SmartSuite

Framework / Cybersecurity / Other

Saudi OTCC-1:2022

OTCC-1:2022 is the NCA's Operational Technology Cybersecurity Controls: 47 controls and 122 subcontrols at three facility levels for industrial control systems in critical facilities.



What it is

The Operational Technology Cybersecurity Controls (OTCC-1:2022) are the National Cybersecurity Authority's cybersecurity requirements for industrial control systems in critical facilities. They were issued in 2022 for government organizations and for private sector organizations that own, operate or host Critical National Infrastructures, in the Kingdom or abroad. They are implemented as an extension to the Essential Cybersecurity Controls , and compliance with the ECC is a mandatory prerequisite (Executive Summary; Implementation and Compliance). The document contains 4 main domains, 23 subdomains, 47 main controls and 122 subcontrols (Introduction), and the term industrial control systems covers all devices, systems or networks used to operate or automate industrial processes.

At a glance

PUBLISHER National Cybersecurity Authority (NCA)	TYPE Control Framework	VERSION OTCC-1:2022
EFFECTIVE 2022	DOMAIN Cybersecurity	FAMILY Other
REGION Saudi Arabia	INDUSTRY Critical Infrastructure	ADOPTION MODEL Regulatory Compliance
IMPLEMENTATION COMPLEXITY High		

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

Why it matters

- **Safety systems are treated as crown jewels** Safety Instrumented Systems controllers must stay in modes that prevent unauthorized changes (2-3-1-5), must be segmented from other OT networks (2-4-1-3), and physical access to them is strictly limited (2-13-1-5); qualitative cyber risk analysis joins the Process Hazard Analysis for any change in plant operations (1-3-1-5).
- **Zones, choke points and a DMZ jump host** The OT environment is segmented from other networks (2-4-1-1), zones inside it are segmented by level with traffic directed to choke points (2-4-1-2), wireless is restricted and segmented (2-4-1-4, 2-4-1-5), and direct corporate-to-OT communication is prevented, with required connections routed through a dedicated hardened jump host in the DMZ (2-4-1-9).

 © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports OTCC-1:2022

Facility Level Register

Record each critical facility, the outcome of the Facility Level Identification Tool against the three criteria, the approved methodology behind it (1-3-1-4) and the resulting L1, L2 or L3 control set.

Leveled Control Library

Hold every OTCC control with its level marking and its ECC reference so that an L2 facility sees exactly its 117 controls and subcontrols and the evidence for the ECC prerequisite sits beside them.

Exceptions and Risk Acceptance

Use Cyber & IT Risk to document any requirement that cannot be applied in the OT environment with its justification and approvals (1-3-1-6), and the alternative controls, period and reassessment dates for accepted risks (1-3-1-7).

OT Asset Inventory

Use IT Asset Management (ITAM) to keep the OT inventory in electronic form with owner, criticality rating and review date (2-1-1-1 to 2-1-1-5), including Safety Instrumented Systems and engineering workstations.

Change and Remote Access Records

Log OT changes with their separate-environment validation (1-5-3-2) and device replacement checks (1-5-3-3), and each remote access grant with its risk assessment, duration, privileges and session recording (2-2-1-7).

Third-Party and Review Evidence

Use Third Party Risk Management for vendor SDLC evidence and periodic assessments (4-1-1-3, 4-1-1-4), and Internal Audit Management for the annual (1-6-1) and three-yearly independent (1-6-2) reviews the NCA may request.

Common framework mappings

CIS Controls v8.1 · IEC 62443 · 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

Which facilities and systems are in scope of OTCC-1:2022?

Industrial control systems that reside in critical facilities owned or operated by government organizations or by private sector organizations owning, operating or hosting Critical National Infrastructures, in the Kingdom or abroad (Scope of Work). A critical facility is one whose destruction or dysfunction may disrupt or discontinue the organization's operation, and industrial control systems means all devices, systems or networks used to operate or automate industrial processes. Other organizations are encouraged to adopt the controls.

What are the three OTCC levels and how many controls apply at each?

The OTCC Facility Level Identification Tool assigns each critical facility Level 1, 2 or 3 based on the criticality and impact on business and service availability, the impact on health, safety and environment, and the impact on the national economy, national security or society. Table 1 gives the totals: L1 (high criticality) 151 controls and subcontrols including L2 and L3, L2 (moderate) 117 including L3, and L3 (low) 56. Every control in the document carries its level marking.

Updated Oct 29, 2026 · © 2026 SmartSuite Inc. All rights reserved.

How does the OTCC relate to the ECC?

The OTCC is implemented as an extension to the Essential Cybersecurity Controls, and compliance with the ECC is a mandatory prerequisite (Implementation and Compliance). Each OTCC control is written against an ECC reference, for example policies and procedures against ECC 1-3-1 to 1-3-4 and asset management against ECC subdomain 2-1. The Methodology and Mapping Annex describes the relationship to ECC domain 5, the industrial control systems domain of ECC-1:2018 that ECC-2:2024 removed and moved into the OTCC.

What does the OTCC require for network segmentation and remote access?

The OT environment must be segmented logically or physically from other networks (2-4-1-1), zones inside it segmented by level with traffic directed through choke points (2-4-1-2), Safety Instrumented Systems segmented from other OT networks (2-4-1-3), wireless restricted and segmented (2-4-1-4, 2-4-1-5), and direct corporate-to-OT communication prevented with connections routed through a hardened jump host in the DMZ (2-4-1-9). Remote access is restricted and enabled only when justified, after a risk assessment, through a multi-factor authenticated and encrypted channel for a defined period with limited privileges, and the session is monitored and recorded (2-2-1-7).

How does the NCA assess compliance with the OTCC?

All in-scope organizations must comply with the applicable controls at the appropriate level under item 3 of Article 10 of the NCA mandate and Royal Decree 57231 of 10/11/1439H. The NCA evaluates compliance through self-assessment by the organization and audit field visits by the NCA or designated third parties, and issues an OTCC-1:2022 Assessment and Compliance Tool to organize the evaluation. Internally, the cybersecurity function reviews implementation at least annually (1-6-1) and independent parties review it at least every three years (1-6-2).

License included / downloadable: Yes The National Cybersecurity Authority publishes the OTCC-1:2022 PDF as a public document (Document Classification: Public, Sharing Notice: White) on its regulatory documents page; the Arabic version is the binding text.

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