

## NCA OTCC APPLICABILITY & SCOPING CHECKLIST

# NCA OTCC Applicability & Scoping Checklist

A practical pre-assessment guide for organizations in Saudi Arabia reviewing Operational Technology Cybersecurity Controls (OTCC-1:2022).

### OTCC-1:2022 at a glance

|                        |                                                                                                    |
|------------------------|----------------------------------------------------------------------------------------------------|
| <b>Purpose</b>         | Minimum cybersecurity requirements for OT and industrial control system environments within scope. |
| <b>Structure</b>       | 4 main domains, 23 subdomains, 47 main controls and 122 subcontrols.                               |
| <b>Facility levels</b> | L1, L2 and L3 based on facility criticality and impact criteria.                                   |
| <b>Assessment</b>      | NCA provides an OTCC Assessment and Compliance Tool and a Facility Level Identification Tool.      |

### Before a detailed OTCC assessment

Use this checklist to organize regulatory scope, facility criticality, OT/ICS boundaries, applicable controls, evidence ownership and next actions.

SECURELINK RESOURCE - NOT AN NCA-ISSUED DOCUMENT

**OTCC**  
L1 L2 L3

# 1. Organization & Regulatory Applicability

Establish whether the organization and relevant OT/ICS environment fall within the OTCC scope before moving into detailed control testing.

| CHECK                    | ITEM                                                                                                                                 | STATUS / NOTES |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------|----------------|
| <input type="checkbox"/> | 01 Identify whether the organization is a Saudi government organization or related company/entity within the scope described by NCA. |                |
| <input type="checkbox"/> | 02 For private sector, determine whether the organization owns, operates or hosts Critical National Infrastructure (CNI).            |                |
| <input type="checkbox"/> | 03 Identify the facilities that contain Industrial Control Systems (ICS) and determine which are considered critical.                |                |
| <input type="checkbox"/> | 04 Document the regulatory driver for the review and any related sector or contractual obligations.                                  |                |
| <input type="checkbox"/> | 05 Record the legal entity, business unit and accountable owner for the OTCC programme.                                              |                |
| <input type="checkbox"/> | 06 Confirm whether ECC obligations also apply and identify the relevant cross-references to review.                                  |                |
| <input type="checkbox"/> | 07 Document any additional NCA control sets or regulatory requirements that must be considered separately.                           |                |
| <input type="checkbox"/> | 08 Record the formal scope decision, assumptions, evidence sources and approval owner.                                               |                |

Scope note: NCA published OTCC for critical facilities and ICS within its defined scope. NCA also encourages other organizations in the Kingdom to use OTCC as cybersecurity best practice where relevant.

## 2. Facility Criticality & L1 / L2 / L3

Use NCA methodology rather than assigning a level informally. Record the evidence supporting the decision.

|                                 |                                                                                                                                                                                                                 |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>L1 - Highest criticality</b> | Facility where an incident could have severe effects on operations, assets, resources, or health, safety and the environment. L1 facilities implement all OTCC controls and subcontrols stated in the document. |
| <b>L2 - Medium criticality</b>  | Facility where an incident could still cause significant adverse effects or operational impact. L2 facilities implement the controls identified for L2 and L3.                                                  |
| <b>L3 - Lower criticality</b>   | Facility where an incident could result in moderate adverse effects or operational impact. L3 facilities implement the L3 controls at minimum.                                                                  |

### Decision checks

| CHECK                    | ITEM                                                                                                                                                           | STATUS / NOTES |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|
| <input type="checkbox"/> | 01 Use the NCA Facility Level Identification Tool or documented methodology to support the facility-level decision.                                            |                |
| <input type="checkbox"/> | 02 Capture impact criteria, facility characteristics and supporting records used in the classification.                                                        |                |
| <input type="checkbox"/> | 03 Where systems with different criticality levels exist within one facility, document how the highest-criticality system affects the classification decision. |                |
| <input type="checkbox"/> | 04 Record the resulting facility level, applicable control set and approval/acceptance owner.                                                                  |                |

## 3. OT/ICS Boundaries & Dependencies

Make the assessment boundary explicit before mapping controls or requesting evidence.

| CHECK                    | ITEM                                                                                                                      | STATUS / NOTES |
|--------------------------|---------------------------------------------------------------------------------------------------------------------------|----------------|
| <input type="checkbox"/> | 01 Define the physical facilities and operational areas included in the review.                                           |                |
| <input type="checkbox"/> | 02 Identify OT/ICS assets, industrial networks, control systems, supporting systems and key dependencies.                 |                |
| <input type="checkbox"/> | 03 Map interfaces between OT, IT, cloud, enterprise systems and external connections that affect the assessment boundary. |                |
| <input type="checkbox"/> | 04 Document remote access paths, maintenance arrangements, supplier connections and support channels.                     |                |
| <input type="checkbox"/> | 05 Identify safety, operational continuity and engineering constraints that affect assessment or remediation activity.    |                |
| <input type="checkbox"/> | 06 Record systems or environments that are excluded and explain the reason for exclusion.                                 |                |
| <input type="checkbox"/> | 07 Identify dependencies on shared services, identity systems, network infrastructure or third parties.                   |                |
| <input type="checkbox"/> | 08 Obtain agreement on the final OTCC assessment boundary before detailed evidence review.                                |                |

Good practice: A defensible scope should show what is included, what is excluded, why the boundary was selected, and which dependencies could change the assessment outcome.

## 4. OTCC Domains & Applicable Control Areas

Use the official OTCC-1:2022 document and the applicable facility level to identify the controls that should be assessed.

### 01 Cybersecurity Governance

Governance structures, policies, responsibilities, OT cybersecurity risk management, project and change requirements, periodic reviews and workforce-related cybersecurity duties.

### 02 Cybersecurity Defense

OT/ICS asset management, identity and access control, network security, information protection, backup and recovery, monitoring, vulnerability-related controls and incident protection.

### 03 Cybersecurity Resilience

Operational continuity, recovery and the resilience of critical OT/ICS services and the dependencies they rely on.

### 04 Third-Party Cybersecurity

Suppliers, contractors, integrators, maintenance providers, remote support and other third parties that can affect the security of OT environments.

## Control review checks

| CHECK                    | ITEM                                                                                                           | STATUS / NOTES |
|--------------------------|----------------------------------------------------------------------------------------------------------------|----------------|
| <input type="checkbox"/> | 01 Confirm the control set applicable to each facility level.                                                  |                |
| <input type="checkbox"/> | 02 Map each applicable control/subcontrol to current policies, procedures, technical safeguards and evidence.  |                |
| <input type="checkbox"/> | 03 Flag controls that are implemented but not adequately evidenced.                                            |                |
| <input type="checkbox"/> | 04 Identify controls that require separate technical testing or engineering work and scope them appropriately. |                |
| <input type="checkbox"/> | 05 Record cross-references with the applicable NCA ECC baseline and other regulatory requirements.             |                |

## 5. Evidence Ownership, Gaps & Remediation

Turn control requirements into evidence, owners and actions that can be maintained.

| CHECK                    | ITEM                                                                                                                        | STATUS / NOTES |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------|----------------|
| <input type="checkbox"/> | 01 Identify the owner for each applicable control and the person responsible for supplying evidence.                        |                |
| <input type="checkbox"/> | 02 Collect current policies, procedures, standards, registers, architecture records and operational documentation.          |                |
| <input type="checkbox"/> | 03 Collect technical and operational evidence that shows controls are implemented and operating in practice.                |                |
| <input type="checkbox"/> | 04 Record missing, outdated, inconsistent or unapproved evidence as a finding or readiness gap.                             |                |
| <input type="checkbox"/> | 05 Link each gap to the relevant control, evidence requirement, risk, dependency and responsible owner.                     |                |
| <input type="checkbox"/> | 06 Prioritize remediation actions based on compliance urgency, risk, feasibility, dependencies and operational constraints. |                |
| <input type="checkbox"/> | 07 Create a remediation tracker with status, target date, owner and management escalation path.                             |                |
| <input type="checkbox"/> | 08 Retest or review evidence after remediation to confirm the gap is actually closed.                                       |                |

## 6. Assessment Readiness & Final Scope Decision

Complete this page before treating the OTCC work as assessment-ready.

| CHECK                    | ITEM                                                                                                          | STATUS / NOTES |
|--------------------------|---------------------------------------------------------------------------------------------------------------|----------------|
| <input type="checkbox"/> | 01 Applicability decision is documented and approved by the accountable owner.                                |                |
| <input type="checkbox"/> | 02 In-scope facilities and OT/ICS boundaries are confirmed.                                                   |                |
| <input type="checkbox"/> | 03 Facility levels L1, L2 or L3 are supported by documented evidence.                                         |                |
| <input type="checkbox"/> | 04 Applicable OTCC controls and subcontrols are identified for each facility.                                 |                |
| <input type="checkbox"/> | 05 Control owners and evidence owners are assigned.                                                           |                |
| <input type="checkbox"/> | 06 High-priority gaps and remediation actions are documented and tracked.                                     |                |
| <input type="checkbox"/> | 07 Key policies, procedures, records and technical evidence are available or have a defined remediation plan. |                |
| <input type="checkbox"/> | 08 Related ECC and other applicable requirements have been considered without blurring the OTCC scope.        |                |
| <input type="checkbox"/> | 09 Open risks, exclusions, assumptions and dependencies have been reported to management.                     |                |
| <input type="checkbox"/> | 10 A final readiness review has been completed before formal assessment activity.                             |                |

### FINAL DECISION

☐ Ready for assessment 
 ☐ Ready with actions outstanding 
 ☐ Scope or applicability still needs confirmation

## Official NCA source checkpoints

| SOURCE                             | REFERENCE                            |
|------------------------------------|--------------------------------------|
| NCA OTCC publication               | <a href="#">Open official source</a> |
| NCA OTCC official page             | <a href="#">Open official source</a> |
| OTCC Methodology and Mapping Annex | <a href="#">Open official source</a> |
| OTCC Implementation Guideline      | <a href="#">Open official source</a> |