SmartSuite

Framework / Cybersecurity / Other

Saudi Arabia CSCC-1:2019

CSCC-1:2019 is the NCA's Critical Systems Cybersecurity Controls: 32 main controls and 73 subcontrols added to the ECC for the systems Saudi organizations identify as critical.



What it is

The Critical Systems Cybersecurity Controls (CSCC-1:2019) are the National Cybersecurity Authority's minimum cybersecurity requirements for the systems a Saudi organization identifies as critical, issued in 2019 as an extension to the Essential Cybersecurity Controls ; any organization that owns or operates a critical system, whether a government body in the Kingdom or abroad, a government subsidiary or a private organization, must comply, and continuous compliance with the ECC is a prerequisite for compliance with the CSCC (Introduction; Scope of Work). The document adds 4 main domains, 21 subdomains, 32 main controls and 73 subcontrols on top of the ECC, each one written as an addition to a named ECC subdomain or control.

At a glance

PUBLISHER National Cybersecurity Authority (NCA)	TYPE Control Framework	VERSION CSCC-1:2019
EFFECTIVE 2019	DOMAIN Cybersecurity	FAMILY Other
REGION Saudi Arabia	ADOPTION MODEL Regulatory Compliance	IMPLEMENTATION COMPLEXITY High

Source: nca.gov.sa/en/regulatory-documents/controls-list/cscc/

Why it matters

- **Hard frequencies replace open-ended review** Risk assessment at least annually and risk register review at least monthly (1-2-1-1, 1-2-1-2); access rights reviewed every three months (2-2-2); configuration and hardening review every six months (2-3-1-6); vulnerability assessments monthly (2-9-2); penetration tests every six months (2-10-2); backup recovery tests every three months (2-8-2).
- **Remote access and identity are locked down** Remote access from outside the Kingdom is prohibited and access from inside must be verified by the security operations center and monitored (2-2-1-1, 2-2-1-2); multi-factor authentication applies to all users (2-2-1-3); direct database access is limited to database administrators (2-2-1-8); privileged accounts work from isolated management-network workstations (2-3-1-4).
- **Networks are isolated by default** Critical systems' networks are segregated (2-4-1-1), may not connect to wireless networks (2-4-1-4), may not connect to the internet where they serve internal needs (2-4-1-6), use whitelist-only firewall rules (2-4-1-9) and must be protected against APT and DDoS attacks (2-4-1-5, 2-4-1-8).
- **Data stays in production and in the Kingdom** Production data may not be used in other environments without masking or scrambling (2-6-1-1) and may not be transferred out of production (2-6-1-5); data in transit and at rest is encrypted (2-7-1-1, 2-7-1-2); hosting must be inside the organization or with government or Saudi cloud providers that comply with the NCA Cloud Cybersecurity Controls (4-2-1-1).

 © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports CSCC-1:2019

Critical Systems Identification Register

Score each candidate system against the seven identification criteria, record the decision and its approval, and keep the Components of Critical Systems list for every system found critical.

CSCC on Top of ECC Library

Hold each CSCC control as a record linked to the ECC subdomain or control it extends, so that evidence for ECC 2-2-3 and CSCC 2-2-1 sits together and the Appendix (A) relationship is visible.

Frequency Calendar

Schedule the recurring obligations the CSCC fixes: monthly risk register review and vulnerability assessment, quarterly access review and backup recovery test, six-monthly hardening review and penetration test, annual risk assessment and disaster recovery test.

Remote Access and Hosting Exceptions

Use Cyber & IT Risk to log any temporary mobile device access (2-5-1-1), in-Kingdom remote access approvals (2-2-1-2) and hosting decisions under 4-2-1-1 with the approver and expiry date.

Third-Party Vetting Evidence

Use Third Party Risk Management to record the screening of outsourcing and managed service companies and personnel (4-1-1-1) and the Saudi-company requirement of 4-1-1-2 for each critical system contract.

NCA Self-Assessment and Audit Pack

Assemble the self-assessment the NCA may request with the 1-4-1 annual review and 1-4-2 independent review results, open findings and remediation plans in Internal Audit Management.

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 (CSCC-1:2019)

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

cdn.nca.gov.sa/ar/cscc-en.pdf

CSCC-1:2019 Implementation Guide

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

cdn.nca.gov.sa/api/public/cms/files/0956104f-2ea1-4ed0-9934-7be6e1ed8861_CSCC_Implementation_Guidelines_en-.pdf

Frequently asked questions

What counts as a critical system under CSCC-1:2019?

Any system or network whose failure, unauthorized change, or unauthorized access to it or its data may harm the availability of the organization's business and services or cause economic, financial, security or social harm at the national level (Critical Systems Definition). The document gives seven identification criteria: harm to national security, harm to the Kingdom's reputation, financial losses above 0.01% of GDP, harm to services used by more than 5% of the population, loss of lives, unauthorized disclosure of Top Secret or Secret data, and harm to the operations of a vital sector. The organization that owns or operates the system makes the identification.

How does the CSCC relate to the ECC?

The CSCC is an extension and complement to the Essential Cybersecurity Controls, and continuous ECC compliance is a prerequisite for CSCC compliance (Introduction). Its controls are written as additions to named ECC subdomains and controls, and Appendix (A) shows that the CSCC adds one new subdomain (2-13 Application Security), adds controls to twenty ECC subdomains and adds none to nine. The text cross-references ECC-1:2018 numbering; the NCA has since issued ECC-2:2024.

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

Which recurring frequencies does the CSCC set?

Annual risk assessment and monthly risk register review (1-2-1-1, 1-2-1-2); annual CSCC implementation review by the cybersecurity function and an independent review every three years (1-4-1, 1-4-2); access rights review every three months (2-2-2); patches within one month for internet-connected and three months for internal critical systems (2-3-1-3, 2-9-1-2); hardening review every six months (2-3-1-6); monthly vulnerability assessments (2-9-2); penetration tests every six months (2-10-2); backup recovery tests every three months (2-8-2); annual disaster recovery plan tests (3-1-1-3); and event log retention of at least 18 months (2-11-2).

Can critical systems be hosted in the cloud or accessed remotely?

Hosting of critical systems and any of their technical components must be inside the organization or with cloud services provided by government organizations or Saudi companies that comply with the NCA Cloud Cybersecurity Controls, taking the classification of the hosted data into account (4-2-1-1). Remote access from outside the Kingdom is prohibited; remote access from inside the Kingdom must be restricted, verified by the security operations center and continuously monitored (2-2-1-1, 2-2-1-2). Access from mobile devices is allowed only temporarily after a risk assessment and approval by the cybersecurity function (2-5-1-1).

How does the NCA check compliance with the CSCC?

Implementation and Compliance requires organizations to identify their critical systems, implement the controls within the compliance period the NCA defines while managing the risks in the meantime, and keep complying afterwards. The NCA evaluates compliance through self-assessments by the organizations and on-site audits, under the mechanisms it considers appropriate, on the authority of item 3 of Article 10 of the NCA mandate and Royal Decrees 57231 of 10/11/1439H and 7732 of 12/2/1440H.

License included / downloadable: Yes The National Cybersecurity Authority publishes the CSCC-1:2019 PDF as an open document (Document Classification: Open, Sharing Indicator: White) on its regulatory documents page; the Arabic version is the binding text.

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