack.	• Document outlining enhanced measures to ensure resilience and continuity of cybersecurity systems dedicated to protecting the Cloud Technology Stack. • Periodical review reports and documents. • Evidence illustrating and methods ensuring resilience and continuity.
TPC-2.109	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.	• Documented and approved Backup and Recovery processes and precedures. • List of critical technologies and information assets. • Evidence of backup of critical technologies and information assets. • Evidence and reports of recovery drills performed on critical technologies and information assets. • Reports of backup performed following cybersecurity incidents
RESPOND		
Incident Management		

CNTL No.	Control Name	Control Guidelines
TPC-2.110 	Third Party **must** test incident response capability periodically.	• Incident response plan/procedure test schedule. • Report outlining the methodology for testing the cybersecurity incident response capabilities. • Lesson learned records.
Incident Analysis		
TPC-2.111 	Third Party **must** perform a root cause analysis of cybersecurity incidents and develop plans to address them.	• Root cause analysis is mandatory part of incident response. • Root cause analysis conclusions are prioritized and addressed. • Incident response plan is constantly improved based on root cause analysis conclusions. • Sample of root cause analysis.
Additional OT Requirements		
TPC-2.112 	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).	• A document (such as an approved policy or procedure) indicating the identification and documentation of the requirements related to this control. • OT cybersecurity awareness program approved by the head of the organization or his/her deputy. • OT cybersecurity awareness training content demonstrating coverage of: ○ account and access control hygiene; ○ portable media and malware control; ○ incident and event reporting; and ○ security maintenance discipline (including patching, hardening, and system integrity). • Action plan to implement the OT cybersecurity awareness program adopted by the organization. • Awareness materials or training records demonstrating that the OT cybersecurity

CNTL No.	Control Name	Control Guidelines
		awareness program has been delivered to personnel with access to OT assets. • List of beneficiaries of the OT cybersecurity awareness program.
TPC-2.113	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.	• Evidence of conducted comprehensive security architecture review for OT/ICS products, ensuring they are designed with security in mind from the ground up. • Evidence of performed threat modeling exercises specific to the OT/ICS domain to identify potential threats and vulnerabilities early in the design phase. • Evidence of configuration OT/ICS products with secure defaults, ensuring that unnecessary services are disabled, and default passwords are changed before deployment.
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).	• Valid certification demonstrating compliance with IEC 62443-4-1 and IEC 62443-3-3 (refer to Appendix D for the certification requirements).

CNTL No.	Control Name	Control Guidelines
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).	• 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).	• Valid organizational-level certification demonstrating compliance with IEC 62443-2-4 (refer to Appendix D for the certification requirements).

7. Cloud Service Model Applicability

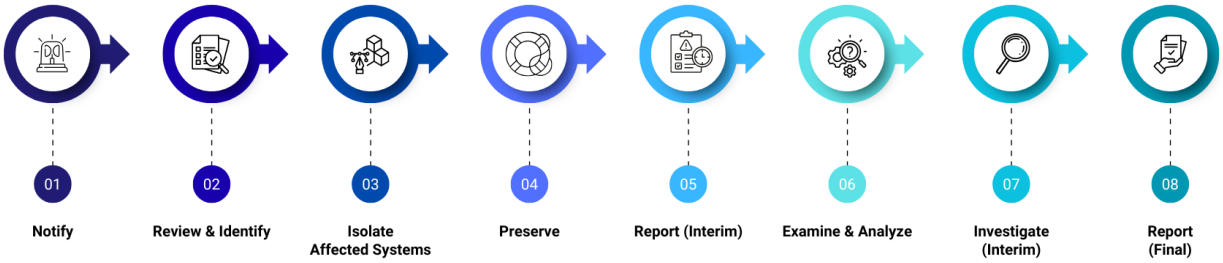
Control #	IAAS	PAAS	SAAS
TPC-2.1	✓	✓	✓
TPC-2.2	✓	✓	✓
TPC-2.3	✓	✓	✓
TPC-2.4	✓	✓	✓
TPC-2.5	✓	✓	✓
TPC-2.6	✓ (Cloud Technology Stack)	✓ (Cloud Technology Stack)	✓ (Cloud Technology Stack)
TPC-2.7	✓	✓	✓
TPC-2.8	a) ✓ b) ✓ c) ✓	a) ✓(Resources and Cloud Technology Stack) b) ✓ (Resources and Cloud Technology 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 twenty-four (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, 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

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:

- The Third Party's Name;
- The 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:

- The Third Party's Name;
- The Third Party's Incident Coordinator and contact information;
- The proponent 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 the Incident impact (i.e., Reputational, operational, customer, financial and legal);
- Incident details:
  1. List of individuals and other Third Parties that were involved with any aspect of the Incident handling;
  2. How/when the Incident was initially detected;
  3. How/when the Incident was initially reported to Proponent;
  4. Description of what resources/services were impacted;
  5. Description of Incident's impact to Proponent (volume and type where applicable);
  6. Containment - How was the Incident contained;
  7. Root Cause - What was the cause for disruption;
  8. Corrective action during the Incident – What steps were taken to reduce exposure during the Incident (in most cases, there are interim steps taken to reduce exposure, e.g., Filtering, rerouting services, etc);
  9. Permanent corrective actions/preventative measures – What permanent corrective actions have been put in place as a result of this Incident?;
  10. 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	Third Party computing infrastructure is provided with network connectivity (e.g., SSL VPN, Leased line) to the Corporate Network.
Outsourcing & Managed Services	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	Third Party is processing or storing Corporate Critical Data or maintaining Critical Systems.
Customized Software third-party	Third Party is developing software for the corporation.
Cloud Computing Service third-party	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))