NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Saudi Arabia - SACS - 002 Third Party Cybersecurity Standard (2022)
Focal Document URL: https://www.aramco.com/-/media/downloads/working-with-us/ccc/sacs-002-third-party-cybersecurity-standard.pdf
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-sau-sacs-002-2022.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
I	Purpose	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
II	Scope	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
III	Change Control	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
IV	Conflicts and Deviations	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
V	Revision	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
VI	Cybersecurity Controls Instructions	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
VII	Third Party Cybersecurity Controls	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
VII.A	General Requirements	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
VII.A.TPC-1	Governance (GV)	Third Party must establish, maintain and communicate a Cybersecurity Acceptable Use Policy (AUP) governing the use of Third Party Technology Assets.	Functional	Intersects With	Terms of Employment	HRS-05	Mechanisms exist to require all employees and contractors to apply cybersecurity and data protection principles in their daily work to enable secure, compliant and resilient capabilities.	5	
VII.A.TPC-1	Governance (GV)	Third Party must establish, maintain and communicate a Cybersecurity Acceptable Use Policy (AUP) governing the use of Third Party Technology Assets.	Functional	Intersects With	Rules of Behavior	HRS-05.1	Mechanisms exist to define acceptable and unacceptable rules of behavior for the use of technologies, including consequences for unacceptable behavior.	5	
VII.A.TPC-2	Access Control (AC)	Password protection measures must be enforced by the Third Party. The following are recommended measures:	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
VII.A.TPC-2	Access Control (AC)	Password protection measures must be enforced by the Third Party. The following are recommended measures:	Functional	Intersects With	Password-Based Authentication	IAC-10.1	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	5	
VII.A.TPC-2-BP1	Access Control (AC)	Minimum length: 8 alphanumeric characters and special characters.	Functional	Subset Of	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	10	Bullet points within FD were not labeled so numbering was added to improve mappability.
VII.A.TPC-2-BP2	Access Control (AC)	History: last 12 passwords.	Functional	Subset Of	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	10	Bullet points within FD were not labeled so numbering was added to improve mappability.
VII.A.TPC-2-BP3	Access Control (AC)	Maximum age: 90 days for login authentication.	Functional	Subset Of	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	10	Bullet points within FD were not labeled so numbering was added to improve mappability.
VII.A.TPC-2-BP4	Access Control (AC)	Account lockout threshold: 10 invalid login attempts.	Functional	Subset Of	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	10	Bullet points within FD were not labeled so numbering was added to improve mappability.
VII.A.TPC-2-BP5	Access Control (AC)	Screen saver settings: automatically locked within 15 minutes of inactivity.	Functional	Subset Of	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	10	Bullet points within FD were not labeled so numbering was added to improve mappability.
VII.A.TPC-3	Access Control (AC)	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.	Functional	Intersects With	Protection of Authenticators	IAC-10.5	Mechanisms exist to protect authenticators commensurate with the sensitivity of the information to which use of the authenticator permits access.	5	
VII.A.TPC-4	Access Control (AC)	Multi-factor authentication must be enforced on all remote access, including access from the Internet, to Third Party Company computing resources.	Functional	Intersects With	Multi-Factor Authentication (MFA)	IAC-06	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/ or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive and/or regulated data.	5	
VII.A.TPC-5	Access Control (AC)	Multi-factor authentication must be enforced on all access to Cloud services utilized by the Third Party, including access to cloud-based email.	Functional	Intersects With	Multi-Factor Authentication (MFA)	IAC-06	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/ or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive and/or regulated data.	5	
VII.A.TPC-6	Access Control (AC)	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.	Functional	Intersects With	Automated Employment Status Notifications	HRS-09.4	Automated mechanisms exist to notify Identity and Access Management (IAM) personnel or roles upon termination of an individual employment or contract.	5	
VII.A.TPC-6	Access Control (AC)	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.	Functional	Intersects With	User Provisioning & De-Provisioning	IAC-07	Mechanisms exist to utilize a formal user registration and de-registration process that governs the assignment of access rights.	5	
VII.A.TPC-7	Awareness and Training (AT)	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:	Functional	Intersects With	Security, Compliance & Resilience Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate security, compliance and resilience awareness education and training that is relevant for their job function.	5	
VII.A.TPC-7.1	Awareness and Training (AT)	Internet and social media security	Functional	Subset Of	Security, Compliance & Resilience Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate security, compliance and resilience awareness education and training that is relevant for their job function.	10	
VII.A.TPC-7.2	Awareness and Training (AT)	Cybersecurity Acceptable Use	Functional	Subset Of	Security, Compliance & Resilience Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate security, compliance and resilience awareness education and training that is relevant for their job function.	10	
VII.A.TPC-7.3	Awareness and Training (AT)	Social Engineering and phishing emails	Functional	Intersects With	Social Engineering & Mining	SAT-02.2	Mechanisms exist to include awareness training on recognizing and reporting potential and actual instances of social engineering and social mining.	5	
VII.A.TPC-7.4	Awareness and Training (AT)	Sharing credentials (i.e. username and password)	Functional	Subset Of	Security, Compliance & Resilience Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate security, compliance and resilience awareness education and training that is relevant for their job function.	10	
VII.A.TPC-7.5	Awareness and Training (AT)	Data Security	Functional	Subset Of	Security, Compliance & Resilience Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate security, compliance and resilience awareness education and training that is relevant for their job function.	10	
VII.A.TPC-8	Awareness and Training (AT)	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.	Functional	Intersects With	Technology Use Restrictions	HRS-05.3	Mechanisms exist to establish usage restrictions and implementation guidance for organizational technologies based on the potential to cause damage to Technology Assets, Applications and/or Services (TAAS), if used maliciously.	5	
VII.A.TPC-8	Awareness and Training (AT)	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.	Functional	Subset Of	Security, Compliance & Resilience Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate security, compliance and resilience awareness education and training that is relevant for their job function.	10	
VII.A.TPC-9	Awareness and Training (AT)	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.	Functional	Intersects With	Confidentiality Agreements	HRS-06.1	Mechanisms exist to require Non-Disclosure Agreements (NDAs) or similar confidentiality agreements that reflect the needs to protect data and operational details, or both employees and third-parties.	5	
VII.A.TPC-9	Awareness and Training (AT)	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.	Functional	Subset Of	Security, Compliance & Resilience Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate security, compliance and resilience awareness education and training that is relevant for their job function.	10	
VII.A.TPC-10	Data Security (DS)	All Third Party Technology Assets and Systems must be password protected.	Functional	Subset Of	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	10	
VII.A.TPC-11	Data Security (DS)	Third Party Technology Assets and Systems must be regularly updated with operating system (OS), software and applets patches (i.e. Adobe, Flash, Java etc.).	Functional	Intersects With	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	5	
VII.A.TPC-12	Data Security (DS)	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.	Functional	Intersects With	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize antimalware technologies to detect and eradicate malicious code.	5	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Saudi Arabia - SACS - 002 Third Party Cybersecurity Standard (2022)
Focal Document URL: https://www.aramco.com/-/media/downloads/working-with-us/ccc/sacs-002-third-party-cybersecurity-standard.pdf
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-sau-sacs-002-2022.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
VII.A.TPC-13	Data Security (DS)	Third party must implement Sender Policy Framework (SPF) technology on the mail server.	Functional	Intersects With	Sender Policy Framework (SPF)	NET-10.3	Mechanisms exist to validate the legitimacy of email communications through configuring a Domain Naming Service (DNS) Sender Policy Framework (SPF) record to specify the IP addresses and/or hostnames that are authorized to send email from the specified domain.	5	
VII.A.TPC-14	Data Security (DS)	Third party must enforce Sender Policy Framework (SPF) feature on Saudi Aramco email domains: Aramco.com and Aramco.com.sa.	Functional	Intersects With	Sender Policy Framework (SPF)	NET-10.3	Mechanisms exist to validate the legitimacy of email communications through configuring a Domain Naming Service (DNS) Sender Policy Framework (SPF) record to specify the IP addresses and/or hostnames that are authorized to send email from the specified domain.	5	
VII.A.TPC-15	Data Security (DS)	Third Party must publish SPF record in DNS server.	Functional	Intersects With	Sender Policy Framework (SPF)	NET-10.3	Mechanisms exist to validate the legitimacy of email communications through configuring a Domain Naming Service (DNS) Sender Policy Framework (SPF) record to specify the IP addresses and/or hostnames that are authorized to send email from the specified domain.	5	
VII.A.TPC-16	Data Security (DS)	Third Party must inspect all incoming emails originating from the Internet using anti-spam protection.	Functional	Intersects With	Phishing & Spam Protection	END-08	Mechanisms exist to utilize anti-phishing and spam protection technologies to detect and take action on unsolicited messages transported by electronic mail.	5	
VII.A.TPC-17	Data Security (DS)	Third Party must use a private email domain. Generic domains, such as Gmail and Hotmail, must not be used.	Functional	Intersects With	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	5	
VII.A.TPC-18	Information Protection Processes and Procedures (IP)	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.	Functional	Intersects With	Onboarding, Transferring & Offboarding Personnel	HRS-01.1	Mechanisms exist to proactively govern the following personnel management actions: (1) Onboarding new personnel (e.g., new hires); (2) Transferring personnel into new roles within the organization; and (3) Offboarding personnel (e.g., termination of employment).	5	
VII.A.TPC-19	Information Protection Processes and Procedures (IP)	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. Third party shall certify in a signed letter to Saudi Aramco that the data sanitization has been successfully completed.	Functional	Intersects With	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	5	
VII.A.TPC-19	Information Protection Processes and Procedures (IP)	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. Third party shall certify in a signed letter to Saudi Aramco that the data sanitization has been successfully completed.	Functional	Intersects With	System Media Sanitization	DCH-09	Mechanisms exist to sanitize system media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse.	5	
VII.A.TPC-19	Information Protection Processes and Procedures (IP)	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. Third party shall certify in a signed letter to Saudi Aramco that the data sanitization has been successfully completed.	Functional	Intersects With	Media & Data Retention	DCH-18	Mechanisms exist to retain media and data in accordance with applicable statutory, regulatory and contractual obligations.	5	
VII.A.TPC-20	Protective Technology (PT)	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.	Functional	Intersects With	Third-Party Attestation (3PA)	TPM-05.8	Mechanisms exist to obtain an attestation from an independent Third-Party Assessment Organization (3PAO) that provides assurance of conformity with specified statutory, regulatory and contractual obligations for security, compliance and resilience controls, including any flow-down requirements to contractors and subcontractors.	5	
VII.A.TPC-21	Protective Technology (PT)	Third Party must renew the CCC every two (2) years.	Functional	Intersects With	Third-Party Attestation (3PA)	TPM-05.8	Mechanisms exist to obtain an attestation from an independent Third-Party Assessment Organization (3PAO) that provides assurance of conformity with specified statutory, regulatory and contractual obligations for security, compliance and resilience controls, including any flow-down requirements to contractors and subcontractors.	5	
VII.A.TPC-22	Protective Technology (PT)	Firewalls must be configured and enabled on endpoint devices.	Functional	Intersects With	Software Firewall	END-05	Mechanisms exist to utilize host-based firewall software, or a similar technology, on all endpoint devices, where technically feasible.	5	
VII.A.TPC-23	Communications (CO)	If Third Party discovers a Cybersecurity Incident, Third Party must (besides its continuous efforts to resolve and mitigate the Incident):	Functional	Intersects With	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity and data protection-related incidents.	5	
VII.A.TPC-23-BP1	Communications (CO)	Notify SAUDI ARAMCO within twenty-four (24) hours of discovering the Incident	Functional	Intersects With	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	5	Bullet points within FD were not labeled so numbering was added to improve mappability.
VII.A.TPC-23-BP2	Communications (CO)	Follow the Cybersecurity Incident Response Instructions set forth in Appendix A.	Functional	Intersects With	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	5	Bullet points within FD were not labeled so numbering was added to improve mappability.
VII.A.TPC-23-BP2	Communications (CO)	Follow the Cybersecurity Incident Response Instructions set forth in Appendix A.	Functional	Intersects With	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	5	Bullet points within FD were not labeled so numbering was added to improve mappability.
VII.B	Specific Requirements	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
VII.B.TPC-24	Asset Management (AM)	Third Party must have policies and processes to classify information in terms of its value, criticality and confidentiality.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	
VII.B.TPC-24	Asset Management (AM)	Third Party must have policies and processes to classify information in terms of its value, criticality and confidentiality.	Functional	Intersects With	Data & Asset Classification	DCH-02	Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.	5	
VII.B.TPC-25	Governance (GV)	Third Party must establish, maintain and communicate Cybersecurity Policies and Standards.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	
VII.B.TPC-26	Governance (GV)	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.	Functional	Subset Of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	
VII.B.TPC-26	Governance (GV)	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.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
VII.B.TPC-26	Governance (GV)	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.	Functional	Intersects With	Competency Requirements for Security-Related Positions	HRS-03.2	Mechanisms exist to ensure that all security-related positions are staffed by qualified individuals who have the necessary skill set.	5	
VII.B.TPC-27	Risk Assessment (RA)	Third Party must conduct annual external Penetration Testing on its IT infrastructure systems, and internet facing applications.	Functional	Intersects With	Penetration Testing	VPM-07	Mechanisms exist to conduct penetration testing on Technology Assets, Applications and/or Services (TAAS).	5	
VII.B.TPC-28	Risk Assessment (RA)	Third Party must conduct annual external Penetration Testing on Cloud Computing Service(s) used by Saudi Aramco	Functional	Intersects With	Penetration Testing	VPM-07	Mechanisms exist to conduct penetration testing on Technology Assets, Applications and/or Services (TAAS).	5	
VII.B.TPC-29	Risk Assessment (RA)	If Third Party is hosting a website for Saudi Aramco, annual Penetration Testing must be conducted to test website security.	Functional	Intersects With	Penetration Testing	VPM-07	Mechanisms exist to conduct penetration testing on Technology Assets, Applications and/or Services (TAAS).	5	
VII.B.TPC-30	Risk Assessment (RA)	Third party data center must be certified by industry recognized authority	Functional	No Relationship	N/A	N/A	N/A	0	
VII.B.TPC-31	Risk Management Strategy (RM)	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.	Functional	Intersects With	Risk Assessment	RSK-04	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Saudi Arabia - SACS - 002 Third Party Cybersecurity Standard (2022)
Focal Document URL: https://www.aramco.com/-/media/downloads/working-with-us/ccc/sacs-002-third-party-cybersecurity-standard.pdf
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-sau-sacs-002-2022.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
VII.B.TPC-32	Access Control (AC)	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.	Functional	Intersects With	Identification & Authentication for Organizational Users	IAC-02	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) organizational users and processes acting on behalf of organizational users.	5	
VII.B.TPC-32	Access Control (AC)	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.	Functional	Intersects With	Identification & Authentication for Non-Organizational Users	IAC-03	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) third-party users and processes that provide services to the organization.	5	
VII.B.TPC-32	Access Control (AC)	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.	Functional	Intersects With	Account Management	IAC-15	Mechanisms exist to: (1) Define authorized system account types; (2) Define prohibited system account types; and (3) Proactively govern individual, group, system, service, application, guest and temporary accounts.	5	
VII.B.TPC-33	Access Control (AC)	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.	Functional	Intersects With	Periodic Review of Account Privileges	IAC-17	Mechanisms exist to periodically-review the privileges assigned to individuals and service accounts to validate the need for such privileges and reassign or remove unnecessary privileges, as necessary.	5	
VII.B.TPC-34	Access Control (AC)	All privileged accounts must be limited, justified and reviewed on regular basis.	Functional	Intersects With	Role-Based Access Control (RBAC)	IAC-08	Mechanisms exist to enforce Role-Based Access Control (RBAC) for Technology Assets, Applications, Services and/or Data (TAASD) to restrict access to individuals assigned specific roles with legitimate business needs.	5	
VII.B.TPC-34	Access Control (AC)	All privileged accounts must be limited, justified and reviewed on regular basis.	Functional	Intersects With	Least Privilege	IAC-21	Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business functions.	5	
VII.B.TPC-35	Access Control (AC)	Remote administrative access from the Internet must not be allowed, unless explicitly approved, restricted and controlled.	Functional	Intersects With	Remote Privileged Commands & Sensitive Data Access	NET-14.4	Mechanisms exist to restrict the execution of privileged commands and access to security-relevant information via remote access only for compelling operational needs.	5	
VII.B.TPC-36	Access Control (AC)	Network connections to information systems and applications at the Third Parties location must be authorized and monitored.	Functional	Intersects With	Use of External Technology Assets, Applications and/or Services (TAAS)	DCH-13	Mechanisms exist to govern how external parties, including Technology Assets, Applications and/or Services (TAAS), are used to securely store, process and transmit data.	5	
VII.B.TPC-36	Access Control (AC)	Network connections to information systems and applications at the Third Parties location must be authorized and monitored.	Functional	Intersects With	External System Connections	NET-05.1	Mechanisms exist to prohibit the direct connection of a sensitive system to an external network without the use of an organization-defined boundary protection device.	5	
VII.B.TPC-36	Access Control (AC)	Network connections to information systems and applications at the Third Parties location must be authorized and monitored.	Functional	Intersects With	Third-Party Services	TPM-04	Mechanisms exist to mitigate the risks associated with third-party access to the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5	
VII.B.TPC-37	Access Control (AC)	Multi-factor authentication must be enforced on all privileged accounts access including remote access to information systems and applications.	Functional	Intersects With	Multi-Factor Authentication (MFA)	IAC-06	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/ or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive and/or regulated data.	5	
VII.B.TPC-38	Access Control (AC)	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.	Functional	Intersects With	Sensitive / Regulated Data Enclave (Secure Zone)	NET-06.3	Mechanisms exist to implement segmentation controls to restrict inbound and outbound connectivity for sensitive and/or regulated data enclaves (secure zones).	8	
VII.B.TPC-38	Access Control (AC)	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.	Functional	Intersects With	On-Site Client Segregation	PES-18	Mechanisms exist to ensure client-specific sensitive and/or regulated data is isolated from other data when client-specific sensitive and/or regulated data is processed or stored within multi-client workspaces.	3	
VII.B.TPC-39	Access Control (AC)	Saudi Aramco Critical Data documents must only be shared with limited individuals who are part of the work specified in the Contract.	Functional	Intersects With	Sensitive / Regulated Data Protection	DCH-01.2	Mechanisms exist to protect sensitive and/or regulated data wherever it is processed and/or stored.	5	
VII.B.TPC-39	Access Control (AC)	Saudi Aramco Critical Data documents must only be shared with limited individuals who are part of the work specified in the Contract.	Functional	Intersects With	Defining Access Authorizations for Sensitive / Regulated Data	DCH-01.4	Mechanisms exist to explicitly define authorizations for specific individuals and/or roles for logical and /or physical access to sensitive and/or regulated data.	5	
VII.B.TPC-40	Access Control (AC)	Servers and workstations subnets must be segmented and access between them is restricted and monitored.	Functional	Intersects With	Network Segmentation (macrosegmentation)	NET-06	Mechanisms exist to implement network segmentation within network architectures to isolate Technology Assets, Applications and/or Services (TAAS) from other network resources.	5	
VII.B.TPC-41	Access Control (AC)	Servers accessible from the Internet must be placed in a DMZ (i.e. perimeter network) with restricted access to internal subnets.	Functional	Intersects With	Use of Demilitarized Zones (DMZ)	WEB-02	Mechanisms exist to utilize a Demilitarized Zone (DMZ) to restrict inbound traffic to authorized Technology Assets, Applications and/or Services (TAAS) on certain services, protocols and ports.	5	
VII.B.TPC-42	Access Control (AC)	Wireless networks accessing information systems must use strong encryption for authentication and transmission, such as WPA2 or WPA2 Enterprise.	Functional	Intersects With	Wireless Access Authentication & Encryption	CRY-07	Mechanisms exist to protect the confidentiality and integrity of wireless networking technologies by implementing authentication and strong encryption.	5	
VII.B.TPC-42	Access Control (AC)	Wireless networks accessing information systems must use strong encryption for authentication and transmission, such as WPA2 or WPA2 Enterprise.	Functional	Intersects With	Authentication & Encryption	NET-15.1	Mechanisms exist to secure Wi-Fi (e.g., IEEE 802.11) and prevent unauthorized access by: (1) Authenticating devices trying to connect; and	5	
VII.B.TPC-43	Access Control (AC)	Third Party data center must have the required tier rating and high-availability of service failover as determined by Saudi Aramco	Functional	No Relationship	N/A	N/A	N/A	0	
VII.B.TPC-44	Access Control (AC)	Multi-Factor authentication must be enforced on Saudi Aramco users accessing Cloud Service Provider's Public Cloud Computing Service	Functional	Intersects With	Multi-Factor Authentication (MFA)	IAC-06	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for:	5	
VII.B.TPC-45	Access Control (AC)	Multi-Factor authentication must be enforced on end-users accessing Content Management Services (CMS) of Cloud Computing Service.	Functional	Intersects With	Multi-Factor Authentication (MFA)	IAC-06	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/ or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive and/or regulated data.	5	
VII.B.TPC-46	Access Control (AC)	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.	Functional	Intersects With	Lockable Physical Casings	PES-03.2	Physical access control mechanisms exist to protect system components from unauthorized physical access (e.g., lockable physical casings).	5	
VII.B.TPC-46	Access Control (AC)	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.	Functional	Intersects With	Access To Critical Systems	PES-03.4	Physical access control mechanisms exist to enforce physical access to critical systems or sensitive and/or regulated data, in addition to the physical access controls for the facility.	5	
VII.B.TPC-47	Access Control (AC)	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:	Functional	Intersects With	Visitor Control	PES-06	Physical access control mechanisms exist to identify, authorize and monitor visitors before allowing access to the facility (other than areas designated as publicly accessible).	5	
VII.B.TPC-47-BP1	Access Control (AC)	Visitor identification (e.g. Government ID(	Functional	Intersects With	Identification Requirement	PES-06.2	Physical access control mechanisms exist to requires at least one(1) form of government-issued or organization-issued photo identification to authenticate individuals before they can gain access to the facility.	5	
VII.B.TPC-47-BP2	Access Control (AC)	Visit Purpose	Functional	Intersects With	Visitor Control	PES-06	Physical access control mechanisms exist to identify, authorize and monitor visitors before allowing access to the facility (other than areas designated as publicly accessible).	5	
VII.B.TPC-47-BP3	Access Control (AC)	Check in/check out date and time	Functional	Intersects With	Visitor Control	PES-06	Physical access control mechanisms exist to identify, authorize and monitor visitors before allowing access to the facility (other than areas designated as publicly accessible).	5	
VII.B.TPC-48	Access Control (AC)	Visitors accessing Critical Facilities must be escorted at all times.	Functional	Intersects With	Restrict Unescorted Access	PES-06.3	Physical access control mechanisms exist to restrict unescorted access to facilities to personnel with required security clearances, formal access authorizations and validate the need for access.	5	
VII.B.TPC-49	Access Control (AC)	Third Party must dedicate an access restricted working area for personnel with access to Saudi Aramco network.	Functional	Intersects With	Working in Secure Areas	PES-04.1	Physical security mechanisms exist to allow only authorized personnel access to secure areas.	5	
VII.B.TPC-49	Access Control (AC)	Third Party must dedicate an access restricted working area for personnel with access to Saudi Aramco network.	Functional	Intersects With	On-Site Client Segregation	PES-18	Mechanisms exist to ensure client-specific sensitive and/or regulated data is isolated from other data when client-specific sensitive and/or	5	
VII.B.TPC-50	Access Control (AC)	Backup media must be secured to block/inhibit unauthorized physical access.	Functional	Intersects With	Cryptographic Protection	BCD-11.4	Cryptographic mechanisms exist to prevent the unauthorized disclosure and/or modification of backup information.	5	
VII.B.TPC-51	Access Control (AC)	Technology Assets and Systems connected to the internet must be licensed and supported by the provider.	Functional	Intersects With	Unsupported Technology Assets, Applications	TDA-17	Mechanisms exist to prevent unsupported Technology Assets, Applications and/or Services (TAAS) by:	5	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Saudi Arabia - SACS - 002 Third Party Cybersecurity Standard (2022)
Focal Document URL: https://www.aramco.com/-/media/downloads/working-with-us/ccc/sacs-002-third-party-cybersecurity-standard.pdf
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-sau-sacs-002-2022.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
VII.B.TPC-52	Access Control (AC)	Third Party must encrypt data in transit (e.g. SSH, FTPS, HTTPS, TLS, IPSEC).	Functional	Intersects With	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	5	
VII.B.TPC-53	Access Control (AC)	Third Party must encrypt (e.g. using HTTPS) sessions where Critical Saudi Aramco information or data will be transmitted from and to the Public	Functional	Intersects With	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	5	
VII.B.TPC-54	Access Control (AC)	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.	Functional	Intersects With	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	5	
VII.B.TPC-55	Access Control (AC)	Encryption key management capability, including preservation and retrieval, must be defined, applied, and periodically reviewed.	Functional	Intersects With	Cryptographic Key Management	CRY-09	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	5	
VII.B.TPC-56	Access Control (AC)	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.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening	5	
VII.B.TPC-57	Access Control (AC)	Access to the Internet must be restricted by Content-filtering technologies to block:	Functional	Intersects With	DNS & Content Filtering	NET-18	Mechanisms exist to force Internet-bound network traffic through a proxy device (e.g., Policy Enforcement Point (PEP)) for URL content filtering and DNS filtering to limit a user's ability to connect to dangerous or prohibited Internet sites.	5	
VII.B.TPC-57-BP1	Access Control (AC)	Malicious and suspicious websites.	Functional	Intersects With	DNS & Content Filtering	NET-18	Mechanisms exist to force Internet-bound network traffic through a proxy device (e.g., Policy Enforcement Point (PEP)) for URL content filtering and DNS filtering to limit a user's ability to connect to dangerous or prohibited Internet sites.	5	
VII.B.TPC-57-BP2	Access Control (AC)	Personal and non-company email services.	Functional	Intersects With	DNS & Content Filtering	NET-18	Mechanisms exist to force Internet-bound network traffic through a proxy device (e.g., Policy Enforcement Point (PEP)) for URL content filtering and DNS filtering to limit a user's ability to connect to dangerous or prohibited Internet sites.	5	
VII.B.TPC-57-BP3	Access Control (AC)	Personal and non-company approved public cloud services.	Functional	Intersects With	DNS & Content Filtering	NET-18	Mechanisms exist to force Internet-bound network traffic through a proxy device (e.g., Policy Enforcement Point (PEP)) for URL content filtering and DNS filtering to limit a user's ability to connect to dangerous or prohibited Internet sites.	5	
VII.B.TPC-58	Access Control (AC)	Documents containing Saudi Aramco Critical Data, must be encrypted and stored securely with access limited to authorized personnel.	Functional	Intersects With	Sensitive / Regulated Data Protection	DCH-01.2	Mechanisms exist to protect sensitive and/or regulated data wherever it is processed and/or stored.	5	
VII.B.TPC-59	Access Control (AC)	Remote wipe solution must be installed on all tablets and mobile phones used to receive, store and/or produce Critical Data for Saudi Aramco.	Functional	Intersects With	Remote Purging	MDM-05	Mechanisms exist to remotely purge selected information from mobile devices.	5	
VII.B.TPC-60	Access Control (AC)	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.	Functional	Intersects With	Input Data Validation	TDA-18	Mechanisms exist to check the validity of information inputs.	5	
VII.B.TPC-61	Access Control (AC)	Application error messages must not display any sensitive technical information.	Functional	Intersects With	Error Handling	TDA-19	Mechanisms exist to handle error conditions by: (1) Identifying potentially security-relevant error conditions; (2) Generating error messages that provide information necessary for	5	
VII.B.TPC-61	Access Control (AC)	Application error messages must not display any sensitive technical information.	Functional	Intersects With	Designated Roles To View Error Messages	TDA-19.1	Mechanisms exist to: (1) Define personnel and/or role(s) authorized to receive security-relevant error messages; and (2) Restrict access to error messages to authorized personnel and/or role(s).	5	
VII.B.TPC-62	Access Control (AC)	Application or Cloud Computing Services must not store, generate, transmit, or use plain-text passwords.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
VII.B.TPC-62	Access Control (AC)	Application or Cloud Computing Services must not store, generate, transmit, or use plain-text passwords.	Functional	Intersects With	Authenticator Management	IAC-10	Mechanisms exist to: (1) Securely manage authenticators for users and devices; and (2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.	5	
VII.B.TPC-63	Information Protection Processes and Procedures (IP)	Third Party must create and manage baseline configurations to harden information systems. The hardening process must address configurations such as:	Functional	Equal	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	10	
VII.B.TPC-63-BP1	Information Protection Processes and Procedures (IP)	Resetting default usernames/passwords	Functional	Subset Of	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	10	
VII.B.TPC-63-BP2	Information Protection Processes and Procedures (IP)	Disabling unneeded software	Functional	Subset Of	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	10	
VII.B.TPC-63-BP3	Information Protection Processes and Procedures (IP)	Disabling unneeded services	Functional	Subset Of	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	10	
VII.B.TPC-63-BP4	Information Protection Processes and Procedures (IP)	Removing administrative access of users on workstations.	Functional	Subset Of	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	10	
VII.B.TPC-64	Information Protection Processes and Procedures (IP)	Third Party must establish and follow regular procedures for backup of critical systems and Saudi Aramco's data, software and websites.	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR)	10	
VII.B.TPC-64	Information Protection Processes and Procedures (IP)	Third Party must establish and follow regular procedures for backup of critical systems and Saudi Aramco's data, software and websites.	Functional	Intersects With	Data Backups	BCD-11	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfy Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	8	
VII.B.TPC-65	Information Protection Processes and Procedures (IP)	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.	Functional	Intersects With	Separate Storage for Critical Information	BCD-11.2	Mechanisms exist to store backup copies of critical software and other security-related information in a separate facility or in a fire-rated container that is not collocated with the system being backed up.	3	
VII.B.TPC-65	Information Protection Processes and Procedures (IP)	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.	Functional	Intersects With	Cryptographic Protection	BCD-11.4	Cryptographic mechanisms exist to prevent the unauthorized disclosure and/or modification of backup information.	8	
VII.B.TPC-66	Information Protection Processes and Procedures (IP)	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.	Functional	Intersects With	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	5	
VII.B.TPC-66	Information Protection Processes and Procedures (IP)	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.	Functional	Intersects With	System Media Sanitization	DCH-09	Mechanisms exist to sanitize system media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse.	5	
VII.B.TPC-67	Information Protection Processes and Procedures (IP)	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.	Functional	Intersects With	Business Continuity & Disaster Recovery (BC/DR) Plans	BCD-01.7	Mechanisms exist for process owners to establish and maintain formal Business Continuity & Disaster Recovery (BC/DR) plans to ensure information is detailed enough, accurate and representative of current operations in order to sustain and/or restore operations under adverse	5	
VII.B.TPC-68	Information Protection Processes and Procedures (IP)	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:	Functional	Intersects With	Business Continuity & Disaster Recovery (BC/DR) Plans	BCD-01.7	Mechanisms exist for process owners to establish and maintain formal Business Continuity & Disaster Recovery (BC/DR) plans to ensure information is detailed enough, accurate and representative of current operations in order to sustain and/or restore operations under adverse conditions.	5	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Saudi Arabia - SACS - 002 Third Party Cybersecurity Standard (2022)
Focal Document URL: https://www.aramco.com/-/media/downloads/working-with-us/ccc/sacs-002-third-party-cybersecurity-standard.pdf
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-sau-sacs-002-2022.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
VII.B.TPC-68(a)	Information Protection Processes and Procedures (IP)	Equipment failure.	Functional	Subset Of	Business Continuity & Disaster Recovery (BC/DR) Plans	BCD-01.7	Mechanisms exist for process owners to establish and maintain formal Business Continuity & Disaster Recovery (BC/DR) plans to ensure information is detailed enough, accurate and representative of current operations in order to sustain and/or restore operations under adverse conditions.	10	
VII.B.TPC-68(b)	Information Protection Processes and Procedures (IP)	Disruption of power supply or communication.	Functional	Subset Of	Business Continuity & Disaster Recovery (BC/DR) Plans	BCD-01.7	Mechanisms exist for process owners to establish and maintain formal Business Continuity & Disaster Recovery (BC/DR) plans to ensure information is detailed enough, accurate and representative of current operations in order to sustain and/or restore operations under adverse conditions.	10	
VII.B.TPC-68(c)	Information Protection Processes and Procedures (IP)	Application failure or corruption of database.	Functional	Subset Of	Business Continuity & Disaster Recovery (BC/DR) Plans	BCD-01.7	Mechanisms exist for process owners to establish and maintain formal Business Continuity & Disaster Recovery (BC/DR) plans to ensure information is detailed enough, accurate and representative of current operations in order to sustain and/or restore operations under adverse conditions.	10	
VII.B.TPC-68(d)	Information Protection Processes and Procedures (IP)	Human error, sabotage or strike.	Functional	Subset Of	Business Continuity & Disaster Recovery (BC/DR) Plans	BCD-01.7	Mechanisms exist for process owners to establish and maintain formal Business Continuity & Disaster Recovery (BC/DR) plans to ensure information is detailed enough, accurate and representative of current operations in order to sustain and/or restore operations under adverse conditions.	10	
VII.B.TPC-68(e)	Information Protection Processes and Procedures (IP)	Malicious Software attack.	Functional	Subset Of	Business Continuity & Disaster Recovery (BC/DR) Plans	BCD-01.7	Mechanisms exist for process owners to establish and maintain formal Business Continuity & Disaster Recovery (BC/DR) plans to ensure information is detailed enough, accurate and representative of current operations in order to sustain and/or restore operations under adverse conditions.	10	
VII.B.TPC-68(f)	Information Protection Processes and Procedures (IP)	Hacking or other Internet attacks.	Functional	Subset Of	Business Continuity & Disaster Recovery (BC/DR) Plans	BCD-01.7	Mechanisms exist for process owners to establish and maintain formal Business Continuity & Disaster Recovery (BC/DR) plans to ensure information is detailed enough, accurate and representative of current operations in order to sustain and/or restore operations under adverse conditions.	10	
VII.B.TPC-68(g)	Information Protection Processes and Procedures (IP)	Social unrest or terrorist attacks.	Functional	Subset Of	Business Continuity & Disaster Recovery (BC/DR) Plans	BCD-01.7	Mechanisms exist for process owners to establish and maintain formal Business Continuity & Disaster Recovery (BC/DR) plans to ensure information is detailed enough, accurate and representative of current operations in order to sustain and/or restore operations under adverse conditions.	10	
VII.B.TPC-68(h)	Information Protection Processes and Procedures (IP)	Environmental disasters.	Functional	Subset Of	Business Continuity & Disaster Recovery (BC/DR) Plans	BCD-01.7	Mechanisms exist for process owners to establish and maintain formal Business Continuity & Disaster Recovery (BC/DR) plans to ensure information is detailed enough, accurate and representative of current operations in order to sustain and/or restore operations under adverse conditions.	10	
VII.B.TPC-68(i)	Information Protection Processes and Procedures (IP)	Emergency contact information for personnel.	Functional	Subset Of	Business Continuity & Disaster Recovery (BC/DR) Plans	BCD-01.7	Mechanisms exist for process owners to establish and maintain formal Business Continuity & Disaster Recovery (BC/DR) plans to ensure information is detailed enough, accurate and representative of current operations in order to sustain and/or restore operations under adverse conditions.	10	
VII.B.TPC-69	Information Protection Processes and Procedures (IP)	Third Party must ensure that owners of the Business Continuity (BC) plan are identified and that the BC plan is reviewed and updated annually.	Functional	Intersects With	Business Continuity & Disaster Recovery (BC/DR) Plans	BCD-01.7	Mechanisms exist for process owners to establish and maintain formal Business Continuity & Disaster Recovery (BC/DR) plans to ensure information is detailed enough, accurate and representative of current operations in order to sustain and/or restore operations under adverse conditions.	5	
VII.B.TPC-69	Information Protection Processes and Procedures (IP)	Third Party must ensure that owners of the Business Continuity (BC) plan are identified and that the BC plan is reviewed and updated annually.	Functional	Intersects With	Commitment To Continual Improvements	GOV-01.3	Mechanisms exist to commit appropriate resources needed for continual improvement of the organization's Security, Compliance & Resilience Program (SCRP), including: (1) Staffing; (2) Budget;	3	
VII.B.TPC-70	Information Protection Processes and Procedures (IP)	Third Party must conduct Business Continuity drills at least annually.	Functional	Intersects With	Contingency Plan Testing & Exercises	BCD-04	Mechanisms exist to conduct tests and/or exercises to evaluate the contingency plan's effectiveness and the organization's readiness to execute the plan.	5	
VII.B.TPC-71	Information Protection Processes and Procedures (IP)	Third Party must have formal procedures for on-boarding employees. On-boarding procedures must include background checks (e.g. Verification of work histories).	Functional	Intersects With	Onboarding, Transferring & Offboarding Personnel	HRS-01.1	Mechanisms exist to proactively govern the following personnel management actions: (1) Onboarding new personnel (e.g., new hires);	5	
VII.B.TPC-72	Information Protection Processes and Procedures (IP)	Third Party must conduct security and sourcecode vulnerability scanning on all developed applications, and close all discovered vulnerabilities before deployment in production.	Functional	Intersects With	Specialized Assessments	IAO-02.2	Mechanisms exist to conduct specialized assessments for: (1) Statutory, regulatory and contractual compliance obligations; (2) Monitoring capabilities; (3) Mobile devices; (4) Databases; (5) Application security;	5	
VII.B.TPC-72	Information Protection Processes and Procedures (IP)	Third Party must conduct security and sourcecode vulnerability scanning on all developed applications, and close all discovered vulnerabilities before deployment in production.	Functional	Intersects With	Threat Analysis & Flaw Remediation During Development	IAO-04	Mechanisms exist to require system developers and integrators to create and execute a Security Testing and Evaluation (ST&E) plan, or similar process, to identify and remediate flaws during development.	5	
VII.B.TPC-72	Information Protection Processes and Procedures (IP)	Third Party must conduct security and sourcecode vulnerability scanning on all developed applications, and close all discovered vulnerabilities before deployment in production.	Functional	Intersects With	Technical Verification	IAO-06	Mechanisms exist to perform Information Assurance Program (IAP) activities to evaluate the design, implementation and effectiveness of technical security, compliance and resilience controls.	5	
VII.B.TPC-72	Information Protection Processes and Procedures (IP)	Third Party must conduct security and sourcecode vulnerability scanning on all developed applications, and close all discovered vulnerabilities before deployment in production.	Functional	Intersects With	Security Authorization	IAO-07	Mechanisms exist to ensure Technology Assets, Applications and/or Services (TAAS) are officially authorized prior to "go live" in a production environment.	5	
VII.B.TPC-73	Information Protection Processes and Procedures (IP)	All changes to the application must be properly authorized and tested in a testing environment before moving to production.	Functional	Intersects With	Technical Verification	IAO-06	Mechanisms exist to perform Information Assurance Program (IAP) activities to evaluate the design, implementation and effectiveness of technical security, compliance and resilience controls.	5	
VII.B.TPC-73	Information Protection Processes and Procedures (IP)	All changes to the application must be properly authorized and tested in a testing environment before moving to production.	Functional	Intersects With	Security Authorization	IAO-07	Mechanisms exist to ensure Technology Assets, Applications and/or Services (TAAS) are officially authorized prior to "go live" in a production environment.	5	
VII.B.TPC-74	Information Protection Processes and Procedures (IP)	Third Party must have a process for secure system and software development life cycle in alignment with industry best practice.	Functional	Intersects With	Secure Software Development Practices (SSDP)	TDA-06	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	5	
VII.B.TPC-75	Protective Technology (PT)	Third Party must retain all audit logs from information systems and applications storing, processing or transmitting Saudi Aramco data for one (1) year.	Functional	Intersects With	Event Log Retention	MON-10	Mechanisms exist to retain event logs for a time period consistent with records retention requirements to provide support for after-the-fact investigations of security incidents and to meet statutory, regulatory	5	
VII.B.TPC-76	Protective Technology (PT)	Firewalls must be implemented at the network perimeter and only required services must be allowed. Vulnerable services or insecure protocols should be blocked.	Functional	Subset Of	Boundary Protection	NET-03	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.	10	
VII.B.TPC-77	Protective Technology (PT)	Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS) must be implemented at the network perimeter.	Functional	Intersects With	Network Intrusion Detection / Prevention Systems (NIDS / NIPS)	NET-08	Mechanisms exist to employ Network Intrusion Detection / Prevention Systems (NIDS/NIPS) to detect and/or prevent intrusions into the network.	5	
VII.B.TPC-78	Protective Technology (PT)	Signatures of firewalls, IDS and IPS must be upto-date.	Functional	Intersects With	Update Tool Capability	VPM-06.1	Mechanisms exist to update vulnerability scanning tools.	5	
VII.B.TPC-79	Protective Technology (PT)	If Third Party is hosting an application or a website for Saudi Aramco or providing cloudbased web application, Web Application Firewall (WAF)	Functional	Intersects With	Web Application Firewall (WAF)	WEB-03	Mechanisms exist to deploy Web Application Firewalls (WAFs) to provide defense-in-depth protection for application-specific threats.	5	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Saudi Arabia - SACS - 002 Third Party Cybersecurity Standard (2022)
Focal Document URL: https://www.aramco.com/-/media/downloads/working-with-us/ccc/sacs-002-third-party-cybersecurity-standard.pdf
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-sau-sacs-002-2022.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
VII.B.TPC-80	Anomalies and Events (AE)	Third Party must monitor Technology Assets, Systems and applications to identify unauthorized access, or unauthorized activity.	Functional	Intersects With	Anomalous Behavior	MON-16	Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.	5	
VII.B.TPC-80	Anomalies and Events (AE)	Third Party must monitor Technology Assets, Systems and applications to identify unauthorized access, or unauthorized activity.	Functional	Intersects With	Monitoring for Indicators of Compromise (IOC)	MON-11.3	Automated mechanisms exist to identify and alert on Indicators of Compromise (IoC).	5	
VII.B.TPC-80	Anomalies and Events (AE)	Third Party must monitor Technology Assets, Systems and applications to identify unauthorized access, or unauthorized activity.	Functional	Intersects With	Indicators of Compromise (IOC)	IRO-03	Mechanisms exist to define specific Indicators of Compromise (IOC) to identify the signs of potential cybersecurity events.	5	
VII.B.TPC-81	Anomalies and Events (AE)	Third Party must periodically aggregate and correlate data from multiple systems and critical applications such as Firewalls, IDS/IPS, and anti-virus	Functional	Intersects With	Correlate Monitoring Information	MON-02.1	Automated mechanisms exist to correlate both technical and non-technical information from across the enterprise by a Security Incident	5	
VII.B.TPC-82	Continuous Monitoring (CM)	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.	Functional	Intersects With	Physical Access Control	PES-03	Physical access control mechanisms exist to enforce physical access authorizations for all physical access points (including designated entry/exit points) to facilities (excluding those areas within the facility officially designated as publicly accessible).	5	
VII.B.TPC-83	Continuous Monitoring (CM)	Privileged accounts activity must be logged and monitored on a regular basis.	Functional	Intersects With	Privileged User Oversight	MON-01.15	Mechanisms exist to implement enhanced activity monitoring for privileged users.	5	
VII.B.TPC-84	Continuous Monitoring (CM)	Non-authorized devices (such as personal devices and mobile phones) must not be used to store, process or access Assets.	Functional	Intersects With	Use of Mobile Devices	HRS-05.5	Mechanisms exist to manage business risks associated with permitting mobile device access to organizational resources.	5	
VII.B.TPC-84	Continuous Monitoring (CM)	Non-authorized devices (such as personal devices and mobile phones) must not be used to store, process or access Assets.	Functional	Intersects With	Personally-Owned Mobile Devices	MDM-06	Mechanisms exist to restrict the connection of personally-owned, mobile devices to organizational Technology Assets, Applications	5	
VII.B.TPC-85	Continuous Monitoring (CM)	Monthly Vulnerability scans must be conducted to evaluate configuration, Patches and services for known Vulnerabilities.	Functional	Intersects With	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	5	
VII.B.TPC-86	Continuous Monitoring (CM)	Physical access to the facility where information systems reside must be restricted to authorized personnel and reviewed on a regular basis.	Functional	Intersects With	Physical Access Authorizations	PES-02	Physical access control mechanisms exist to maintain a current list of personnel with authorized access to organizational facilities (except for	5	
VII.B.TPC-86	Continuous Monitoring (CM)	Physical access to the facility where information systems reside must be restricted to authorized personnel and reviewed on a regular basis.	Functional	Intersects With	Role-Based Physical Access	PES-02.1	Physical access control mechanisms exist to authorize physical access to facilities based on the position or role of the individual.	5	
VII.B.TPC-87	Continuous Monitoring (CM)	Information systems and applications must log auditable events as stated in Appendix C.	Functional	Intersects With	Content of Event Logs	MON-03	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to produce event logs that contain sufficient	5	
VII.B.TPC-88	Communications (CO)	Incident management policy and plan must be documented, maintained and communicated to management and appropriate team members.	Functional	Intersects With	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	5	
VII.B.TPC-89	Communications (CO)	Third Party must have an Incident Response capability that includes preparation, detection and analysis, containment, eradication, recovery, documentation and preservation of evidence, communication protocols	Functional	Intersects With	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake;	5	
VII.B.TPC-89	Communications (CO)	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.	Functional	Intersects With	Root Cause Analysis (RCA) & Lessons Learned	IRO-13	Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity and data protection incidents to reduce the likelihood or impact of future incidents.	5	
VII.B.TPC-90	Communications (CO)	Third Party must track, classify and document all Cybersecurity Incidents.	Functional	Intersects With	Situational Awareness For Incidents	IRO-09	Mechanisms exist to document, monitor and report the status of cybersecurity and data protection incidents to internal stakeholders all the way through the resolution of the incident.	5	
VII.B.TPC-91	Communications (CO)	Third Party must resolve or mitigate the identified security Vulnerabilities on a system, computer, network, or other computer equipment within the following timeframes:	Functional	Intersects With	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	5	
VII.B.TPC-91-BP1	Communications (CO)	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.	Functional	Subset Of	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	10	
VII.B.TPC-91-BP2	Communications (CO)	High Risk: within one (1) month of vendor patch release, or discovered security breach whichever is earlier.	Functional	Subset Of	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	10	
VII.B.TPC-91-BP3	Communications (CO)	Medium and Low Risk: within three (3) months of discovery.	Functional	Subset Of	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	10	
VII.B.TPC-92	Communications (CO)	If Third Party is hosting a website for Saudi Aramco or providing a Cloud Computing Service, the website / Cloud Computing Service must be	Functional	Intersects With	Resource Priority	CAP-02	Mechanisms exist to control resource utilization of Technology Assets, Applications and/or Services (TAAS) that are susceptible to Denial of	5	
VIII	Reference	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
IX	Approval	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	