

Saudi Arabian Cloud Security Controls Standard SACS-002

SACS-002 defines cloud security controls to protect cloud services and data and ensure compliance with Saudi Arabian regulations.



What it is

Saudi Arabia SACS-002 — Saudi Arabian Cloud Security Controls Standard is a national cybersecurity framework that helps organizations establish and maintain security controls for cloud computing environments. Its primary purpose is to safeguard cloud-hosted data and services, ensuring resilience against cyber threats while supporting compliance with regulatory requirements.

Issued by the Saudi National Cybersecurity Authority (NCA), SACS-002 applies to public and private sector entities that provide or utilize cloud services within Saudi Arabia. The standard covers a broad range of areas including risk management, data protection, access control, incident response, and monitoring, aligning with both local regulations and leading international security best practices.

At a glance

PUBLISHER Saudi Aramco	TYPE Standard	VERSION February 2022
EFFECTIVE February 2022	DOMAIN Cloud Security	FAMILY CSA STAR
REGION Saudi Arabia	INDUSTRY Cloud & Technology Providers	ADOPTION MODEL Regulatory Compliance
IMPLEMENTATION COMPLEXITY High		

Source: <https://www.aramco.com/en/what-we-do/suppliers/supplier-resources/cybersecurity-compliance-certificate-program>

Why it matters

- **Strengthen security governance** Establishes clear accountability and oversight structures for cloud security, ensuring leadership engagement and effective management of controls.
- **Enhance regulatory alignment** Facilitates adherence to national cloud compliance requirements, supporting organizations in fulfilling Saudi regulatory and legal obligations.
- **Improve service availability** Reduces risks associated with cloud outages by requiring robust business continuity and disaster recovery planning across environments.
- **Increase audit readiness** Standardizes security documentation and reporting practices, streamlining preparations for internal and external audits.

How SmartSuite supports SACS-002

Cloud Control Framework Library

Structure SACS control domains covering cloud infrastructure, data protection, and service governance.

Cloud Service and Environment Tracking

Track cloud services, environments, and data flows across providers and systems.

Risk Assessment and Control Implementation

Link cloud risks to controls and manage mitigation across cloud deployments.

Cloud Authentication and Access Management

Manage authentication, permissions, and secure configurations across cloud environments.

Monitoring, Logging, and Incident Response

Track cloud security events and manage detection and response workflows.

Cloud Control and Regulatory Readiness Reporting

Provide dashboards showing cloud control coverage, risk posture, and regulatory readiness.

Common framework mappings

CIS Controls v8.1

GDPR

ISO 27001:2022

ISO 27017

ISO 27018

NIST CSF 2.0

NIST 800-53 Rev.5

PCI DSS 4.0.1

SOC 2

Official resources

SACS-002 Third-Party Cybersecurity Standard

Defines the full set of mandatory cybersecurity controls third parties must implement.

aramco.com/en/what-we-do/suppliers/supplier-resources/cybersecurity-compliance-certificate-program

Third-Party Cybersecurity Controls Guideline

Provides implementation guidance supporting the SACS-002 standard controls for vendors.

aramco.com/en/what-we-do/suppliers/supplier-resources/cybersecurity-compliance-certificate-program

Frequently asked questions

What is Saudi Arabia SACS-002 used for?

Saudi Arabia SACS-002 provides mandatory cloud security controls for entities that offer or consume cloud services within the Kingdom of Saudi Arabia. It aims to ensure the confidentiality, integrity, and availability of data processed or stored in the cloud, especially for government entities and organizations handling sensitive information.

Is SACS-002 a mandatory requirement in Saudi Arabia?

Yes, SACS-002 is mandatory for government agencies, their affiliated organizations, and entities that process, store, or transmit government data using cloud environments in Saudi Arabia. Compliance is essential to obtain authorization to deliver or utilize cloud services within the country.

What is the scope of SACS-002 and who must comply?

The scope of SACS-002 covers all cloud service providers operating in Saudi Arabia, as well as organizations (public or private) that use cloud solutions to process governmental or regulated data. It applies to IaaS, PaaS, and SaaS models, and organizations must ensure that both technical and organizational measures are in place.

What are the key security controls required by SACS-002?

SACS-002 outlines technical and administrative controls across domains such as data protection, access management, incident response, compliance monitoring, and business continuity. Organizations must implement controls like encryption, secure configuration, identity management, and regular security audits.

How do organizations implement SACS-002 requirements?

Implementation involves conducting a risk assessment, mapping SACS-002 controls to internal processes, and maintaining documentation for governance and technical measures. Continuous monitoring, employee training, and periodic audits are also required to maintain compliance.

How does SACS-002 relate to other international cloud security standards?

SACS-002 incorporates global standards such as ISO/IEC 27017 and 27018 but includes additional requirements relevant to local regulatory and cultural context in Saudi Arabia. Organizations already certified in international frameworks must map and extend their controls to address unique SACS-002 provisions.

What are the ongoing compliance requirements for SACS-002?

Ongoing compliance includes regular control assessments, evidence collection, incident reporting, and responding to government or regulator audits. Organizations must maintain up-to-date documentation and remediate any identified findings or deficiencies in a timely manner.

How would SmartSuite support Saudi Arabia SACS-002?

SmartSuite enables organizations to efficiently manage SACS-002 compliance by tracking risks, mapping and monitoring required controls, collecting and organizing evidence, and maintaining audit readiness. Its reporting features support the generation of compliance status updates and executive summaries to facilitate regulatory communication and continuous improvement.

License included / downloadable: Yes The Saudi Arabian Cloud Security Controls Standard (SACS-002) is published by the Saudi National Cybersecurity Authority (NCA) and is publicly available for download from the NCA website. License included with platform

Full framework page and mappings: smartsuite.com/frameworks/saudi-arabia-cloud-security-controls-standard-sacs-002