Third Party Cybersecurity Controls Guideline

12/7/2022

Table of Contents

Objective

The objective of Third Party Cybersecurity Compliance Certification Program is to ensure all third parties adherence to the cybersecurity requirements in SACS-002 Third Party Cybersecurity Standard by obtaining a Cybersecurity Compliance Certification form an Authorized Audit Firm. This manual will provide the third party with the required guidance to fulfill the cybersecurity controls' requirements for each control. This will ensure that supported, required and comprehensive evidences are provided part of the third party compliance package that will be submitted to authorized audit firm.

Cybersecurity Controls' Requirement

The cybersecurity controls guidance document must be used as a reference to ensure unified expectations for the evidences to be provided for each cybersecurity control. The guideline must be utilized for remote assessments where third parties must provide a comprehensive assessment package in accordance to all the controls' requirements stated in this document. Moreover, this guideline can be used for on-site assessments where audit firms can verify the evidences against each control's requirements. In case of inapplicability, third party must fill the inapplicability form with required justifications for each inapplicable control.

1. General Requirements

Control #	Control Statement	Controls' Requirements
TPC-1	Third Party must establish, maintain and communicate a Cybersecurity Acceptable Use Policy (AUP) governing the use of Third Party Technology Assets.	- Provide a copy of approved (AUP) - Provide sample of communication regarding sharing (AUP) to employees - Provide different versions of approved and communicated AUP, that shows different releases and updates
TPC-2	Password protection measures must be enforced by the Third Party. The following are recommended measures: - Minimum length: 8 alphanumeric characters and special characters. - History: last 12 passwords - Maximum age: 90 days for login authentication - Account lockout threshold: 10 invalid login attempts. - Screen saver settings: automatically locked within 15 minutes of inactivity.	- Provide technical check evidence to confirm the compliance of the control requirements. - Provide evidence of the password configuration on Active directory to ensure that default settings are not used. If active directory does not exist, provide evidences from the local password policy on sample systems. - Provide a copy of password policy that should comply with the control requirements and technical check findings.
TPC-3	Third party must not write down, electronically store in clear text, or disclose any password or authentication code that is used to access Assets or Critical Facilities.	- Provide a copy of password disclosure policy - Provide a copy of actions taken in case password disclosure happened part of the consequence management

Control #	Control Statement	Controls’ Requirements
TPC-4	Multi-factor authentication must be enforced on all remote access, including access from the Internet, to Third Party Company computing resources.	- Provide technical check evidence to confirm that strong authentication is in place on remote users’ access (e.g., multifactor) a clear evidence of the Authentication page must be provided. - Provide policies and procedures related to remote users' access policy part of the third party access control policy.
TPC-5	Multi-factor authentication must be enforced on all access to Cloud services utilized by the Third Party, including access to cloud-based email.	- Provide technical check evidence to confirm that strong authentication is in place on cloud access (e.g., multifactor) a clear evidence of the Authentication page must be provided. - Provide policies and procedures related to cloud security policy part of the third party access control policy.
TPC-6	Third Party must inform Saudi Aramco when employees provided with Saudi Aramco user credentials no longer need their access, or are transferred, re-assigned, retired, resigned or no longer associated with the Third Party.	- Provide the third party policy/contract in term of dealing with Saudi Aramco credentials. - Provide a sample of communication (Email) to Saudi Aramco to revoke invalid accounts. - Provide evidence for revoked accounts that are invalid accounts for people who are retired, resigned or no longer associated with the Third Party.
TPC-7	Third Party must require all information systems users to take a yearly mandatory Cybersecurity training that addresses acceptable use and good computing practices. Training must address the following topics: 1. Internet and social media security 2. Cybersecurity Acceptable Use 3. Social Engineering and phishing emails 4. Sharing credentials (i.e. username and password) 5. Data Security	- Provide acceptable use policy and/or training materials to ensure content is adequate. - Provide user training reports and/or documentation to ensure users are trained in accordance with applicable policy, guidance, and/or requirement (e.g., annual cybersecurity training of all employees). - Provide evidences of updating the training materials based on changes in cyber threat environment.
TPC-8	Third Party must inform personnel, in keeping with Third Party Company Policy, that using personal email to share and transmit Saudi Aramco data is strictly prohibited.	- Provide Third Party Company Policy and contract of using personal email. - Provide the Third Party policy / contract ensure third parties are complying with cybersecurity responsibilities defined in contracts and agreements. -Provide related emails communicated to third party’s employees to ensure the compliance of this control. - Provide relevant counter measure that third party has taken to comply with the control requirements.

Control #	Control Statement	Controls' Requirements
TPC-9	Third Party must inform personnel, in keeping with Third Party Company Policy, that disclosing Saudi Aramco policies, procedures and standards or any type of data with unauthorized entities or on the Internet is strictly prohibited.	- Provide Third Party policy including contracts and agreements that highlight the prohibited disclosure of Aramco related data. -Provide related emails communicated to third party's employees to ensure the compliance of this control - Provide relevant counter measure that third party has taken in case of disclosing Saudi Aramco Data
TPC-10	All Third Party Technology Assets and Systems must be password protected.	- Provide evidence of related assets management policy that define Technology assets' protection. -Provide evidence of related policy for all third party systems to be password protected.
TPC-11	Third Party Technology Assets and Systems must be regularly updated with operating system (OS), software and applets patches (i.e. Adobe, Flash, Java etc.)	- Provide evidence of patch management policy and procedures - Provide evidence of on sample of workstations to ensure that OS and software are up-to-date - Provide evidence of scheduling and technology used for patch and updates deployment.
TPC-12	Third Party Technology Assets must be protected with anti-virus (AV) software. Updates must be applied daily, and full system scans must be performed every two weeks.	- Provide evidence of the anti-virus installed on endpoint devices - Provide evidence of configuration console of the installed anti-virus software to determine the last updates and full system scan that were performed - Provide evidence of the history of updates
TPC-13	Third party must implement Sender Policy Framework (SPF) technology on the mail server.	- Provide evidence of SPF implementation on the third party mail server.
TPC-14	Third party must enforce Sender Policy Framework (SPF) feature on Saudi Aramco email domains: Aramco.com and Aramco.com.sa.	- Provide evidence of SPF enforcement on Saudi Aramco email domains: Aramco.com and Aramco.com.sa.
TPC-15	Third Party must publish SPF record in DNS server.	- Provide evidence of SPF record on the third party DNS server.
TPC-16	Third Party must inspect all incoming emails originating from the Internet using anti-spam protection.	- Provide evidence of using an anti-spam protection for all incoming emails on the email security appliance.
TPC-17	Third Party must use a private email domain. Generic domains, such as Gmail and Hotmail, must not be used.	- Provide 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.
TPC-18	Third Party must have formal procedures for off-boarding employees. Off-boarding procedures must include the return of assets, and removal of all associated access.	- Provide evidence of the third party termination procedures to determine whether accounts/access are disabled in a timely manner. -Provide evidence of the return of assets. - Provide samples of the removal of all access to Assets part of the third party Off-boarding procedures.

Control #	Control Statement	Controls' Requirements
TPC-19	Assets used to process or store Saudi Aramco data and information must be sanitized by the end of the Data Life Cycle, or by the end of the retention period as stated in the Contract, if defined. This includes all data copies such as backup copies created at any Third Party site(s).Third party shall certify in writing to Saudi Aramco that the data sanitization has been completed.	- 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 proof (e.g., destruction certificates) that media sanitization is occurring according to policy
TPC-20	Third Party must obtain a Cybersecurity Compliance Certificate (CCC) from Saudi Aramco authorized audit firms in accordance to the third-party classification requirements set forth in this Standard (Section II). Third Parties must submit the CCC to Saudi Aramco through the Saudi Aramco e-Marketplace system.	- Saudi Aramco third parties must obtain a Cybersecurity Compliance Certificate (CCC) from Saudi Aramco authorized audit firms, which provides the adherence to this standard. -In case CCC has been previously obtained, an evidence of certificate submission should be provided.
TPC-21	Third Party must renew the CCC every two (2) years.	- Saudi Aramco third parties must renew the CCC every two (2) years as per the standard requirements. -A copy of latest CCC obtained needs to be provided.
TPC-22	Firewalls must be configured and enabled on endpoint devices.	- Provide evidence of the firewall setting for all third party endpoint devices including related policies for enabling firewalls. - Provide evidence of the firewall being enabled on domain, public and private firewall settings on sample of third party endpoint devices.
TPC-23	If Third Party discovers a Cybersecurity Incident, Third Party must (besides its continuous efforts to resolve and mitigate the Incident): - Notify SAUDI ARAMCO within two (24) hours of discovering the Incident - Follow the Cybersecurity Incident Response Instructions set forth in Appendix A.	- Provide evidence of the third party cybersecurity Incident management policies and procedures that conform with the requirements of this control.

2. Specific Requirements

Control #	Control Statement	Controls' Requirements
TPC-24	Third Party must have policies and processes to classify information in terms of its value, criticality and confidentiality.	- Provide evidence of the third party data classification policy - Provide evidence of the third party Data Classification program that cover all key resources (e.g., hardware, devices, data, software) are classified based on risk
TPC-25	Third Party must establish, maintain and communicate Cybersecurity Policies and Standards.	- Provide evidence of the third party Cybersecurity Policies and Standards. - Provide evidence of communicating Cybersecurity Policies to employees. - Provide different policy updates versions
TPC-26	Third Party must be staffed by employee(s) whose primary responsibility is Cybersecurity. Responsibilities of that personnel must include maintaining the security of information systems and ensuring compliance with existing policies.	- Provide a copy of the organizational chart. - Provide evidence of job descriptions, agreements, RACI charts, service level agreements (SLAs) and/or contracts to determine if they include cybersecurity roles and responsibilities.
TPC-27	Third Party must conduct annual external Penetration Testing on its IT infrastructure systems, and internet facing applications.	- Provide evidence of Penetration testing reports conducted and analyzed on IT infrastructure considering all critical, internal and external systems, and internet facing applications. - Provide evidence of a policy tackling penetration test schedule, scope and requirements exist and communicated to stakeholders - Provide evidence of remediation and action plan related to penetration test results.
TPC-28	Third Party must conduct annual external Penetration Testing on Cloud Computing Service(s) used by Saudi Aramco.	- Provide evidence of Penetration testing reports conducted on Cloud Computing Service(s) used by Saudi Aramco. - Provide evidence of a policy tackling penetration test schedule, scope and requirements exist and communicated to stakeholders - Provide evidence of remediation and action plan related to penetration test results.
TPC-29	If Third Party is hosting a website for Saudi Aramco, annual Penetration Testing must be conducted to test website security.	- Provide evidence of Penetration testing reports conducted to test website security. - Provide evidence of a policy tackling penetration test schedule, scope and requirements exist and communicated to stakeholders - Provide evidence of remediation and action plan related to penetration test results.
TPC-30	Third party data center must be certified by an internationally-recognized authority.	-Provide evidence of data center certificate from internationally-recognized authority.

Control #	Control Statement	Controls’ Requirements
TPC-31	Third Party must have a process to conduct Cybersecurity Risk Assessment on regular basis, to identify, assess and remediate Risks to data and information systems.	- Provide evidence of the framework or process used for risk management. Consider the following. - Provide evidence of the organization's risk management plan showing the organization's response to risk levels - Provide evidence of risk register - Provide evidence of risk management plan that is designed to accept or reduce risk level in accordance with the organization's risk appetite/ tolerance.
TPC-32	Users accessing applications and information systems must be issued unique user logins and passwords. Generic accounts must not be allowed, unless explicitly approved, restricted and controlled.	- Provide evidence of access management policy that shows the requirement of using unique accounts. - Test sample of servers/ systems to determine if unique account is used for on-site assessment.
TPC-33	User access to the operating system, applications and database must be reviewed on a semiannual basis to determine if accessing personnel still require such access.	- Provide evidence of access management policy. - Provide evidence of user access profiles are consistent with their job functions (based on least privilege). - Provide evidence of role-based access controls are implemented (e.g., roles vs. users are assigned access rights). - Provide evidence that ensure excessive permission are not granted.
TPC-34	All privileged accounts must be limited, justified and reviewed on regular basis.	- Provide evidence of a policy that shows the procedure of obtaining and revoking the admin privileges based on the job requirements/ function - Provide evidence of the third party process to identify privileged users. - Provide evidence of privileged accounts reviewed regularly.
TPC-35	Remote administrative access from the Internet must not be allowed, unless explicitly approved, restricted and controlled.	- Provide evidence of policies and procedures related to remote users' access capabilities are explicitly approved, restricted and controlled. Consider that remote connections are only opened as required and remote connections are encrypted.
TPC-36	Network connections to information systems and applications at the Third Parties location must be authorized and monitored.	- Provide evidence of policies and procedures related to remote users' access capabilities are formalized. Consider that remote users (e.g., employees, contractors, third parties) with access to critical systems are approved and documented and remote connections are logged and monitored.

Control #	Control Statement	Controls' Requirements
TPC-37	Multi-factor authentication must be enforced on all privileged accounts access including remote access to information systems and applications.	- Provide evidence of policies enforcing the use of Multi-factor authentication on all privileged accounts access including remote access to information systems and applications. - Provide evidence of Multi-factor authentication page and configuration console.
TPC-38	Third Party must logically (e.g. partitioning a physical drive) and/or physically segregate data-at-rest related to Saudi Aramco from the data of other clients or customers.	- Provide evidence of logical segregation on physical drives use to store Saudi Aramco data. - Provide evidence of physical segregation including dedicated data room/ files for Saudi Aramco data. - Provide evidence of Third Party Policy of treating third party data including Saudi Aramco.
TPC-39	Saudi Aramco Critical Data documents must only be shared with limited individuals who are part of the work specified in the Contract.	- Provide evidence of Saudi Aramco Critical Data documents are classified and differentiated from other critical data. - Provide evidence of Third Party Policy of sharing Saudi Aramco data.
TPC-40	Servers and workstations subnets must be segmented and access between them is restricted and monitored.	- Provide evidence of server and workstation subnets are segmented. - Provide evidence of a range of subnets assigned on different assets - Provide evidence of monitoring the segmentation.
TPC-41	Servers accessible from the Internet must be placed in a DMZ (i.e. perimeter network) with restricted access to internal subnets.	- Provide evidence of high-value/critical systems are separated from high-risk systems (e.g., VLAN, DMZ, hard backups, air-gapping) where possible. - Provide evidence of network diagrams and data flow diagrams. - Provide evidence of monitoring the traffic travels between different DMZ zone and internal subnets.
TPC-42	Wireless networks accessing information systems must use strong encryption for authentication and transmission, such as WPA2 or WPA2 Enterprise.	- Provide evidence of access point configuration. - Provide evidence of Wireless baseline details.
TPC-43	Third Party data center must have the required tier rating and high-availability of service fail over as determined by Saudi Aramco	-Provide evidence of data center tier rating. -Provide evidence of and high-availability of service fail over.

Control #	Control Statement	Controls' Requirements
TPC-44	Multi-Factor authentication must be enforced on Saudi Aramco users accessing Cloud Service Provider's Public Cloud Computing Service storing or hosting Saudi Aramco Critical Data.	- Provide technical check evidence to confirm that strong authentication is in place on Saudi Aramco users accessing Cloud Service Provider's, Public Cloud Computing Service storing or hosting Saudi Aramco Critical Data. (e.g., multifactor) - A clear evidence of the Authentication page must be provided. - Provide policies and procedures related to cloud security policy part of access control policy.
TPC-45	Multi-Factor authentication must be enforced on end-users accessing Content Management Services (CMS) of Cloud Computing Service	- Provide technical check evidence to confirm that strong authentication is in place on Content Management Services (CMS) of Cloud Computing Service (e.g., multifactor) - A clear evidence of the Authentication page must be provided. - Provide policies and procedures related to cloud security policy part of access control policy.
TPC-46	All systems (routers, switches, servers and firewalls) must be housed in a communication room and locked rack(s). The access to the communication room must be contingent on security requirements such as access card readers or biometric devices.	- Provide evidence of Physical security controls are used to prevent unauthorized access to telecommunication systems. - Provide evidence of access is restricted to authorized people.
TPC-47	Third party must define a process for visitor management. The process should include maintaining and regularly reviewing visitor logs. The visitor log should capture information such as: - Visitor identification e.g. Government ID - Visit Purpose - Check in/check out date and time	- Provide evidence of the third party visitor management policy - Provide evidence of visitor logs, including the following: - Visitor Government ID - Visit Purpose - Check in/check out date and time
TPC-48	Visitors accessing Critical Facilities must be escorted at all times.	- Provide evidence of a policy that state the requirement of escorting visitors accessing critical facilities on the company premise.
TPC-49	Third Party must dedicate an access restricted working area for personnel with access to Saudi Aramco network.	- Provide evidence of dedicated working area is allocated for Saudi Aramco projects and workstations. - Provide evidence of physical security control implementation on Aramco working area.
TPC-50	Backup media must be secured to block/inhibit unauthorized physical access.	- Provide evidence of backup media physical security controls implemented. - Provide evidence of backup media related policy and configuration.

Control #	Control Statement	Controls' Requirements
TPC-51	Technology Assets and Systems connected to the internet must be licensed and supported by the provider.	- Provide evidence of third party asset management inventory, determine system and assets connected to the internet are licensed and supported by the provider.
TPC-52	Third Party must encrypt data in transit (e.g. SSH, FTPS, HTTPS, IPSEC).	- Provide evidence of web security appliance to ensure that encryption technology is used and enabled when data is transmitted across publicly-accessible networks. - Provide evidence of adequate policies are in place regarding transmission of data, especially the one transmitted via email.
TPC-53	Third Party must encrypt (e.g. using HTTPS) sessions where Critical Saudi Aramco information or data will be transmitted from and to the Public Cloud Computing Services, and enforce session authentication, lockout, and timeout.	-Provide evidence of applied configurations from the available security appliance, showing the use of secure transmission protocols. - Provide evidence of configurations for session authentication enforcement, lockout, and timeout.
TPC-54	Third Party must implement encryption mechanisms, using at least AES encryption algorithm, and 256 bit key, on all devices or storage media hosting sensitive data per the Third Party's assets classification policy.	- Provide evidence of encryption mechanisms applied on all devices, including disk drives by checking BitLocker Drive encryption. - Provide evidence of a policy ensuring mobile devices (e.g., laptops, tablets, and removable media) that are used to store confidential data are encrypted.
TPC-55	Encryption key management capability, including preservation and retrieval, must be defined, applied, and periodically reviewed.	-Provide evidence of encryption key management procedure and policy. -Provide evidence of key management configurations
TPC-56	Third Party must implement a device control mechanism on Assets that are used to receive, store, process or transmit Saudi Aramco data such as disabling the use of external storage media.	- Provide evidence of assets used to perform/conduct Aramco business with removable media restrictions to ensure restrictions are working as expected and comply with the organization's policy. - Provide evidence of the removable media policy, which may include: - Encryption of removable media - Restricted access to removable media (e.g., USB restrictions)

Control #	Control Statement	Controls' Requirements
TPC-57	Access to the Internet must be restricted by Content-filtering technologies to block: • Malicious and suspicious websites. • Personal and non-company email services. • Personal and non-company approved public cloud services.	- Provide evidence of the technology used for content filtering - Provide evidence of no related business site like malicious websites, personal, non-company email Services, non-company approved public cloud services being blocked. - Provide evidence of appropriate configuration for accessing web-based email, cloud Storage services.
TPC-58	Documents containing Saudi Aramco Critical Data, must be encrypted and stored securely with access limited to authorized personnel.	- Provide evidence of policy where documents must only be shared with limited individuals who are part of the work specified in the Contract. - Provide evidence of documents with Passwords to unlock these documents: - Must never be stored. - Must never be shared in the same communication method (e.g. email) as the documents. - Must be communicated to the recipient(s) over the phone, in person or via SMS text message. - Must be in line with the password protection measures stated in Control Number "TPC-2" in this Standard in agreement with a Saudi Aramco eligible recipient of the document. -Provide evidence for hardcopy documents being stored securely in dedicated and locked cabinet with access limited to authorized personnel.
TPC-59	Remote wipe solution must be installed on all tablets and mobile phones used to receive, store and/or produce Critical Data for Saudi Aramco.	- Provide evidence of ability to wipe data remotely on mobile devices when data are missing or stolen is enabled. - Provide evidence of policy related to remote access and remote wipe solution used
TPC-60	Third Party must implement data validation on all input fields for applications or Cloud Computing Services used by Saudi Aramco to only accept input with valid data type, syntax and length range	- Provide evidence of Test sample input fields for accepting valid data types, syntax and length range part of the user accepting testing. - Provide evidence of Data Validation policy. - Provide evidence of applied configuration.
TPC-61	Application error messages must not display any technical information.	- Provide evidence of error messages handling part of the application design document. - Provide evidence of samples of error messages generated by the application. - Provide evidence of the login failure for username and password. The error messages. - Provide evidence of Secure Programming Policy.

Control #	Control Statement	Controls’ Requirements
TPC-62	Application or Cloud Computing Services must not store, generate, transmit, or use plain-text passwords.	- Provide evidence of application password management policy. - Provide evidence of security controls applied on application passwords including: encryption and the use of hash function. - Provide evidence of the configuration file of the application. -Provide evidence of LDAP and Active Directory in case it was use for authentication.
TPC-63	Third Party must create and manage baseline configurations to harden information systems. The hardening process must address configurations such as: - Resetting default usernames/passwords - Disabling unneeded software - Disabling unneeded services - Removing administrative access of users on workstations.	- Provide evidence of the baseline configurations for systems (e.g., servers, desktops, routers). - Provide evidence of samples against the third party's baseline configurations to ensure standards are followed and enforced, for the following: - Resetting default usernames/passwords - Disabling unneeded software - Disabling unneeded services - Removing administrative access of users on workstations.
TPC-64	Third Party must establish and follow regular procedures for backup of critical systems and Saudi Aramco’s data, software and websites.	- Provide evidence of third party backup policy, process and procedures. - Provide evidence of a formal backup is performed with defined schedule. - Provide evidence of periodic backup testing is performed to verify data are accessible and readable.
TPC-65	Backup stored at an off-site location must be encrypted using at least AES encryption algorithm, and 256 bit key, except for data classified as public.	- Provide evidence of third party backup policy, process and procedures. - Provide evidence of the backup tapes are encrypted for off-site location.
TPC-66	Third Party must implement a sanitization process before any Assets are loaned, donated, destroyed, transferred, or surplused. The process must be aligned to industry best practices such as NIST 800-88.	- Provide evidence of media 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 proof (e.g., destruction certificates) that media sanitization is occurring according to policy.

Control #	Control Statement	Controls' Requirements
TPC-67	Third Party must have a Disaster Recovery Plan (DR Plan) which is documented, maintained and communicated to appropriate parties. The DR Plan should address the recovery of Assets and communications following a major disruption to business operations.	- Provide evidence of Disaster Recovery plans addressing the control requirements. - Provide evidence of samples of communicating DR to responsible parties and stakeholders.
TPC-68	Third Party must have a comprehensive Business Continuity (BC) plan which is documented, maintained and communicated to appropriate parties. The BC plan should address the occurrence of the following scenarios: a) Equipment failure. b) Disruption of power supply or communication. c) Application failure or corruption of database. d) Human error, sabotage or strike. e) Malicious Software attack. f) Hacking or other Internet attacks. g) Social unrest or terrorist attacks. h) Environmental disasters. i) Emergency contact information for personnel.	- Provide evidence of business continuity plans to determine if the third party has documented how it will respond to a cyber-incident. - Provide evidence of the BC plan, which includes all the related subjects/ topics of the control requirements.
TPC-69	Third Party must ensure that owners of the Business Continuity (BC) plan are identified and that the BC plan is reviewed and updated annually.	- Provide evidence of the plan to ensure that Business Continuity (BC) plan owners are identified. - Provide evidence of different plans releases to determine how frequently they are updated and approved.
TPC-70	Third Party must conduct Business Continuity drills at least annually.	- Provide evidence of business continuity tests / drills are performed according to the policy as required by the control.
TPC-71	Third Party must have formal procedures for on-boarding employees. On-boarding procedures must include background checks (e.g. Verification of work histories).	- Provide evidence of hiring procedures to determine whether background checks/screenings are performed for all employees. - Provide HR screening policy.
TPC-72	Third Party must conduct security and source code vulnerability scanning on all developed applications, and close all discovered vulnerabilities before deployment in production.	- Provide evidence of different security scans and vulnerability reports found on all developed applications. - Provide evidence of remediation of all security issues and findings discovered and closed prior the deployment in production. - Provide Application Vulnerability scanning policy.

Control #	Control Statement	Controls' Requirements
TPC-73	All changes to the application must be properly authorized and tested in a testing environment before moving to production.	- Provide evidence of application design packages and testing reports that show different application testing conducted by the authorized testing team. - Provide evidence of different testing results conducted on testing environments including (production and quality assurance) - Provide evidence of approved change requests to applications prior deployment.
TPC-74	Third Party must have a process for secure system and software development life cycle in alignment with industry best practice.	- Provide evidence of implemented process for secure system and software development life cycle.
TPC-75	Third Party must retain all audit logs from information systems and applications storing, processing or transmitting Saudi Aramco data for one (1) year.	- Provide evidence of audit logs (e.g., security, activity) are maintained and reviewed in a timely manner. - Provide evidence of Log files are sized such that logs are not deleted prior to review and/or being backed up. - Provide evidence of the third party policy of logs handling - Provide evidence of Audit logs and log management & analysis tools that are protected from unauthorized access, modification and deletion. - Provide evidence of Audit records contain appropriate content (e.g., type of event, when the event occurred, where the event occurred, source of the event, and outcome of the event, identity of any individuals or subjects associated with the event).
TPC-76	Firewalls must be implemented at the network perimeter and only required services must be allowed. Vulnerable services or insecure protocols should be blocked.	- Provide evidence of firewall settings ensure that rules are configured to allow only required services and unneeded protocols and vulnerable services are closed and blocked. - Provide evidence of network diagram for firewalls placement.
TPC-77	Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS) must be implemented at the network perimeter.	- Provide evidence of IPS/IDS configurations and enablement.
TPC-78	Signatures of firewalls, IDS and IPS must be up-to-date.	- Provide evidence of firewalls, IDS and IPS signature up-to-date.
TPC-79	If Third Party is hosting an application or a website for Saudi Aramco or providing cloud-based web application, Web Application Firewall (WAF) must be implemented to inspect all incoming traffic for potential threats and malicious activity e.g. SQL injection and Cross Site Scripting	- Provide evidence of implementing Web Application Firewall (WAF). - Provide evidence of the WAF configuration and activation.

Control #	Control Statement	Controls’ Requirements
TPC-80	Third Party must monitor Technology Assets, Systems and applications to identify unauthorized access, or unauthorized activity.	- Provide evidence of policies and procedures regarding system and network monitoring. - Provide evidence of detected events (e.g., alerts from IDS) and the organization's response to them. Review the events and responses to ensure thorough analysis of detected events is performed.
TPC-81	Third Party must periodically aggregate and correlate data from multiple systems and critical applications such as Firewalls, IDS/IPS, and anti-virus in a central repository for event monitoring and analysis purposes.	- Provide evidence of listing of event aggregation and monitoring systems in use at the organization (e.g., SIEMs, event log correlation systems). - Provide evidence of list of sources that provide data to each event aggregation and monitoring system (e.g., firewalls, routers, servers).
TPC-82	Multiple physical security measures must be implemented to prevent unauthorized access to facilities. Entrances and exits must be secured with authentication card key, door locks and monitored by video cameras.	- Provide evidence that physical access to key assets (e.g., server rooms, network closets, zones) are physically restricted: a. Locked doors b. Surveillance c. Fences or walls d. Logs e. Visitor escorts - Provide evidence of policies and procedures allow only authorized personnel access to sensitive areas. - Provide evidence of termination /off-boarding procedures to ensure physical access is removed once an employee leaves.
TPC-83	Privileged accounts activity must be logged and monitored on a regular basis.	- Provide evidence of policies highlighting the monitoring of Privileged accounts activity. - Provide evidence of logged Privileged accounts activity.
TPC-84	Non-authorized devices (such as personal devices and mobile phones) must not be used to store, process or access Assets.	- Provide evidence of policies of using personal assets.
TPC-85	Monthly Vulnerability scans must be conducted to evaluate configuration, Patches and services for known Vulnerabilities.	- 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. - Provide Vulnerability scanning policy.

Control #	Control Statement	Controls' Requirements
TPC-86	Physical access to the facility where information systems reside must be restricted to authorized personnel and reviewed on a regular basis.	- Provide evidence of an inventory of critical facilities (e.g., data centers, network closets, operations centers, critical control centers). - Provide evidence of physical security monitoring controls are implemented and appropriate to detect potential cybersecurity events (e.g., sign in/out logs, motion detectors, security cameras, security lighting, security guards, door/window locks, automatic system lock when idle, restricted physical access to servers, workstations, network devices, network ports).
TPC-87	Information systems and applications must log auditable events as stated in Appendix C.	- Provide a list of the monitoring controls implemented by the third party at the application/user account level (e.g., account management, user access roles, and user activity monitoring, file and database access). - Provide evidence of monitoring reports includes detection and alerting of cybersecurity events (e.g., unauthorized account access, unauthorized file/system access, access out of hours, access to sensitive data, unusual access, unauthorized physical access, privilege escalation attacks). - Consider Appendix C on Third Party Standard.
TPC-88	Incident management policy and plan must be documented, maintained and communicated to management and appropriate team members.	- Provide evidence of incident management policy and procedures to determine if reporting structure and communication channels are clearly defined. - Provide evidence that employees are trained to report suspected security incidents. - Provide copies of reports from recent incidents to validate reporting is consistent and follows the plan.
TPC-89	Third Party must have an Incident Response capability that includes preparation, detection and analysis, containment, eradication, recovery, documentation and preservation of evidence, communication protocols and lessons learned.	- Provide evidence of the incident response plan to determine if appropriate steps are taken consider the following: 1. Obtain evidence of event notifications (e.g., detection alerts, reports) from different systems. 2. Determine who receives alerts or reports from detection systems and what actions are taken once reports are received. 3. Review the incident response plan to determine if actions taken follow the plan.

Control #	Control Statement	Controls' Requirements
		4. Steps to contain and control the incident to prevent further harm 5. Procedures to notify potentially impacted third parties 6. Strategies to control different types of incidents (e.g., distributed denial-of-service [DDoS], malware, etc.) 7. Steps to mitigate the incident to prevent further harm 8. Review any documented incidents to determine whether mitigation efforts were implemented and effective 9. Review the organization's incident handling reports and incident testing documentation for action items and lessons learned.
TPC-90	Third Party must track, classify and document all Cybersecurity Incidents.	- Provide evidence of the incident response plan to determine if there is a process to formally analyze and classify incidents based on their potential impact. - Provide incident response plan to determine if it is designed to prioritize incidents, enabling a rapid response for significant incidents or vulnerabilities.
TPC-91	Third Party must resolve or mitigate the identified security Vulnerabilities on a system, computer, network, or other computer equipment within the following timeframes: - Critical Risk: immediate correction up to fourteen (14) calendar days of critical vendor patch release, notification from Saudi Aramco, or discovered security breach whichever is earlier. - High Risk: within one (1) month of vendor patch release, or discovered security breach whichever is earlier. - Medium and Low Risk: within three (3) months of discovery.	- Provide evidence of the organization's schedule for performing internal and external vulnerability scans and the results of the most recent internal and external vulnerability scans. - Review the schedule and results for the following: - Frequency - Successful completion - Documented resolution or mitigation of identified vulnerabilities - Scope of testing includes all critical systems - Provide evidence of vulnerability scan results were reported to individuals or teams with appropriate authority to ensure resolution. - Provide Vulnerability scanning policy.
TPC-92	f Third Party is hosting a website for Saudi Aramco or providing a Cloud Computing Service, the website / Cloud Computing Service must be secured by a Distributed Denial of Service (DDOS) protection.	- Provide evidence that the third party is deploying Distributed Denial of Service (DDOS) protection appliance that sit in front of network firewalls. - Provide evidence that the third party is deploying web application firewalls, and use load balancers.