SmartSuite

Framework / Cybersecurity / Other

Saudi OTCC-1:2022

OTCC-1:2022 defines cybersecurity controls to protect operational technology systems and critical industrial infrastructure in Saudi Arabia.

What it is

Saudi Arabia OTCC-1:2022 — Operational Technology Cybersecurity Controls is a national cybersecurity framework that guides organizations in securing operational technology (OT) environments and protecting critical infrastructure against cyber threats. The framework outlines minimum cybersecurity requirements to reduce risks associated with OT systems in sectors such as energy, utilities, manufacturing, and transportation.

Published by the Saudi National Cybersecurity Authority (NCA), OTCC-1:2022 is used by operators of essential services and critical infrastructure providers in Saudi Arabia. The framework covers areas including security controls implementation, risk management processes, access control, incident response, and monitoring for operational technology networks.

At a glance

PUBLISHER National Cybersecurity Authority (NCA)	TYPE Control Framework	VERSION 2022
EFFECTIVE 07 April 2022	DOMAIN Cybersecurity	FAMILY Other
REGION Saudi Arabia	INDUSTRY Energy & Utilities	ADOPTION MODEL Regulatory Compliance
IMPLEMENTATION COMPLEXITY High		

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

Why it matters

- **Strengthen OT cybersecurity governance** Establishes defined roles, responsibilities, and policies to improve oversight of OT cybersecurity efforts across the organization.
- **Promote operational resilience** Ensures organizations can anticipate, withstand, and quickly recover from disruptions to OT environments and essential industrial processes.
- **Enhance regulatory alignment** Supports compliance with Saudi national requirements and industry-specific mandates, improving readiness for regulatory audits and inspections.
- **Improve incident detection capabilities** Enables earlier identification and response to cyber threats within OT systems, reducing potential impact on operations and safety.

Updated Sep 26, 2026 · © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports OTCC-1:2022

OT Control Framework Library

Structure OTCC control domains covering industrial systems, networks, and operational processes.

Asset Inventory and OT Environment Mapping

Track industrial assets, control systems, and network zones across OT environments.

OT Risk and Control Mitigation

Link OT risks to controls and manage mitigation across critical infrastructure systems.

OT Identity and Segmentation Controls

Manage identity, privileged access, and segmentation between IT and OT environments.

Monitoring, Detection, and Incident Response

Track OT security events, anomalies, and coordinated response activities across operations.

OT Control and Regulatory Readiness Reporting

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

Common framework mappings

CIS Controls v8.1 | ISO 27001:2022 | ISO 27002:2022 | NERC CIP | NIST CSF 2.0 | NIST 800-53 Rev.5 | PCI DSS 4.0.1 | SOC 2

Official resources

Operational Technology Cybersecurity Controls (OTCC-1:2022)

Defines the minimum cybersecurity requirements for operational technology and industrial control systems.

nca.gov.sa/en/regulatory-documents/controls-list/otcc

Operational Technology Cybersecurity Controls Methodology and Mapping Annex (OTCC-1:2022)

Provides methodology and mapping details aligning OTCC-1:2022 with related standards and frameworks.

cdn.nca.gov.sa/api/public/cms/files/071d52fc-014b-4f15-84ce-1289f3f5c3a9_Operational-Technology-Cybersecurity-Controls-Methodology-and-Mapping-Annex.pdf

Frequently asked questions

What is Saudi Arabia OTCC-1:2022 used for?

Saudi Arabia OTCC-1:2022 establishes national requirements for cybersecurity controls in operational technology (OT) environments, such as those found in critical infrastructure sectors. The framework provides a baseline to help organizations identify, protect, detect, respond to, and recover from cyber threats targeting industrial control systems.

Is compliance with Saudi Arabia OTCC-1:2022 mandatory?

Yes, OTCC-1:2022 is mandated by the Saudi National Cybersecurity Authority (NCA) for organizations operating critical national infrastructure in Saudi Arabia. Non-compliance may result in legal and regulatory consequences, making adherence essential for organizations in the covered sectors.

What is the scope of Saudi Arabia OTCC-1:2022?

The scope of OTCC-1:2022 applies to entities operating or managing operational technology environments within critical infrastructure sectors, including energy, water, transportation, and others designated by the NCA. It covers all OT assets, systems, networks, and associated personnel under the organization's control.

What are the key concepts or required artifacts in OTCC-1:2022?

Key concepts in OTCC-1:2022 include the identification of OT assets, risk assessment, implementation of specified technical and organizational controls, and the management of OT-specific incidents. Required artifacts typically involve documented policies, asset inventories, risk assessments, control implementation records, and incident response procedures.

Updated Sep 26, 2026 · © 2026 SmartSuite Inc. All rights reserved.

How should organizations implement Saudi Arabia OTCC-1:2022 controls?

Organizations should begin with a gap assessment against the control requirements, define the OT environment scope, and establish project plans to remediate identified deficiencies. Implementation involves applying technical safeguards, training OT staff, documenting processes, and regularly reviewing compliance as part of a continuous improvement cycle.

How does OTCC-1:2022 relate to other cybersecurity frameworks?

OTCC-1:2022 aligns with international standards such as IEC 62443 and NIST SP 800-82, but is tailored to the Saudi regulatory and threat environment. Organizations may leverage existing controls from other frameworks as foundational elements but must ensure specific OTCC-1:2022 requirements are met.

What are the ongoing compliance requirements for OTCC-1:2022?

Ongoing compliance requires periodic risk assessments, regular audits, continuous monitoring of OT systems, incident response testing, and maintenance of evidence documentation. Organizations must also stay updated on any OTCC-1:2022 updates issued by the NCA and adjust controls accordingly.

How would SmartSuite support Saudi Arabia OTCC-1:2022?

SmartSuite helps organizations manage OTCC-1:2022 compliance by enabling risk tracking, centralizing control management, and simplifying evidence collection. The platform supports audit readiness with automated workflows and dashboards, while comprehensive reporting features provide real-time oversight of control status and regulatory alignment.

License included / downloadable: Yes The National Cybersecurity Authority (NCA) of Saudi Arabia publishes OTCC-1:2022 and the official document is freely available on the NCA website. License included with platform

Full framework page and mappings: smartsuite.com/frameworks/saudi-arabia-otcc-1-2022-operational-technology-cybersecurity-controls