

Saudi Arabia CSCC-1:2019

CSCC-1:2019 defines essential cybersecurity controls to protect Saudi Arabian organizations' information systems and improve baseline security practices.



What it is

Saudi Arabia CSCC-1:2019 — Essential Cybersecurity Controls is a national cybersecurity framework that establishes baseline security controls for organizations operating in Saudi Arabia. The framework aims to support effective risk management, protect critical information assets, and ensure compliance with regulatory requirements across public and private sectors.

Published by the National Cybersecurity Authority (NCA) of Saudi Arabia, CSCC-1:2019 is mandated for government entities and encouraged for organizations that handle sensitive or critical infrastructure. The framework covers key areas such as access control, data protection, incident response, business continuity, compliance oversight, and third-party risk management, aligning with recognized international standards.

At a glance

PUBLISHER National Cybersecurity Authority (NCA)	TYPE Control Framework	VERSION 2019
EFFECTIVE 18 December 2019	DOMAIN Cybersecurity	FAMILY Other
REGION Saudi Arabia	ADOPTION MODEL Regulatory Compliance	IMPLEMENTATION COMPLEXITY High

Source: <https://nca.gov.sa/en/regulatory-documents/csccl/>

Why it matters

- **Strengthen cybersecurity governance** Establish clear accountability for cybersecurity practices, ensuring leadership support and alignment with organizational risk management objectives.
- **Enable regulatory compliance** Support organizations in meeting Saudi national cybersecurity requirements, minimizing legal and regulatory risks through well-defined controls.
- **Enhance incident detection capabilities** Improve the ability to identify, respond to, and recover from cybersecurity incidents through systematic monitoring and response processes.
- **Promote operational resilience** Reduce downtime from cyber threats by ensuring continuity plans, asset management, and proactive vulnerability management across all systems.

How SmartSuite supports CCCC-1:2019

NCA Control Framework Library

Structure CCCC domains and sub-controls with ownership, scope, and implementation status.

Risk Assessment and Control Mapping

Link cybersecurity risks to CCCC controls to prioritize remediation and reduce exposure.

Policy and Governance Management

Centralize cybersecurity policies, standards, and approvals aligned to NCA requirements.

Identity, Authentication, and Operations Management

Manage identity, authentication, monitoring, and operational controls across systems.

Incident Response and Threat Management

Track incidents, response actions, and threat intelligence aligned to CCCC expectations.

NCA Compliance Monitoring and Audit Reporting

Provide dashboards showing control coverage, gaps, and readiness for NCA audits.

Common framework mappings

CIS Controls v8.1

COBIT 2019

GDPR

ISO 27001:2022

ISO 27017

NIST CSF 2.0

NIST 800-53 Rev.5

PCI DSS 4.0.1

SOC 2

Official resources

Critical Systems Cybersecurity Controls (CCCC-1:2019)

Defines the mandatory controls—32 main and 73 subcontrols—for protecting Saudi Arabia’s critical systems.

<cdn.nca.gov.sa/ar/cccc-en.pdf>

CCCC-1:2019 Implementation Guide

Provides practical guidance for national entities to apply and comply with CCCC-1:2019 requirements.

backend.nca.gov.sa/api/public/cms/files/0956104f-2ea1-4ed0-9934-7be6e1ed8861_CCCC_Implementation_Guidelines_en-.pdf

Frequently asked questions

What is the Saudi Arabia CCCC-1:2019 used for?

The Saudi Arabia CCCC-1:2019 establishes a baseline set of essential cybersecurity controls for organizations operating in Saudi Arabia. It aims to improve national cybersecurity resilience by providing structured requirements for protecting information assets, systems, and networks against emerging threats.

Is compliance with CCCC-1:2019 mandatory?

Yes, compliance with CCCC-1:2019 is mandatory for government entities and organizations providing critical national infrastructure in Saudi Arabia. The National Cybersecurity Authority (NCA) enforces adherence to these controls, and non-compliance can result in regulatory penalties.

What organizations are required to implement CCCC-1:2019?

CCCC-1:2019 applies to all government entities, as well as companies and service providers that manage or operate critical infrastructure within Saudi Arabia. Organizations in sectors such as energy, healthcare, finance, and telecommunications are typically within its scope.

What are the key control domains within CCCC-1:2019?

CCCC-1:2019 consists of 114 controls organized into 5 main domains: cybersecurity governance, operational management, asset management, risk management, and compliance. Each domain covers specific requirements such as access control, incident response, data protection, and periodic risk assessments.

How do organizations implement the controls of CSCC-1:2019?

Organizations should start with a gap analysis to identify deficiencies relative to the CSCC-1:2019 controls, followed by developing and implementing remediation plans. Documented policies, regular risk assessments, technical safeguards, and continuous monitoring are key to successful implementation.

How does CSCC-1:2019 relate to other cybersecurity frameworks?

CSCC-1:2019 is aligned with internationally recognized frameworks such as ISO 27001, NIST Cybersecurity Framework, and CIS Controls, but it incorporates local regulatory and national security requirements specific to Saudi Arabia. Many controls can be mapped across these frameworks to streamline compliance efforts.

What ongoing activities are required to maintain CSCC-1:2019 compliance?

Maintaining compliance involves regular review and updates of cybersecurity policies, recurring risk assessments, continuous monitoring of controls, user awareness training, and periodic audits. Organizations must also prepare for NCA inspections and submit required evidence of control effectiveness.

How would SmartSuite support Saudi Arabia CSCC-1:2019?

SmartSuite can help organizations manage CSCC-1:2019 compliance through centralized risk tracking, automated control management workflows, evidence collection modules, and readiness assessments. The platform also supports audit preparation and real-time compliance reporting, streamlining the ongoing management and demonstration of adherence to CSCC-1:2019.

License included / downloadable: Yes Saudi National Cybersecurity Authority (NCA) publishes CSCC-1:2019 and the Essential Cybersecurity Controls are available for free from the NCA official website. License included with platform

Full framework page and mappings: smartsuite.com/frameworks/saudi-arabia-cscc-1-2019-essential-cybersecurity-controls