

Third Party Cybersecurity Compliance Report

Report #: [To be Filled by Audit Firm]

**[Third Party Company Name]**

Table of Contents

[1. Third Party Information 3](#_Toc101084659)

[2. Audit Firm Information 4](#_Toc101084660)

[3. Guidelines 4](#_Toc101084661)

[4. Assessment Controls 6](#_Toc101084662)

[General Requirements 6](#_Toc101084663)

[Specific Requirements 13](#_Toc101084664)

[5. Report Summary 38](#_Toc101084665)

1. Third Party Information

|  |  |  |
| --- | --- | --- |
| Company Name | Click here to enter text. | |
| Vendor ID | Click here to enter text. | |
| Business Address | **Country** | Click here to enter text. |
| **City** | Click here to enter text. |
| **Address** | Click here to enter text. |
| Third Party Classification | * General Requirements (Applicable on all third parties)   Outsourced Infrastructure  Customized Software  Network Connectivity  Critical Data Processor  Cloud Computing Service | |
| Contact Person | **Name** | Click here to enter text. |
| **Position** | Click here to enter text. |
| **Email** | Click here to enter text. |
| **Phone** | Click here to enter text. |
| **Mobile Number** | Click here to enter text. |

1. Audit Firm Information

\*This section to be filled by the Audit Firm

* 1. Report Control

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Author | Comment |
| 0.1 | MM/DD/YYYY | Assessor | Initial Draft |
| 1.0 | MM/DD/YYYY | Reviewer | Final |

* 1. Assessors

|  |  |
| --- | --- |
| Name | Date |
| Click here to enter text. | MM/DD/YYYY |
| Click here to enter text. | MM/DD/YYYY |

* 1. Approved by

|  |  |  |
| --- | --- | --- |
| Entity | Signature | Date |
| Name, Position |  | MM/DD/YYYY |
| Name, Position |  | MM/DD/YYYY |

1. Guidelines
   1. Ensure the answers are comprehensive, clearly described, and attach supporting documents.
   2. Ensure evidence:
   * Is clear, readable, and time stamped
   * Shows proof of its relation to the Third Party
   * Is clearly pointed out/highlighted in the screenshots

Executive Summary

The purpose of this cybersecurity assessment is to confirm that [Third Party] has implemented the general requirement information security controls defined in the Third Party Cybersecurity Standard (SACS-002), in addition to the relevant controls as per the Third Party classification. This assessment captures and documents a point-in-time implementation status of the existence of the applicable controls as per the Third Party Cybersecurity Standard (SACS-002).

The Cybersecurity Assessment Report identifies and highlights the areas of concern, which must be addressed by the Third Party, to acquire the Third Party Cybersecurity Compliance certificate that requires full compliance with the Third Party Cybersecurity Standard (SACS-002). The Information Security controls implementation status in [Third Party] is illustrated in the chart below.

1. Assessment Controls

General Requirements

| Control # | 1 | Compliance Status | Compliance  Noncompliance  [To be filled by audit firm assessors] |
| --- | --- | --- | --- |
| Reference # | TPC-1 | Source | SACS-002 Third Party Cybersecurity Standard |
| Control Statement | The Third Party must establish, maintain, and communicate a Cybersecurity Acceptable Use Policy (AUP) governing the use of Third Party Technology Assets. | | |
| Supporting Evidence | | | |
| [To be filled by audit firm assessors for on-site assessment or by Third Party representative for remote assessment] | | | |
| Compliance Analysis and Remarks | | | |
| [To be filled by audit firm assessors] | | | |

| Control # | 2 | Compliance Status | Compliance  Noncompliance  [To be filled by audit firm assessors] |
| --- | --- | --- | --- |
| Reference # | TPC-2 | Source | SACS-002 Third Party Cybersecurity Standard |
| Control Statement | Password protection measures must be enforced by the Third Party. The following are recommended measures:  - Minimum length: eight 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 five minutes of inactivity | | |
| Supporting Evidence | | | |
| [To be filled by audit firm assessors for on-site assessment or by the Third Party representative for remote assessment] | | | |
| Compliance Analysis and Remarks | | | |
| [To be filled by audit firm assessors] | | | |

| Control # | 3 | Compliance Status | Compliance  Noncompliance  [To be filled by audit firm assessors] |
| --- | --- | --- | --- |
| Reference # | TPC-3 | Source | SACS-002 Third Party Cybersecurity Standard |
| Control Statement | 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. This should be part of Third Party cybersecurity polices. | | |
| Supporting Evidence | | | |
| [To be filled by audit firm assessors for on-site assessment or by the Third Party representative for remote assessment] | | | |
| Compliance Analysis and Remarks | | | |
| [To be filled by audit firm assessors] | | | |

| Control # | 4 | Compliance Status | Compliance  Noncompliance  [To be filled by audit firm assessors] |
| --- | --- | --- | --- |
| Reference # | TPC-4 | Source | SACS-002 Third Party Cybersecurity Standard |
| Control Statement | Two-Factor authentication must be enforced on all remote access, including access from the Internet, to Third Party Company computing resources. | | |
| Supporting Evidence | | | |
| [To be filled by audit firm assessors for on-site assessment or by the Third Party representative for remote assessment] | | | |
| Compliance Analysis and Remarks | | | |
| [To be filled by audit firm assessors] | | | |

| Control # | 5 | Compliance Status | Compliance  Noncompliance  [To be filled by audit firm assessors] |
| --- | --- | --- | --- |
| Reference # | TPC-5 | Source | SACS-002 Third Party Cybersecurity Standard |
| Control Statement | Multi-factor authentication must be enforced on all access to Cloud services utilized by the Third Party, including access to cloud-based email. | | |
| Supporting Evidence | | | |
| [To be filled by audit firm assessors for on-site assessment or by the Third Party representative for remote assessment] | | | |
| Compliance Analysis and Remarks | | | |
| [To be filled by audit firm assessors] | | | |

| Control # | 6 | Compliance Status | Compliance  Noncompliance  [To be filled by audit firm assessors] |
| --- | --- | --- | --- |
| Reference # | TPC-6 | Source | SACS-002 Third Party Cybersecurity Standard |
| Control Statement | The Third Party must inform Saudi Aramco when employees provided with Saudi Aramco user credentials no longer need their access, or are transferred, reassigned, have retired, or resigned, or no longer associated with the Third Party. | | |
| Supporting Evidence | | | |
| [To be filled by audit firm assessors for on-site assessment or by the Third Party representative for remote assessment] | | | |
| Compliance Analysis and Remarks | | | |
| [To be filled by audit firm assessors] | | | |

| Control # | 7 | Compliance Status | Compliance  Noncompliance  [To be filled by audit firm assessors] |
| --- | --- | --- | --- |
| Reference # | TPC-7 | Source | SACS-002 Third Party Cybersecurity Standard |
| Control Statement | The Third Party must require all information systems users to take annual 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 | | |
| Supporting Evidence | | | |
| [To be filled by audit firm assessors for on-site assessment or by the Third Party representative for remote assessment] | | | |
| Compliance Analysis and Remarks | | | |
| [To be filled by audit firm assessors] | | | |

| Control # | 8 | Compliance Status | Compliance  Noncompliance  [To be filled by audit firm assessors] |
| --- | --- | --- | --- |
| Reference # | TPC-8 | Source | SACS-002 Third Party Cybersecurity Standard |
| Control Statement | The Third Party must inform personnel, in keeping with the Third Party Company Policy, that using personal email to share and transmit Saudi Aramco data is strictly prohibited. | | |
| Supporting Evidence | | | |
| [To be filled by audit firm assessors for on-site assessment or by the Third Party representative for remote assessment] | | | |
| Compliance Analysis and Remarks | | | |
| [To be filled by audit firm assessors] | | | |

| Control # | 9 | Compliance Status | Compliance  Noncompliance  [To be filled by audit firm assessors] |
| --- | --- | --- | --- |
| Reference # | TPC-9 | Source | SACS-002 Third Party Cybersecurity Standard |
| Control Statement | The Third Party must inform personnel, in keeping with the 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. | | |
| Supporting Evidence | | | |
| [To be filled by audit firm assessors for on-site assessment or by the Third Party representative for remote assessment] | | | |
| Compliance Analysis and Remarks | | | |
| [To be filled by audit firm assessors] | | | |

| Control # | 10 | Compliance Status | Compliance  Noncompliance  [To be filled by audit firm assessors] |
| --- | --- | --- | --- |
| Reference # | TPC-10 | Source | SACS-002 Third Party Cybersecurity Standard |
| Control Statement | All Third Party Technology Assets and Systems must be password protected. | | |
| Supporting Evidence | | | |
| [To be filled by audit firm assessors for on-site assessment or by the Third Party representative for remote assessment] | | | |
| Compliance Analysis and Remarks | | | |
| [To be filled by audit firm assessors] | | | |

| Control # | 11 | Compliance Status | Compliance  Noncompliance  [To be filled by audit firm assessors] |
| --- | --- | --- | --- |
| Reference # | TPC-11 | Source | SACS-002 Third Party Cybersecurity Standard |
| Control Statement | Third Party Technology Assets and Systems must be regularly updated with operating system (OS), software and applets patches (i.e. Adobe, Flash, Java etc.). | | |
| Supporting Evidence | | | |
| [To be filled by audit firm assessors for onsite assessment or by the Third Party representative for remote assessment] | | | |
| Compliance Analysis and Remarks | | | |
| [To be filled by audit firm assessors] | | | |

| Control # | 12 | Compliance Status | Compliance  Noncompliance  [To be filled by audit firm assessors] |
| --- | --- | --- | --- |
| Reference # | TPC-12 | Source | SACS-002 Third Party Cybersecurity Standard |
| Control Statement | 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. | | |
| Supporting Evidence | | | |
| [To be filled by audit firm assessors for on-site assessment or by the Third Party representative for remote assessment] | | | |
| Compliance Analysis and Remarks | | | |
| [To be filled by audit firm assessors] | | | |

| Control # | 13 | Compliance Status | Compliance  Noncompliance  [To be filled by audit firm assessors] |
| --- | --- | --- | --- |
| Reference # | TPC-13 | Source | SACS-002 Third Party Cybersecurity Standard |
| Control Statement | The Third Party must implement Sender Policy Framework (SPF) technology on the mail server. | | |
| Supporting Evidence | | | |
| [To be filled by audit firm assessors for on-site assessment or by the Third Party representative for remote assessment] | | | |
| Compliance Analysis and Remarks | | | |
| [To be filled by audit firm assessors] | | | |

| Control # | 14 | Compliance Status | Compliance  Noncompliance  [To be filled by audit firm assessors] |
| --- | --- | --- | --- |
| Reference # | TPC-14 | Source | SACS-002 Third Party Cybersecurity Standard |
| Control Statement | The Third Party must enforce Sender Policy Framework (SPF) feature on Saudi Aramco email domains: Aramco.com and Aramco.com.sa. | | |
| Supporting Evidence | | | |
| [To be filled by audit firm assessors for on-site assessment or by the Third Party representative for remote assessment] | | | |
| Compliance Analysis and Remarks | | | |
| [To be filled by audit firm assessors] | | | |

| Control # | 15 | Compliance Status | Compliance  Noncompliance  [To be filled by audit firm assessors] |
| --- | --- | --- | --- |
| Reference # | TPC-15 | Source | SACS-002 Third Party Cybersecurity Standard |
| Control Statement | The Third Party must publish the SPF record in the DNS server. | | |
| Supporting Evidence | | | |
| [To be filled by audit firm assessors for onsite assessment or by the Third Party representative for remote assessment] | | | |
| Compliance Analysis and Remarks | | | |
| [To be filled by audit firm assessors] | | | |

| Control # | 16 | Compliance Status | Compliance  Noncompliance  [To be filled by audit firm assessors] |
| --- | --- | --- | --- |
| Reference # | TPC-16 | Source | SACS-002 Third Party Cybersecurity Standard |
| Control Statement | The Third Party must inspect all incoming emails originating from the Internet using anti-spam protection. | | |
| Supporting Evidence | | | |
| [To be filled by audit firm assessors for on-site assessment or by the Third Party representative for remote assessment] | | | |
| Compliance Analysis and Remarks | | | |
| [To be filled by audit firm assessors] | | | |

| Control # | 17 | Compliance Status | Compliance  Noncompliance  [To be filled by audit firm assessors] |
| --- | --- | --- | --- |
| Reference # | TPC-17 | Source | SACS-002 Third Party Cybersecurity Standard |
| Control Statement | The Third Party must use a private email domain. Generic domains, such as Gmail and Hotmail, must not be used. | | |
| Supporting Evidence | | | |
| [To be filled by audit firm assessors for on-site assessment or by the Third Party representative for remote assessment] | | | |
| Compliance Analysis and Remarks | | | |
| [To be filled by audit firm assessors] | | | |

| Control # | 18 | Compliance Status | Compliance  Noncompliance  [To be filled by audit firm assessors] |
| --- | --- | --- | --- |
| Reference # | TPC-18 | Source | SACS-002 Third Party Cybersecurity Standard |
| Control Statement | 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. | | |
| Supporting Evidence | | | |
| [To be filled by audit firm assessors for on-site assessment or by the Third Party representative for remote assessment] | | | |
| Compliance Analysis and Remarks | | | |
| [To be filled by audit firm assessors] | | | |

| Control # | 19 | Compliance Status | Compliance  Noncompliance  [To be filled by audit firm assessors] |
| --- | --- | --- | --- |
| Reference # | TPC-19 | Source | SACS-002 Third Party Cybersecurity Standard |
| Control Statement | 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). The sanitization must be conducted in alignment to industry best practices such as NIST 800-88. The Third party shall certify in a signed letter to Saudi Aramco that the data sanitization has been successfully completed. | | |
| Supporting Evidence | | | |
| [To be filled by audit firm assessors for onsite assessment or by the Third Party representative for remote assessment] | | | |
| Compliance Analysis and Remarks | | | |
| [To be filled by audit firm assessors] | | | |

| Control # | 20 | Compliance Status | Compliance  Noncompliance  [To be filled by audit firm assessors] |
| --- | --- | --- | --- |
| Reference # | TPC-20 | Source | SACS-002 Third Party Cybersecurity Standard |
| Control Statement | The 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. | | |
| Supporting Evidence | | | |
| [To be filled by audit firm assessors for on-site assessment or by the Third Party representative for remote assessment] | | | |
| Compliance Analysis and Remarks | | | |
| [To be filled by audit firm assessors] | | | |

| Control # | 21 | Compliance Status | Compliance  Noncompliance  [To be filled by audit firm assessors] |
| --- | --- | --- | --- |
| Reference # | TPC-21 | Source | SACS-002 Third Party Cybersecurity Standard |
| Control Statement | The Third Party must renew the CCC every two years. | | |
| Supporting Evidence | | | |
| [To be filled by audit firm assessors for on-site assessment or by Third Party representative for remote assessment] | | | |
| Compliance Analysis and Remarks | | | |
| [To be filled by audit firm assessors] | | | |

| Control # | 22 | Compliance Status | Compliance  Noncompliance  [To be filled by audit firm assessors] |
| --- | --- | --- | --- |
| Reference # | TPC-22 | Source | SACS-002 Third Party Cybersecurity Standard |
| Control Statement | Firewalls must be configured and enabled on endpoint devices. | | |
| Supporting Evidence | | | |
| [To be filled by audit firm assessors for on-site assessment or by the Third Party representative for remote assessment] | | | |
| Compliance Analysis and Remarks | | | |
| [To be filled by audit firm assessors] | | | |

| Control # | 23 | Compliance Status | Compliance  Noncompliance  [To be filled by audit firm assessors] |
| --- | --- | --- | --- |
| Reference # | TPC-23 | Source | SACS-002 Third Party Cybersecurity Standard |
| Control Statement | If the Third Party discovers a cybersecurity incident, the Third Party must (besides its continuous efforts to resolve and mitigate the Incident):  - Notify SAUDI ARAMCO within 24 hours of discovering the incident  - Follow the Cybersecurity Incident Response Instructions set forth in Appendix A. | | |
| Supporting Evidence | | | |
| [To be filled by audit firm assessors for onsite assessment or by the Third Party representative for remote assessment] | | | |
| Compliance Analysis and Remarks | | | |
| [To be filled by audit firm assessors] | | | |

Specific Requirements

| Control # | 24 | Compliance Status | Compliance  Noncompliance  [To be filled by audit firm assessors] | |
| --- | --- | --- | --- | --- |
| Reference # | TPC-24 | Source | SACS-002 Third Party Cybersecurity Standard | |
| Classification | * Outsourced Infrastructure * Customized Software | | | * Network Connectivity * Critical Data Processor * Cloud Computing Service |
| Control Statement | Third Party must have policies and processes to classify information in terms of its value, criticality and confidentiality. | | | |
| Supporting Evidence | | | | |
| [To be filled by audit firm assessors for on-site assessment or by the Third Party representative for remote assessment] | | | | |
| Compliance Analysis and Remarks | | | | |
| [To be filled by audit firm assessors] | | | | |

| Control # | 25 | Compliance Status | Compliance  Noncompliance  [To be filled by audit firm assessors] | |
| --- | --- | --- | --- | --- |
| Reference # | TPC-25 | Source | SACS-002 Third Party Cybersecurity Standard | |
| Classification | * Outsourced Infrastructure * Customized Software | | | * Network Connectivity * Critical Data Processor * Cloud Computing Service |
| Control Statement | The Third Party must establish, maintain and communicate cybersecurity policies and standards. | | | |
| Supporting Evidence | | | | |
| [To be filled by audit firm assessors for on-site assessment or by the Third Party representative for remote assessment] | | | | |
| Compliance Analysis and Remarks | | | | |
| [To be filled by audit firm assessors] | | | | |

| Control # | 26 | Compliance Status | Compliance  Noncompliance  [To be filled by audit firm assessors] | |
| --- | --- | --- | --- | --- |
| Reference # | TPC-26 | Source | SACS-002 Third Party Cybersecurity Standard | |
| Classification | * Outsourced Infrastructure * Customized Software | | | * Network Connectivity * Critical Data Processor * Cloud Computing Service |
| Control Statement | Third Party must be staffed by employee(s) whose primary responsibility is cybersecurity. Responsibilities of those personnel must include maintaining the security of information systems, and ensuring compliance with existing policies. | | | |
| Supporting Evidence | | | | |
| [To be filled by audit firm assessors for onsite assessment or by the Third Party representative for remote assessment] | | | | |
| Compliance Analysis and Remarks | | | | |
| [To be filled by audit firm assessors] | | | | |

| Control # | 27 | Compliance Status | Compliance  Noncompliance  [To be filled by audit firm assessors] | |
| --- | --- | --- | --- | --- |
| Reference # | TPC-27 | Source | SACS-002 Third Party Cybersecurity Standard | |
| Classification | * Outsourced Infrastructure * Customized Software | | | * Network Connectivity * Critical Data Processor * Cloud Computing Service |
| Control Statement | The Third Party must conduct annual external Penetration Testing on its IT infrastructure systems and Internet facing applications. | | | |
| Supporting Evidence | | | | |
| [To be filled by audit firm assessors for on-site assessment or by the Third Party representative for remote assessment] | | | | |
| Compliance Analysis and Remarks | | | | |
| [To be filled by audit firm assessors] | | | | |

| Control # | 28 | Compliance Status | Compliance  Noncompliance  [To be filled by audit firm assessors] | |
| --- | --- | --- | --- | --- |
| Reference # | TPC-28 | Source | SACS-002 Third Party Cybersecurity Standard | |
| Classification | * Outsourced Infrastructure * Customized Software | | | * Network Connectivity * Critical Data Processor * Cloud Computing Service |
| Control Statement | Third Party must conduct annual external Penetration Testing on Cloud Computing Service(s) used by Saudi Aramco | | | |
| Supporting Evidence | | | | |
| [To be filled by audit firm assessors for on-site assessment or by the Third Party representative for remote assessment] | | | | |
| Compliance Analysis and Remarks | | | | |
| [To be filled by audit firm assessors] | | | | |

| Control # | 29 | Compliance Status | Compliance  Noncompliance  [To be filled by audit firm assessors] | |
| --- | --- | --- | --- | --- |
| Reference # | TPC-29 | Source | SACS-002 Third Party Cybersecurity Standard | |
| Classification | * Outsourced Infrastructure * Customized Software | | | * Network Connectivity * Critical Data Processor * Cloud Computing Service |
| Control Statement | If Third Party is hosting a website for Saudi Aramco, annual Penetration Testing must be conducted to test website security. | | | |
| Supporting Evidence | | | | |
| [To be filled by audit firm assessors for on-site assessment or by the Third Party representative for remote assessment] | | | | |
| Compliance Analysis and Remarks | | | | |
| [To be filled by audit firm assessors] | | | | |

| Control # | 30 | Compliance Status | Compliance  Noncompliance  [To be filled by audit firm assessors] | |
| --- | --- | --- | --- | --- |
| Reference # | TPC-30 | Source | SACS-002 Third Party Cybersecurity Standard | |
| Classification | * Outsourced Infrastructure * Customized Software | | | * Network Connectivity * Critical Data Processor * Cloud Computing Service |
| Control Statement | Third party data center must be certified by industry recognized authority | | | |
| Supporting Evidence | | | | |
| [To be filled by audit firm assessors for on-site assessment or by the Third Party representative for remote assessment] | | | | |
| Compliance Analysis and Remarks | | | | |
| [To be filled by audit firm assessors] | | | | |

| Control # | 31 | Compliance Status | Compliance  Noncompliance  [To be filled by audit firm assessors] | |
| --- | --- | --- | --- | --- |
| Reference # | TPC-31 | Source | SACS-002 Third Party Cybersecurity Standard | |
| Classification | * Outsourced Infrastructure * Customized Software | | | * Network Connectivity * Critical Data Processor * Cloud Computing Service |
| Control Statement | The Third Party must have a process to conduct a Cybersecurity Risk Assessment on a regular basis, to identify, assess, and remediate risks to data and information systems. | | | |
| Supporting Evidence | | | | |
| [To be filled by audit firm assessors for on-site assessment or by the Third Party representative for remote assessment] | | | | |
| Compliance Analysis and Remarks | | | | |
| [To be filled by audit firm assessors] | | | | |

| Control # | 32 | Compliance Status | Compliance  Noncompliance  [To be filled by audit firm assessors] | |
| --- | --- | --- | --- | --- |
| Reference # | TPC-32 | Source | SACS-002 Third Party Cybersecurity Standard | |
| Classification | * Outsourced Infrastructure * Customized Software | | | * Network Connectivity * Critical Data Processor * Cloud Computing Service |
| Control Statement | Users accessing applications and information systems must be issued unique user logins and passwords. Generic accounts must not be allowed. | | | |
| Supporting Evidence | | | | |
| [To be filled by audit firm assessors for onsite assessment or by the Third Party representative for remote assessment] | | | | |
| Compliance Analysis and Remarks | | | | |
| [To be filled by audit firm assessors] | | | | |

| Control # | 33 | Compliance Status | Compliance  Noncompliance  [To be filled by audit firm assessors] | |
| --- | --- | --- | --- | --- |
| Reference # | TPC-33 | Source | SACS-002 Third Party Cybersecurity Standard | |
| Classification | * Outsourced Infrastructure * Customized Software | | | * Network Connectivity * Critical Data Processor * Cloud Computing Service |
| Control Statement | 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. | | | |
| Supporting Evidence | | | | |
| [To be filled by audit firm assessors for on-site assessment or by the Third Party representative for remote assessment] | | | | |
| Compliance Analysis and Remarks | | | | |
| [To be filled by audit firm assessors] | | | | |

| Control # | 34 | Compliance Status | Compliance  Noncompliance  [To be filled by audit firm assessors] | |
| --- | --- | --- | --- | --- |
| Reference # | TPC-34 | Source | SACS-002 Third Party Cybersecurity Standard | |
| Classification | * Outsourced Infrastructure * Customized Software | | | * Network Connectivity * Critical Data Processor * Cloud Computing Service |
| Control Statement | All privileged accounts must be limited, justified, and reviewed on regular basis. | | | |
| Supporting Evidence | | | | |
| [To be filled by audit firm assessors for on-site assessment or by the Third Party representative for remote assessment] | | | | |
| Compliance Analysis and Remarks | | | | |
| [To be filled by audit firm assessors] | | | | |

| Control # | 35 | Compliance Status | Compliance  Noncompliance  [To be filled by audit firm assessors] | |
| --- | --- | --- | --- | --- |
| Reference # | TPC-35 | Source | SACS-002 Third Party Cybersecurity Standard | |
| Classification | * Outsourced Infrastructure * Customized Software | | | * Network Connectivity * Critical Data Processor * Cloud Computing Service |
| Control Statement | Remote administrative access from the Internet must not be allowed, unless explicitly approved, restricted, and controlled. | | | |
| Supporting Evidence | | | | |
| [To be filled by audit firm assessors for on-site assessment or by the Third Party representative for remote assessment] | | | | |
| Compliance Analysis and Remarks | | | | |
| [To be filled by audit firm assessors] | | | | |

| Control # | 36 | Compliance Status | Compliance  Noncompliance  [To be filled by audit firm assessors] | |
| --- | --- | --- | --- | --- |
| Reference # | TPC-36 | Source | SACS-002 Third Party Cybersecurity Standard | |
| Classification | * Outsourced Infrastructure * Customized Software | | | * Network Connectivity * Critical Data Processor * Cloud Computing Service |
| Control Statement | Network connections to information systems and applications at the Third Parties location must be authorized and monitored. | | | |
| Supporting Evidence | | | | |
| [To be filled by audit firm assessors for on-site assessment or by the Third Party representative for remote assessment] | | | | |
| Compliance Analysis and Remarks | | | | |
| [To be filled by audit firm assessors] | | | | |

| Control # | 37 | Compliance Status | Compliance  Noncompliance  [To be filled by audit firm assessors] | |
| --- | --- | --- | --- | --- |
| Reference # | TPC-37 | Source | SACS-002 Third Party Cybersecurity Standard | |
| Classification | * Outsourced Infrastructure * Customized Software | | | * Network Connectivity * Critical Data Processor * Cloud Computing Service |
| Control Statement | Multi-factor authentication must be enforced on all privileged accounts access, including remote access to information systems and applications. | | | |
| Supporting Evidence | | | | |
| [To be filled by audit firm assessors for on-site assessment, or by the Third Party representative for remote assessment] | | | | |
| Compliance Analysis and Remarks | | | | |
| [To be filled by audit firm assessors] | | | | |

| Control # | 38 | Compliance Status | Compliance  Noncompliance  [To be filled by audit firm assessors] | |
| --- | --- | --- | --- | --- |
| Reference # | TPC-38 | Source | SACS-002 Third Party Cybersecurity Standard | |
| Classification | * Outsourced Infrastructure * Customized Software | | | * Network Connectivity * Critical Data Processor * Cloud Computing Service |
| Control Statement | 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. | | | |
| Supporting Evidence | | | | |
| [To be filled by audit firm assessors for on-site assessment or by the Third Party representative for remote assessment] | | | | |
| Compliance Analysis and Remarks | | | | |
| [To be filled by audit firm assessors] | | | | |

| Control # | 39 | Compliance Status | Compliance  Noncompliance  [To be filled by audit firm assessors] | |
| --- | --- | --- | --- | --- |
| Reference # | TPC-39 | Source | SACS-002 Third Party Cybersecurity Standard | |
| Classification | * Outsourced Infrastructure * Customized Software | | | * Network Connectivity * Critical Data Processor * Cloud Computing Service |
| Control Statement | Saudi Aramco Critical Data documents must only be shared with limited individuals who are part of the work specified in the contract. | | | |
| Supporting Evidence | | | | |
| [To be filled by audit firm assessors for on-site assessment or by the Third Party representative for remote assessment] | | | | |
| Compliance Analysis and Remarks | | | | |
| [To be filled by audit firm assessors] | | | | |

| Control # | 40 | Compliance Status | Compliance  Noncompliance  [To be filled by audit firm assessors] | |
| --- | --- | --- | --- | --- |
| Reference # | TPC-40 | Source | SACS-002 Third Party Cybersecurity Standard | |
| Classification | * Outsourced Infrastructure * Customized Software | | | * Network Connectivity * Critical Data Processor * Cloud Computing Service |
| Control Statement | Servers and workstations subnets must be segmented and access between them is restricted and monitored. | | | |
| Supporting Evidence | | | | |
| [To be filled by audit firm assessors for on-site assessment or by the Third Party representative for remote assessment] | | | | |
| Compliance Analysis and Remarks | | | | |
| [To be filled by audit firm assessors] | | | | |

| Control # | 41 | Compliance Status | Compliance  Noncompliance  [To be filled by audit firm assessors] | |
| --- | --- | --- | --- | --- |
| Reference # | TPC-41 | Source | SACS-002 Third Party Cybersecurity Standard | |
| Classification | * Outsourced Infrastructure * Customized Software | | | * Network Connectivity * Critical Data Processor * Cloud Computing Service |
| Control Statement | Servers accessible from the Internet must be placed in a DMZ (i.e., perimeter network) with restricted access to internal subnets. | | | |
| Supporting Evidence | | | | |
| [To be filled by audit firm assessors for on-site assessment or by the Third Party representative for remote assessment] | | | | |
| Compliance Analysis and Remarks | | | | |
| [To be filled by audit firm assessors] | | | | |

| Control # | 42 | Compliance Status | Compliance  Noncompliance  [To be filled by audit firm assessors] | |
| --- | --- | --- | --- | --- |
| Reference # | TPC-42 | Source | SACS-002 Third Party Cybersecurity Standard | |
| Classification | * Outsourced Infrastructure * Customized Software | | | * Network Connectivity * Critical Data Processor * Cloud Computing Service |
| Control Statement | Wireless networks accessing information systems must use strong encryption for authentication and transmission, such as WPA2 or WPA2 Enterprise. | | | |
| Supporting Evidence | | | | |
| [To be filled by audit firm assessors for on-site assessment or by the Third Party representative for remote assessment] | | | | |
| Compliance Analysis and Remarks | | | | |
| [To be filled by audit firm assessors] | | | | |

| Control # | 43 | Compliance Status | Compliance  Noncompliance  [To be filled by audit firm assessors] | |
| --- | --- | --- | --- | --- |
| Reference # | TPC-43 | Source | SACS-002 Third Party Cybersecurity Standard | |
| Classification | * Outsourced Infrastructure * Customized Software | | | * Network Connectivity * Critical Data Processor * Cloud Computing Service |
| Control Statement | Third Party data center must have the required tier rating and high-availability of service fail-over as determined by Saudi Aramco | | | |
| Supporting Evidence | | | | |
| [To be filled by audit firm assessors for on-site assessment or by the Third Party representative for remote assessment] | | | | |
| Compliance Analysis and Remarks | | | | |
| [To be filled by audit firm assessors] | | | | |

| Control # | 44 | Compliance Status | Compliance  Noncompliance  [To be filled by audit firm assessors] | |
| --- | --- | --- | --- | --- |
| Reference # | TPC-44 | Source | SACS-002 Third Party Cybersecurity Standard | |
| Classification | * Outsourced Infrastructure * Customized Software | | | * Network Connectivity * Critical Data Processor * Cloud Computing Service |
| Control Statement | 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. | | | |
| Supporting Evidence | | | | |
| [To be filled by audit firm assessors for on-site assessment or by the Third Party representative for remote assessment] | | | | |
| Compliance Analysis and Remarks | | | | |
| [To be filled by audit firm assessors] | | | | |

| Control # | 45 | Compliance Status | Compliance  Noncompliance  [To be filled by audit firm assessors] | |
| --- | --- | --- | --- | --- |
| Reference # | TPC-45 | Source | SACS-002 Third Party Cybersecurity Standard | |
| Classification | * Outsourced Infrastructure * Customized Software | | | * Network Connectivity * Critical Data Processor * Cloud Computing Service |
| Control Statement | Multi-Factor authentication must be enforced on end-users accessing Content Management Services (CMS) of Cloud Computing Service. | | | |
| Supporting Evidence | | | | |
| [To be filled by audit firm assessors for on-site assessment or by the Third Party representative for remote assessment] | | | | |
| Compliance Analysis and Remarks | | | | |
| [To be filled by audit firm assessors] | | | | |

| Control # | 46 | Compliance Status | Compliance  Noncompliance  [To be filled by audit firm assessors] | |
| --- | --- | --- | --- | --- |
| Reference # | TPC-46 | Source | SACS-002 Third Party Cybersecurity Standard | |
| Classification | * Outsourced Infrastructure * Customized Software | | | * Network Connectivity * Critical Data Processor * Cloud Computing Service |
| Control Statement | 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. | | | |
| Supporting Evidence | | | | |
| [To be filled by audit firm assessors for on-site assessment or by Third Party representative for remote assessment] | | | | |
| Compliance Analysis and Remarks | | | | |
| [To be filled by audit firm assessors] | | | | |

| Control # | 47 | Compliance Status | Compliance  Noncompliance  [To be filled by audit firm assessors] | |
| --- | --- | --- | --- | --- |
| Reference # | TPC-47 | Source | SACS-002 Third Party Cybersecurity Standard | |
| Classification | * Outsourced Infrastructure * Customized Software | | | * Network Connectivity * Critical Data Processor * Cloud Computing Service |
| Control Statement | 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 | | | |
| Supporting Evidence | | | | |
| [To be filled by audit firm assessors for on-site assessment or by Third Party representative for remote assessment] | | | | |
| Compliance Analysis and Remarks | | | | |
| [To be filled by audit firm assessors] | | | | |

| Control # | 48 | Compliance Status | Compliance  Noncompliance  [To be filled by audit firm assessors] | |
| --- | --- | --- | --- | --- |
| Reference # | TPC-48 | Source | SACS-002 Third Party Cybersecurity Standard | |
| Classification | * Outsourced Infrastructure * Customized Software | | | * Network Connectivity * Critical Data Processor * Cloud Computing Service |
| Control Statement | Visitors accessing Critical Facilities must be escorted at all times. | | | |
| Supporting Evidence | | | | |
| [To be filled by audit firm assessors for on-site assessment or by Third Party representative for remote assessment] | | | | |
| Compliance Analysis and Remarks | | | | |
| [To be filled by audit firm assessors] | | | | |

| Control # | 49 | Compliance Status | Compliance  Noncompliance  [To be filled by audit firm assessors] | |
| --- | --- | --- | --- | --- |
| Reference # | TPC-49 | Source | SACS-002 Third Party Cybersecurity Standard | |
| Classification | * Outsourced Infrastructure * Customized Software | | | * Network Connectivity * Critical Data Processor * Cloud Computing Service |
| Control Statement | Third Party must dedicate an access restricted working area for personnel with access to the Saudi Aramco network. | | | |
| Supporting Evidence | | | | |
| [To be filled by audit firm assessors for on-site assessment or by the Third Party representative for remote assessment] | | | | |
| Compliance Analysis and Remarks | | | | |
| [To be filled by audit firm assessors] | | | | |

| Control # | 50 | Compliance Status | Compliance  Noncompliance  [To be filled by audit firm assessors] | |
| --- | --- | --- | --- | --- |
| Reference # | TPC-50 | Source | SACS-002 Third Party Cybersecurity Standard | |
| Classification | * Outsourced Infrastructure * Customized Software | | | * Network Connectivity * Critical Data Processor * Cloud Computing Service |
| Control Statement | Backup media must be secured to block/inhibit unauthorized physical access. | | | |
| Supporting Evidence | | | | |
| [To be filled by audit firm assessors for on-site assessment or by the Third Party representative for remote assessment] | | | | |
| Compliance Analysis and Remarks | | | | |
| [To be filled by audit firm assessors] | | | | |

| Control # | 51 | Compliance Status | Compliance  Noncompliance  [To be filled by audit firm assessors] | |
| --- | --- | --- | --- | --- |
| Reference # | TPC-51 | Source | SACS-002 Third Party Cybersecurity Standard | |
| Classification | * Outsourced Infrastructure * Customized Software | | | * Network Connectivity * Critical Data Processor * Cloud Computing Service |
| Control Statement | Technology assets and systems connected to the Internet must be licensed and supported by the provider. | | | |
| Supporting Evidence | | | | |
| [To be filled by audit firm assessors for on-site assessment or by the Third Party representative for remote assessment] | | | | |
| Compliance Analysis and Remarks | | | | |
| [To be filled by audit firm assessors] | | | | |

| Control # | 52 | Compliance Status | Compliance  Noncompliance  [To be filled by audit firm assessors] | |
| --- | --- | --- | --- | --- |
| Reference # | TPC-52 | Source | SACS-002 Third Party Cybersecurity Standard | |
| Classification | * Outsourced Infrastructure * Customized Software | | | Network Connectivity   * Critical Data Processor * Cloud Computing Service |
| Control Statement | Third Party must encrypt data in transit (e.g., SSH, FTPS, HTTPS, TLS, IPSEC). | | | |
| Supporting Evidence | | | | |
| [To be filled by audit firm assessors for on-site assessment or by the Third Party representative for remote assessment] | | | | |
| Compliance Analysis and Remarks | | | | |
| [To be filled by audit firm assessors] | | | | |

| Control # | 53 | Compliance Status | Compliance  Noncompliance  [To be filled by audit firm assessors] | |
| --- | --- | --- | --- | --- |
| Reference # | TPC-53 | Source | SACS-002 Third Party Cybersecurity Standard | |
| Classification | * Outsourced Infrastructure * Customized Software | | | * Network Connectivity * Critical Data Processor * Cloud Computing Service |
| Control Statement | 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. | | | |
| Supporting Evidence | | | | |
| [To be filled by audit firm assessors for on-site assessment or by the Third Party representative for remote assessment] | | | | |
| Compliance Analysis and Remarks | | | | |
| [To be filled by audit firm assessors] | | | | |

| Control # | 54 | Compliance Status | Compliance  NonCompliance  [To be filled by audit firm assessors] | |
| --- | --- | --- | --- | --- |
| Reference # | TPC-54 | Source | SACS-002 Third Party Cybersecurity Standard | |
| Classification | * Outsourced Infrastructure * Customized Software | | | * Network Connectivity * Critical Data Processor * Cloud Computing Service |
| Control Statement | 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. | | | |
| Supporting Evidence | | | | |
| [To be filled by audit firm assessors for on-site assessment or by the Third Party representative for remote assessment] | | | | |
| Compliance Analysis and Remarks | | | | |
| [To be filled by audit firm assessors] | | | | |

| Control # | 55 | Compliance Status | Compliance  NonCompliance  [To be filled by audit firm assessors] | |
| --- | --- | --- | --- | --- |
| Reference # | TPC-55 | Source | SACS-002 Third Party Cybersecurity Standard | |
| Classification | * Outsourced Infrastructure * Customized Software | | | * Network Connectivity * Critical Data Processor * Cloud Computing Service |
| Control Statement | Encryption key management capability, including preservation and retrieval, must be defined, applied, and periodically reviewed. | | | |
| Supporting Evidence | | | | |
| [To be filled by audit firm assessors for on-site assessment or by the Third Party representative for remote assessment] | | | | |
| Compliance Analysis and Remarks | | | | |
| [To be filled by audit firm assessors] | | | | |

| Control # | 56 | Compliance Status | Compliance  Noncompliance  [To be filled by audit firm assessors] | |
| --- | --- | --- | --- | --- |
| Reference # | TPC-56 | Source | SACS-002 Third Party Cybersecurity Standard | |
| Classification | * Outsourced Infrastructure * Customized Software | | | * Network Connectivity * Critical Data Processor * Cloud Computing Service |
| Control Statement | 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. | | | |
| Supporting Evidence | | | | |
| [To be filled by audit firm assessors for on-site assessment or by the Third Party representative for remote assessment] | | | | |
| Compliance Analysis and Remarks | | | | |
| [To be filled by audit firm assessors] | | | | |

| Control # | 57 | Compliance Status | Compliance  Noncompliance  [To be filled by audit firm assessors] | |
| --- | --- | --- | --- | --- |
| Reference # | TPC-57 | Source | SACS-002 Third Party Cybersecurity Standard | |
| Classification | * Outsourced Infrastructure   Customized Software | | | * Network Connectivity * Critical Data Processor * Cloud Computing Service |
| Control Statement | 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. | | | |
| Supporting Evidence | | | | |
| [To be filled by audit firm assessors for on-site assessment or by the Third Party representative for remote assessment] | | | | |
| Compliance Analysis and Remarks | | | | |
| [To be filled by audit firm assessors] | | | | |

| Control # | 58 | Compliance Status | Compliance  Noncompliance  [To be filled by audit firm assessors] | |
| --- | --- | --- | --- | --- |
| Reference # | TPC-58 | Source | SACS-002 Third Party Cybersecurity Standard | |
| Classification | * Outsourced Infrastructure * Customized Software | | | * Network Connectivity * Critical Data Processor * Cloud Computing Service |
| Control Statement | Documents containing Saudi Aramco Critical Data, must be encrypted and stored securely with access limited to authorized personnel. | | | |
| Supporting Evidence | | | | |
| [To be filled by audit firm assessors for on-site assessment or by the Third Party representative for remote assessment] | | | | |
| Compliance Analysis and Remarks | | | | |
| [To be filled by audit firm assessors] | | | | |

| Control # | 59 | Compliance Status | Compliance  Noncompliance  [To be filled by audit firm assessors] | |
| --- | --- | --- | --- | --- |
| Reference # | TPC-59 | Source | SACS-002 Third Party Cybersecurity Standard | |
| Classification | * Outsourced Infrastructure * Customized Software | | | * Network Connectivity * Critical Data Processor * Cloud Computing Service |
| Control Statement | Remote wipe solution must be installed on all tablets and mobile phones used to receive, store and/or produce critical data for Saudi Aramco. | | | |
| Supporting Evidence | | | | |
| [To be filled by audit firm assessors for on-site assessment or by the Third Party representative for remote assessment] | | | | |
| Compliance Analysis and Remarks | | | | |
| [To be filled by audit firm assessors] | | | | |

| Control # | 60 | Compliance Status | Compliance  Noncompliance  [To be filled by audit firm assessors] | |
| --- | --- | --- | --- | --- |
| Reference # | TPC-60 | Source | SACS-002 Third Party Cybersecurity Standard | |
| Classification | * Outsourced Infrastructure * Customized Software | | | * Network Connectivity * Critical Data Processor * Cloud Computing Service |
| Control Statement | 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. | | | |
| Supporting Evidence | | | | |
| [To be filled by audit firm assessors for on-site assessment or by the Third Party representative for remote assessment] | | | | |
| Compliance Analysis and Remarks | | | | |
| [To be filled by audit firm assessors] | | | | |

| Control # | 61 | Compliance Status | Compliance  Noncompliance  [To be filled by audit firm assessors] | |
| --- | --- | --- | --- | --- |
| Reference # | TPC-61 | Source | SACS-002 Third Party Cybersecurity Standard | |
| Classification | * Outsourced Infrastructure * Customized Software | | | * Network Connectivity * Critical Data Processor * Cloud Computing Service |
| Control Statement | Application error messages must not display any sensitive technical information. | | | |
| Supporting Evidence | | | | |
| [To be filled by audit firm assessors for on-site assessment or by the Third Party representative for remote assessment] | | | | |
| Compliance Analysis and Remarks | | | | |
| [To be filled by audit firm assessors] | | | | |

| Control # | 62 | Compliance Status | Compliance  Noncompliance  [To be filled by audit firm assessors] | |
| --- | --- | --- | --- | --- |
| Reference # | TPC-55 | Source | SACS-002 Third Party Cybersecurity Standard | |
| Classification | * Outsourced Infrastructure * Customized Software | | | * Network Connectivity * Critical Data Processor * Cloud Computing Service |
| Control Statement | Application or Cloud Computing Services must not store, generate, transmit, or use plain-text passwords. | | | |
| Supporting Evidence | | | | |
| [To be filled by audit firm assessors for on-site assessment or by the Third Party representative for remote assessment] | | | | |
| Compliance Analysis and Remarks | | | | |
| [To be filled by audit firm assessors] | | | | |

| Control # | 63 | Compliance Status | Compliance  Noncompliance  [To be filled by audit firm assessors] | |
| --- | --- | --- | --- | --- |
| Reference # | TPC-63 | Source | SACS-002 Third Party Cybersecurity Standard | |
| Classification | * Outsourced Infrastructure * Customized Software | | | * Network Connectivity * Critical Data Processor * Cloud Computing Service |
| Control Statement | 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 | | | |
| Supporting Evidence | | | | |
| [To be filled by audit firm assessors for on-site assessment or by the Third Party representative for remote assessment] | | | | |
| Compliance Analysis and Remarks | | | | |
| [To be filled by audit firm assessors] | | | | |

| Control # | 64 | Compliance Status | Compliance  Noncompliance  [To be filled by audit firm assessors] | |
| --- | --- | --- | --- | --- |
| Reference # | TPC-64 | Source | SACS-002 Third Party Cybersecurity Standard | |
| Classification | * Outsourced Infrastructure * Customized Software | | | * Network Connectivity * Critical Data Processor * Cloud Computing Service |
| Control Statement | Third Party must establish and follow regular procedures for backup of critical systems and Saudi Aramco’s data, software, and websites. | | | |
| Supporting Evidence | | | | |
| [To be filled by audit firm assessors for on-site assessment or by the Third Party representative for remote assessment] | | | | |
| Compliance Analysis and Remarks | | | | |
| [To be filled by audit firm assessors] | | | | |

| Control # | 65 | Compliance Status | Compliance  Noncompliance  [To be filled by audit firm assessors] | |
| --- | --- | --- | --- | --- |
| Reference # | TPC-65 | Source | SACS-002 Third Party Cybersecurity Standard | |
| Classification | * Outsourced Infrastructure * Customized Software | | | * Network Connectivity * Critical Data Processor * Cloud Computing Service |
| Control Statement | 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. | | | |
| Supporting Evidence | | | | |
| [To be filled by audit firm assessors for on-site assessment or by the Third Party representative for remote assessment] | | | | |
| Compliance Analysis and Remarks | | | | |
| [To be filled by audit firm assessors] | | | | |

| Control # | 66 | Compliance Status | Compliance  Noncompliance  [To be filled by audit firm assessors] | |
| --- | --- | --- | --- | --- |
| Reference # | TPC-66 | Source | SACS-002 Third Party Cybersecurity Standard | |
| Classification | * Outsourced Infrastructure * Customized Software | | | * Network Connectivity * Critical Data Processor * Cloud Computing Service |
| Control Statement | 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. | | | |
| Supporting Evidence | | | | |
| [To be filled by audit firm assessors for on-site assessment or by Third Party representative for remote assessment] | | | | |
| Compliance Analysis and Remarks | | | | |
| [To be filled by audit firm assessors] | | | | |

| Control # | 67 | Compliance Status | Compliance  Noncompliance  [To be filled by audit firm assessors] | |
| --- | --- | --- | --- | --- |
| Reference # | TPC-67 | Source | SACS-002 Third Party Cybersecurity Standard | |
| Classification | * Outsourced Infrastructure * Customized Software | | | * Network Connectivity * Critical Data Processor * Cloud Computing Service |
| Control Statement | 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 communication following a major disruption to business operations. | | | |
| Supporting Evidence | | | | |
| [To be filled by audit firm assessors for on-site assessment or by the Third Party representative for remote assessment] | | | | |
| Compliance Analysis and Remarks | | | | |
| [To be filled by audit firm assessors] | | | | |

| Control # | 68 | Compliance Status | Compliance  Noncompliance  [To be filled by audit firm assessors] | |
| --- | --- | --- | --- | --- |
| Reference # | TPC-68 | Source | SACS-002 Third Party Cybersecurity Standard | |
| Classification | * Outsourced Infrastructure * Customized Software | | | * Network Connectivity * Critical Data Processor * Cloud Computing Service |
| Control Statement | The 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 | | | |
| Supporting Evidence | | | | |
| [To be filled by audit firm assessors for on-site assessment or by the Third Party representative for remote assessment] | | | | |
| Compliance Analysis and Remarks | | | | |
| [To be filled by audit firm assessors] | | | | |

| Control # | 69 | Compliance Status | Compliance  Noncompliance  [To be filled by audit firm assessors] | |
| --- | --- | --- | --- | --- |
| Reference # | TPC-69 | Source | SACS-002 Third Party Cybersecurity Standard | |
| Classification | * Outsourced Infrastructure * Customized Software | | | * Network Connectivity * Critical Data Processor * Cloud Computing Service |
| Control Statement | The Third Party must ensure that owners of the Business Continuity (BC) plan are identified, and that the BC plan is reviewed and updated annually. | | | |
| Supporting Evidence | | | | |
| [To be filled by audit firm assessors for on-site assessment or by the Third Party representative for remote assessment] | | | | |
| Compliance Analysis and Remarks | | | | |
| [To be filled by audit firm assessors] | | | | |

| Control # | 70 | Compliance Status | Compliance  Noncompliance  [To be filled by audit firm assessors] | |
| --- | --- | --- | --- | --- |
| Reference # | TPC-70 | Source | SACS-002 Third Party Cybersecurity Standard | |
| Classification | * Outsourced Infrastructure * Customized Software | | | * Network Connectivity * Critical Data Processor * Cloud Computing Service |
| Control Statement | The Third Party must conduct Business Continuity drills at least annually. | | | |
| Supporting Evidence | | | | |
| [To be filled by audit firm assessors for on-site assessment or by Third Party representative for remote assessment] | | | | |
| Compliance Analysis and Remarks | | | | |
| [To be filled by audit firm assessors] | | | | |

| Control # | 71 | Compliance Status | Compliance  Noncompliance  [To be filled by audit firm assessors] | |
| --- | --- | --- | --- | --- |
| Reference # | TPC-71 | Source | SACS-002 Third Party Cybersecurity Standard | |
| Classification | * Outsourced Infrastructure * Customized Software | | | * Network Connectivity * Critical Data Processor * Cloud Computing Service |
| Control Statement | Third Party must have formal procedures for on-boarding employees. On-boarding procedures must include background checks (e.g. Verification of work histories). | | | |
| Supporting Evidence | | | | |
| [To be filled by audit firm assessors for on-site assessment or by the Third Party representative for remote assessment] | | | | |
| Compliance Analysis and Remarks | | | | |
| [To be filled by audit firm assessors] | | | | |

| Control # | 72 | Compliance Status | Compliance  Noncompliance  [To be filled by audit firm assessors] | |
| --- | --- | --- | --- | --- |
| Reference # | TPC-72 | Source | SACS-002 Third Party Cybersecurity Standard | |
| Classification | * Outsourced Infrastructure * Customized Software | | | * Network Connectivity * Critical Data Processor * Cloud Computing Service |
| Control Statement | Third Party must conduct security and source-code vulnerability scanning on all developed applications, and close all discovered vulnerabilities before deployment in production. | | | |
| Supporting Evidence | | | | |
| [To be filled by audit firm assessors for on-site assessment or by Third Party representative for remote assessment] | | | | |
| Compliance Analysis and Remarks | | | | |
| [To be filled by audit firm assessors] | | | | |

| Control # | 73 | Compliance Status | Compliance  Noncompliance  [To be filled by audit firm assessors] | |
| --- | --- | --- | --- | --- |
| Reference # | TPC-73 | Source | SACS-002 Third Party Cybersecurity Standard | |
| Classification | * Outsourced Infrastructure * Customized Software | | | * Network Connectivity * Critical Data Processor * Cloud Computing Service |
| Control Statement | All changes to the application must be properly authorized, and tested in a testing environment before moving to production. | | | |
| Supporting Evidence | | | | |
| [To be filled by audit firm assessors for on-site assessment or by Third Party representative for remote assessment] | | | | |
| Compliance Analysis and Remarks | | | | |
| [To be filled by audit firm assessors] | | | | |

| Control # | 74 | Compliance Status | Compliance  Noncompliance  [To be filled by audit firm assessors] | |
| --- | --- | --- | --- | --- |
| Reference # | TPC-74 | Source | SACS-002 Third Party Cybersecurity Standard | |
| Classification | * Outsourced Infrastructure * Customized Software | | | * Network Connectivity * Critical Data Processor * Cloud Computing Service |
| Control Statement | Third Party must have a process for secure system and software development life cycle in alignment with industry best practice. | | | |
| Supporting Evidence | | | | |
| [To be filled by audit firm assessors for on-site assessment or by Third Party representative for remote assessment] | | | | |
| Compliance Analysis and Remarks | | | | |
| [To be filled by audit firm assessors] | | | | |

| Control # | 75 | Compliance Status | Compliance  Noncompliance  [To be filled by audit firm assessors] | |
| --- | --- | --- | --- | --- |
| Reference # | TPC-75 | Source | SACS-002 Third Party Cybersecurity Standard | |
| Classification | * Outsourced Infrastructure * Customized Software | | | * Network Connectivity * Critical Data Processor * Cloud Computing Service |
| Control Statement | Third Party must retain all audit logs from information systems and applications storing, processing, or transmitting Saudi Aramco data for one (1) year. | | | |
| Supporting Evidence | | | | |
| [To be filled by audit firm assessors for on-site assessment or by Third Party representative for remote assessment] | | | | |
| Compliance Analysis and Remarks | | | | |
| [To be filled by audit firm assessors] | | | | |

| Control # | 76 | Compliance Status | Compliance  Noncompliance  [To be filled by audit firm assessors] | |
| --- | --- | --- | --- | --- |
| Reference # | TPC-76 | Source | SACS-002 Third Party Cybersecurity Standard | |
| Classification | * Outsourced Infrastructure * Customized Software | | | * Network Connectivity * Critical Data Processor * Cloud Computing Service |
| Control Statement | Firewalls must be implemented at the network perimeter and only required services must be allowed. Vulnerable services or insecure protocols should be blocked. | | | |
| Supporting Evidence | | | | |
| [To be filled by audit firm assessors for on-site assessment or by Third Party representative for remote assessment] | | | | |
| Compliance Analysis and Remarks | | | | |
| [To be filled by audit firm assessors] | | | | |

| Control # | 77 | Compliance Status | Compliance  Noncompliance  [To be filled by audit firm assessors] | |
| --- | --- | --- | --- | --- |
| Reference # | TPC-77 | Source | SACS-002 Third Party Cybersecurity Standard | |
| Classification | * Outsourced Infrastructure * Customized Software | | | * Network Connectivity * Critical Data Processor * Cloud Computing Service |
| Control Statement | Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS) must be implemented at the network perimeter. | | | |
| Supporting Evidence | | | | |
| [To be filled by audit firm assessors for on-site assessment or by Third Party representative for remote assessment] | | | | |
| Compliance Analysis and Remarks | | | | |
| [To be filled by audit firm assessors] | | | | |

| Control # | 78 | Compliance Status | Compliance  Noncompliance  [To be filled by audit firm assessors] | |
| --- | --- | --- | --- | --- |
| Reference # | TPC-78 | Source | SACS-002 Third Party Cybersecurity Standard | |
| Classification | * Outsourced Infrastructure * Customized Software | | | * Network Connectivity * Critical Data Processor * Cloud Computing Service |
| Control Statement | Signatures of firewalls, IDS, and IPS must be up-to-date. | | | |
| Supporting Evidence | | | | |
| [To be filled by audit firm assessors for on-site assessment or by Third Party representative for remote assessment] | | | | |
| Compliance Analysis and Remarks | | | | |
| [To be filled by audit firm assessors] | | | | |

| Control # | 79 | Compliance Status | Compliance  Noncompliance  [To be filled by audit firm assessors] | |
| --- | --- | --- | --- | --- |
| Reference # | TPC-79 | Source | SACS-002 Third Party Cybersecurity Standard | |
| Classification | * Outsourced Infrastructure * Customized Software | | | * Network Connectivity * Critical Data Processor * Cloud Computing Service |
| Control Statement | 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. | | | |
| Supporting Evidence | | | | |
| [To be filled by audit firm assessors for on-site assessment or by the Third Party representative for remote assessment] | | | | |
| Compliance Analysis and Remarks | | | | |
| [To be filled by audit firm assessors] | | | | |

| Control # | 80 | Compliance Status | Compliance  Noncompliance  [To be filled by audit firm assessors] | |
| --- | --- | --- | --- | --- |
| Reference # | TPC-80 | Source | SACS-002 Third Party Cybersecurity Standard | |
| Classification | * Outsourced Infrastructure * Customized Software | | | * Network Connectivity * Critical Data Processor * Cloud Computing Service |
| Control Statement | Third Party must monitor technology assets, systems, and applications to identify unauthorized access, or unauthorized activity. | | | |
| Supporting Evidence | | | | |
| [To be filled by audit firm assessors for on-site assessment or by the Third Party representative for remote assessment] | | | | |
| Compliance Analysis and Remarks | | | | |
| [To be filled by audit firm assessors] | | | | |

| Control # | 81 | Compliance Status | Compliance  Noncompliance  [To be filled by audit firm assessors] | |
| --- | --- | --- | --- | --- |
| Reference # | TPC-81 | Source | SACS-002 Third Party Cybersecurity Standard | |
| Classification | * Outsourced Infrastructure * Customized Software | | | * Network Connectivity * Critical Data Processor * Cloud Computing Service |
| Control Statement | 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. | | | |
| Supporting Evidence | | | | |
| [To be filled by audit firm assessors for on-site assessment or by the Third Party representative for remote assessment] | | | | |
| Compliance Analysis and Remarks | | | | |
| [To be filled by audit firm assessors] | | | | |

| Control # | 82 | Compliance Status | Compliance  Noncompliance  [To be filled by audit firm assessors] | |
| --- | --- | --- | --- | --- |
| Reference # | TPC-82 | Source | SACS-002 Third Party Cybersecurity Standard | |
| Classification | * Outsourced Infrastructure * Customized Software | | | * Network Connectivity * Critical Data Processor * Cloud Computing Service |
| Control Statement | 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. | | | |
| Supporting Evidence | | | | |
| [To be filled by audit firm assessors for on-site assessment or by Third Party representative for remote assessment] | | | | |
| Compliance Analysis and Remarks | | | | |
| [To be filled by audit firm assessors] | | | | |

| Control # | 83 | Compliance Status | Compliance  Noncompliance  [To be filled by audit firm assessors] | |
| --- | --- | --- | --- | --- |
| Reference # | TPC-83 | Source | SACS-002 Third Party Cybersecurity Standard | |
| Classification | * Outsourced Infrastructure * Customized Software | | | * Network Connectivity * Critical Data Processor * Cloud Computing Service |
| Control Statement | Privileged accounts activity must be logged and monitored on a regular basis. | | | |
| Supporting Evidence | | | | |
| [To be filled by audit firm assessors for on-site assessment or by the third Party representative for remote assessment] | | | | |
| Compliance Analysis and Remarks | | | | |
| [To be filled by audit firm assessors] | | | | |

| Control # | 84 | Compliance Status | Compliance  Noncompliance  [To be filled by audit firm assessors] | |
| --- | --- | --- | --- | --- |
| Reference # | TPC-84 | Source | SACS-002 Third Party Cybersecurity Standard | |
| Classification | * Outsourced Infrastructure * Customized Software | | | * Network Connectivity * Critical Data Processor * Cloud Computing Service |
| Control Statement | Non-authorized devices (such as personal devices and mobile phones) must not be used to store, process, or access assets. | | | |
| Supporting Evidence | | | | |
| [To be filled by audit firm assessors for on-site assessment or by Third Party representative for remote assessment] | | | | |
| Compliance Analysis and Remarks | | | | |
| [To be filled by audit firm assessors] | | | | |

| Control # | 85 | Compliance Status | Compliance  Noncompliance  [To be filled by audit firm assessors] | |
| --- | --- | --- | --- | --- |
| Reference # | TPC-85 | Source | SACS-002 Third Party Cybersecurity Standard | |
| Classification | * Outsourced Infrastructure * Customized Software | | | * Network Connectivity * Critical Data Processor * Cloud Computing Service |
| Control Statement | Monthly Vulnerability scans must be conducted to evaluate configuration, patches, and services for known vulnerabilities. | | | |
| Supporting Evidence | | | | |
| [To be filled by audit firm assessors for on-site assessment or by the Third Party representative for remote assessment] | | | | |
| Compliance Analysis and Remarks | | | | |
| [To be filled by audit firm assessors] | | | | |

| Control # | 86 | Compliance Status | Compliance  Noncompliance  [To be filled by audit firm assessors] | |
| --- | --- | --- | --- | --- |
| Reference # | TPC-86 | Source | SACS-002 Third Party Cybersecurity Standard | |
| Classification | * Outsourced Infrastructure * Customized Software | | | * Network Connectivity * Critical Data Processor * Cloud Computing Service |
| Control Statement | Physical access to the facility where information systems reside must be restricted to authorized personnel and reviewed on a regular basis. | | | |
| Supporting Evidence | | | | |
| [To be filled by audit firm assessors for on-site assessment or by the Third Party representative for remote assessment] | | | | |
| Compliance Analysis and Remarks | | | | |
| [To be filled by audit firm assessors] | | | | |

| Control # | 87 | Compliance Status | Compliance  Noncompliance  [To be filled by audit firm assessors] | |
| --- | --- | --- | --- | --- |
| Reference # | TPC-87 | Source | SACS-002 Third Party Cybersecurity Standard | |
| Classification | * Outsourced Infrastructure * Customized Software | | | * Network Connectivity * Critical Data Processor * Cloud Computing Service |
| Control Statement | Information systems and applications must log auditable events as stated in SACS-002 Third Party Cybersecurity Standard Appendix C. | | | |
| Supporting Evidence | | | | |
| [To be filled by audit firm assessors for on-site assessment or by the Third Party representative for remote assessment] | | | | |
| Compliance Analysis and Remarks | | | | |
| [To be filled by audit firm assessors] | | | | |

| Control # | 88 | Compliance Status | Compliance  Noncompliance  [To be filled by audit firm assessors] | |
| --- | --- | --- | --- | --- |
| Reference # | TPC-88 | Source | SACS-002 Third Party Cybersecurity Standard | |
| Classification | * Outsourced Infrastructure * Customized Software | | | * Network Connectivity * Critical Data Processor * Cloud Computing Service |
| Control Statement | Incident management policy and plan must be documented, maintained, and communicated to management and appropriate team members. | | | |
| Supporting Evidence | | | | |
| [To be filled by audit firm assessors for on-site assessment or by the Third Party representative for remote assessment] | | | | |
| Compliance Analysis and Remarks | | | | |
| [To be filled by audit firm assessors] | | | | |

| Control # | 89 | Compliance Status | Compliance  Noncompliance  [To be filled by audit firm assessors] | |
| --- | --- | --- | --- | --- |
| Reference # | TPC-89 | Source | SACS-002 Third Party Cybersecurity Standard | |
| Classification | * Outsourced Infrastructure * Customized Software | | | * Network Connectivity * Critical Data Processor * Cloud Computing Service |
| Control Statement | 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. | | | |
| Supporting Evidence | | | | |
| [To be filled by audit firm assessors for on-site assessment or by the third party representative for remote assessment] | | | | |
| Compliance Analysis and Remarks | | | | |
| [To be filled by audit firm assessors] | | | | |

| Control # | 90 | Compliance Status | Compliance  Noncompliance  [To be filled by audit firm assessors] | |
| --- | --- | --- | --- | --- |
| Reference # | TPC-90 | Source | SACS-002 Third Party Cybersecurity Standard | |
| Classification | * Outsourced Infrastructure * Customized Software | | | * Network Connectivity * Critical Data Processor * Cloud Computing Service |
| Control Statement | The Third Party must track, classify, and document all cybersecurity Incidents. | | | |
| Supporting Evidence | | | | |
| [To be filled by audit firm assessors for on-site assessment or by the third Party representative for remote assessment] | | | | |
| Compliance Analysis and Remarks | | | | |
| [To be filled by audit firm assessors] | | | | |

| Control # | 91 | Compliance Status | Compliance  Noncompliance  [To be filled by audit firm assessors] | |
| --- | --- | --- | --- | --- |
| Reference # | TPC-91 | Source | SACS-002 Third Party Cybersecurity Standard | |
| Classification | * Outsourced Infrastructure * Customized Software | | | * Network Connectivity * Critical Data Processor * Cloud Computing Service |
| Control Statement | 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. | | | |
| Supporting Evidence | | | | |
| [To be filled by audit firm assessors for on-site assessment or by the Third Party representative for remote assessment] | | | | |
| Compliance Analysis and Remarks | | | | |
| [To be filled by audit firm assessors] | | | | |

| Control # | 92 | Compliance Status | Compliance  Noncompliance  [To be filled by audit firm assessors] | |
| --- | --- | --- | --- | --- |
| Reference # | TPC-92 | Source | SACS-002 Third Party Cybersecurity Standard | |
| Classification | * Outsourced Infrastructure * Customized Software | | | * Network Connectivity * Critical Data Processor * Cloud Computing Service |
| Control Statement | If 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. | | | |
| Supporting Evidence | | | | |
| [To be filled by audit firm assessors for on-site assessment or by the Third Party representative for remote assessment] | | | | |
| Compliance Analysis and Remarks | | | | |
| [To be filled by audit firm assessors] | | | | |

1. Report Summary

|  |  |  |
| --- | --- | --- |
|  | **Compliance** | **Noncompliance** |
| **Count (#)** | x | y |
| **Percentage (%)** | % | % |