

# How Ready is Your OT Environment for IEC 62443?

Practical OT security workbook augmented with OThello capabilities



IDENTIFY  
ASSETS



ASSESS  
RISKS



EVALUATE  
CONTROLS



TREAT &  
PRIORITIZE  
RISKS



MONITOR &  
IMPROVE

This page has been intentionally left blank

## Table of Contents

|                                                                         |           |
|-------------------------------------------------------------------------|-----------|
| <b><i>How to use this workbook</i></b> .....                            | <b>4</b>  |
| <b><i>Why OT readiness is different</i></b> .....                       | <b>5</b>  |
| <b><i>The IEC 62443 map: who each part is for</i></b> .....             | <b>6</b>  |
| Reading the map .....                                                   | 6         |
| <b><i>The scoring model</i></b> .....                                   | <b>7</b>  |
| The calculation .....                                                   | 7         |
| Indicative bands .....                                                  | 7         |
| The critical-gap override .....                                         | 7         |
| <b><i>Evidence quality</i></b> .....                                    | <b>9</b>  |
| What evidence looks like .....                                          | 9         |
| <b><i>Worked example (illustrative data)</i></b> .....                  | <b>10</b> |
| <b><i>Assessment worksheets, Domains A–J</i></b> .....                  | <b>11</b> |
| <b><i>Critical-gap identification matrix</i></b> .....                  | <b>17</b> |
| <b><i>30-60-90-day improvement plan</i></b> .....                       | <b>18</b> |
| First 30 days: establish visibility and contain critical exposure ..... | 18        |
| Days 31–60: address priority weaknesses .....                           | 18        |
| Days 61–90: validate and institutionalise .....                         | 18        |
| <b><i>Executive readiness summary template</i></b> .....                | <b>19</b> |
| <b><i>Next step: an evidence-led assessment workflow</i></b> .....      | <b>20</b> |
| What OThello Assess does, per the current product page .....            | 20        |
| Go deeper with Shieldworkz resources .....                              | 20        |
| About Shieldworkz .....                                                 | 21        |

## START HERE

## How to use this workbook

This workbook helps you answer five questions about your OT cybersecurity programme: **how mature is it, what has been addressed, which gaps matter most, what evidence supports your answers, and what to do in the next 30, 60 and 90 days**. It works on paper or on a laptop, and it is useful whether or not you ever use a tool.

|                    |                                                                                                                                     |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| <b>1 Scope</b>     | Define the system, site or plant you are assessing. Write it down. Everything you score is relative to this scope.                  |
| <b>2 Score</b>     | Work through Domains A–J (Section 6). For each question circle a score (0–4 or N/A) and an evidence label (U, D, O or T).           |
| <b>3 Verify</b>    | Ask for the evidence behind every 3 and 4. Downgrade or mark a score provisional when you cannot see it.                            |
| <b>4 Calculate</b> | Total each domain, then the overall score (Section 3). Apply the critical-gap override: some gaps matter regardless of the average. |
| <b>5 Act</b>       | Use the matrix (Section 7) and the 30-60-90 plan (Section 8), then summarise on one page (Section 9).                               |

**WHAT THIS WORKBOOK IS, AND IS NOT**

It is a **Shieldworkz-designed preliminary readiness methodology** to structure a self-assessment. The scale, the bands and the questions are ours. They are **not** an official IEC 62443 scoring system.

A self-assessment is **not** an independent audit, a formal certification or a declaration of compliance. IEC 62443 applicability depends on your system, your risk assessment and your obligations; not every organisation is required to apply it.

## SECTION 1

## Why OT readiness is different

An OT readiness assessment cannot be an IT checklist with different asset names. The same control can be sensible in an office network and hazardous on a live process. These realities shape how you should assess.

| Reality of OT                                        | What it means for the assessment                                                                                             |
|------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|
| <b>Safety and availability come first</b>            | Judge controls by what they do to the process, not only to the data. Ask who can approve an action and what it could affect. |
| <b>Long equipment lifecycles</b>                     | Unsupported components are normal. Assess compensating controls and lifecycle plans, not only patch status.                  |
| <b>Legacy and vendor-specific technology</b>         | Capabilities vary by vendor and version. Inventory and configuration baselines carry more weight than in IT.                 |
| <b>Limited room for intrusive testing</b>            | Lean on document review, walk-downs and passive observation. Active scanning or testing needs engineering approval first.    |
| <b>Interconnected IT, OT and third-party systems</b> | The IT/OT boundary and the supplier path are part of the OT attack surface.                                                  |
| <b>Loss of visibility, integrity or availability</b> | Consequences include losing sight of or control over the process, not only data theft.                                       |
| <b>Policy is not the same as a working control</b>   | Score what you can evidence. A policy shows intent; records, observation and tests show it works.                            |

**Existence is not effectiveness.** A meaningful assessment looks at both: does the practice exist, and is there evidence that it is implemented and works? That is why every question in this workbook carries an evidence column and a separate evidence label.

**WHAT SHIELDWORKZ RESEARCH OBSERVES**

The Shieldworkz *OT Cybersecurity Threat Landscape Analysis Report 2026* describes adversaries using legitimate tools (engineering workstations, vendor remote-access platforms and native OT software) to avoid detection, stolen credentials replacing the rogue insider, industrial protocols still appearing on internet-facing infrastructure, and attacks aimed at safety instrumented systems.

**Implication for this workbook:** the questions marked ▲ (remote and privileged access, boundaries, backups and recovery, process dependencies) are the ones most likely to need management attention whatever your overall score.

Source: Shieldworkz, 2026. Report summary at [shieldworkz.com/reports](https://shieldworkz.com/reports). Findings are qualitative here; consult the report for data and method.

## SECTION 2

## The IEC 62443 map: who each part is for

IEC 62443 is a **series, not a single checklist**. Its parts address different roles. Treating the whole series as one universal list is a common mistake. Applicability depends on the system you assess, your risk assessment, the requirements that are relevant to you and your own obligations.

| Part          | What it covers                                                                                                                                                                                                                                                        | Edition (verified)            | Mainly relevant to                                                                     |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------|----------------------------------------------------------------------------------------|
| IEC 62443-2-1 | Security programme requirements for IACS asset owners: the policies and procedures an owner or operator needs for a system in operation. The 2024 edition restructured requirements into programme elements and defined a maturity model for evaluating requirements. | Ed. 2.0, Aug 2024             | Asset owners and operators                                                             |
| IEC 62443-2-4 | Security programme requirements for IACS service providers: security-related processes offered to asset owners during integration and maintenance. Uses profiles to subset requirements.                                                                              | Ed. 2.0, Dec 2023             | Integrators, maintenance and other service providers; asset owners when selecting them |
| IEC 62443-3-2 | Security risk assessment for system design: defining the system under consideration, partitioning into zones and conduits, assessing risk and setting target security levels.                                                                                         | Ed. 1.0, Jun 2020             | Asset owners and system integrators                                                    |
| IEC 62443-3-3 | System security requirements and security levels, organised under seven foundational requirements.                                                                                                                                                                    | Ed. 1.0, Aug 2013 (COR1 2014) | System integrators, asset owners and designers                                         |
| IEC 62443-4-1 | Secure product development lifecycle requirements.                                                                                                                                                                                                                    | Ed. 1.0, Jan 2018             | Product suppliers and developers                                                       |
| IEC 62443-4-2 | Technical security requirements for IACS components.                                                                                                                                                                                                                  | Ed. 1.0, Feb 2019 (COR1 2022) | Component and product suppliers                                                        |

Editions checked on 19 October 2026 against IEC webstore and national-adoption listings. Some parts are under revision; confirm current status at [webstore.iec.ch](https://webstore.iec.ch) before relying on any edition. Other parts exist (for example 2-3 on patch management and 1-1 on concepts) and are not summarised here.

## Reading the map

- **Asset owners** usually anchor on **2-1** (programme) and **3-2** (risk, zones and conduits), use **3-3** as a reference for system requirements, and ask suppliers for **2-4**, **4-1** and **4-2** evidence.
- **Service providers** map to **2-4**. **Product suppliers** map to **4-1** and **4-2**.
- **Security levels** express a capability or target: a **target** (SL-T) is a design objective derived from risk, an **achieved** level (SL-A) describes the installed system, and a **capability** level (SL-C) describes what a component can do. A target is **not** a claim of compliance.
- The workbook's domain headers show an **indicative, part-level alignment only**. We do not cite clause numbers because they must be checked against the licensed standard text.

**THREE MISREADS TO AVOID**

**Choosing targets by attacker profile alone.** Anchor targets in consequence (safety, production, long-lead assets).

**Treating the series as a technical checklist.** Without a management system, controls decay.

**Relying on supplier claims.** Ask for test evidence and verify independently.

Based on Shieldworkz, IEC 62443 Practical Guide for OT/ICS and IIoT Security ([shieldworkz.com](https://shieldworkz.com)).

## SECTION 3

## The scoring model

A simple, consistent scale. Use it the same way for every question and every site, so that results are comparable over time.

| Score | Label                   | Meaning                                                                          |
|-------|-------------------------|----------------------------------------------------------------------------------|
| 0     | Not implemented         | No known control or documented process.                                          |
| 1     | Ad hoc                  | Some activity exists but is informal, inconsistent or dependent on individuals.  |
| 2     | Partially implemented   | The control exists in some areas but has material gaps in coverage or execution. |
| 3     | Implemented             | The control is documented, deployed and supported by relevant evidence.          |
| 4     | Verified and maintained | Implemented, periodically tested, measured and improved.                         |
| N/A   | Not applicable          | Not applicable to the defined scope, with a documented rationale and a reviewer. |

**N/A is not a 4.** An N/A response needs a written rationale, a named approver and a review date. It is removed from the calculation and reported separately, so it cannot raise your score. A high N/A count is a prompt to re-check your scope.

### The calculation

#### FORMULAS

**Domain score (%)** = points achieved ÷ (4 × applicable questions in the domain) × 100

**Overall readiness score (%)** = total points achieved across all applicable questions ÷ (4 × total applicable questions) × 100

Approved N/A questions are excluded from the denominators. Report the N/A count and list the rationales.

### Indicative bands

| Score  | Band                       | Typical reading                                                   |
|--------|----------------------------|-------------------------------------------------------------------|
| 0–24   | Foundational gaps          | Core practices are missing or informal.                           |
| 25–49  | Early development          | Practices exist in places; coverage and evidence are thin.        |
| 50–74  | Partial implementation     | Many controls exist; consistent evidence and testing are missing. |
| 75–89  | Substantial implementation | Most controls are documented, deployed and evidenced.             |
| 90–100 | High documented readiness  | Controls are evidenced, tested and improved.                      |

These bands are **indicative internal categories**. They are not official IEC 62443 maturity ratings, certification outcomes or proof of compliance.

### The critical-gap override

Averages hide weakness. A high overall score must never bury a severe gap in remote access, privileged access, safety-related dependencies or recovery. Questions marked ▲ are **critical-control questions**.

- Any ▲ question scored **0 or 1** is a **critical gap**. Report it on the first line of your summary, whatever the overall score.
- Any ▲ question scored **2 or higher with Unverified evidence** is **verify first**: do not rely on the score until evidence is seen.

- Report critical gaps and verify-first items next to the overall score, never beneath it.

Averaging has other limits. Equal weighting treats a documented policy and a tested recovery as comparable points, and a domain average can mask one failed control. Read the scores as a guide to where to look, not as a measure of risk.

## SECTION 4

## Evidence quality

Self-reported maturity can overstate real control effectiveness. For each question, record an **evidence label** alongside the score. Evidence quality is **separate** from the numerical score: a 3 with Unverified evidence is a claim, not yet a finding.

| Label      | Code | Meaning                                                                               |
|------------|------|---------------------------------------------------------------------------------------|
| Unverified | U    | Based only on an interview or assertion.                                              |
| Documented | D    | Supported by an applicable policy, procedure or record.                               |
| Observed   | O    | Supported by direct observation, configuration review or relevant technical evidence. |
| Tested     | T    | Supported by a documented test, exercise or repeatable validation.                    |

Practical rule: treat a **3 or 4 with U** as provisional. If you want a conservative view, calculate an optional second, **evidence-adjusted** score that caps every U-labelled answer at 2, and report both.

## What evidence looks like

| Control area                         | Documented                                  | Observed                                   | Tested                                         |
|--------------------------------------|---------------------------------------------|--------------------------------------------|------------------------------------------------|
| Asset inventory                      | Inventory export with owner and criticality | Site walk-down matches inventory           | Reconciliation against independent discovery   |
| Network diagrams, rules and conduits | Approved diagrams; justified rule list      | Configuration review confirms rules        | Rule change tested; unused rules removed       |
| Privileged access                    | Privileged account list; review sign-offs   | Sample of accounts checked in systems      | Leaver test shows access removed               |
| Remote access                        | Approved paths; vendor access register      | Remote access logs for a period            | Unapproved path attempt is blocked and alerted |
| Configuration baselines and change   | Baselines; change records                   | Running configuration compared to baseline | Drift detected and handled in a trial          |
| Backups                              | Backup schedule and coverage list           | Backup files located and checked           | Restoration test report with timings           |
| Incident response                    | OT incident response plan                   | Contacts and roles checked                 | Exercise report with closed actions            |
| Remediation                          | Tracker with owner and due date             | Fix observed in the system                 | Re-test confirms the gap is closed             |

**HANDLE ASSESSMENT EVIDENCE CAREFULLY**

Do **not** send credentials, controller logic, detailed production configurations or sensitive network diagrams through marketing forms, email or any platform your organisation has not approved. Record where evidence is held and who can show it. Use redacted or summary versions where possible, follow your data-classification rules, and complete your own approval process before uploading anything to any tool, including ours.

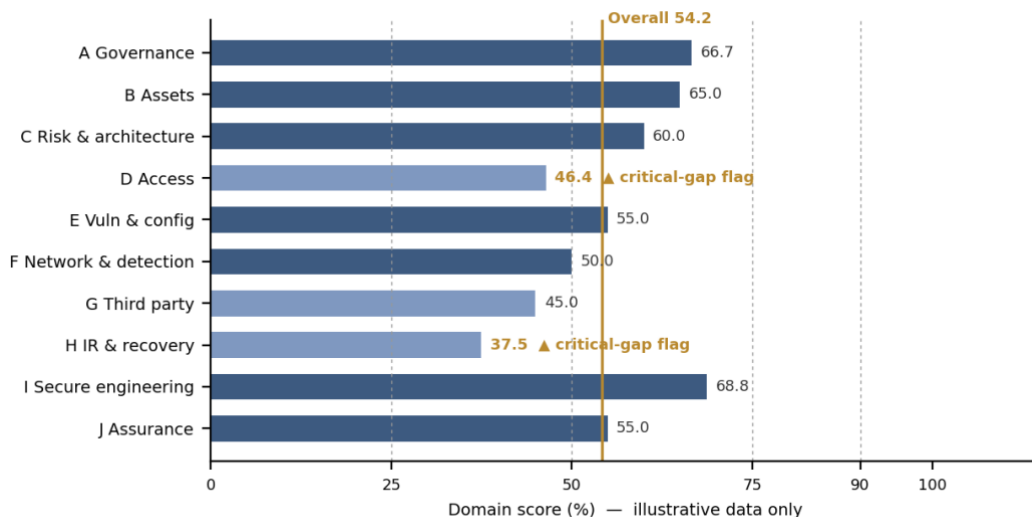
## SECTION 5

## Worked example (illustrative data)

**All data below is fictional and illustrative.** It shows how the arithmetic works and how to read the result. It is not a benchmark and does not describe any real organisation.

| Domain                            | Qs        | N/A      | Applicable | Max pts    | Achieved   | Score %     | Band                          |
|-----------------------------------|-----------|----------|------------|------------|------------|-------------|-------------------------------|
| A Governance                      | 6         | 0        | 6          | 24         | 16         | 66.7        | Partial implementation        |
| B Assets                          | 5         | 0        | 5          | 20         | 13         | 65.0        | Partial implementation        |
| C Risk and architecture           | 5         | 0        | 5          | 20         | 12         | 60.0        | Partial implementation        |
| D Access                          | 7         | 0        | 7          | 28         | 13         | 46.4        | Early development             |
| E Vulnerability and configuration | 5         | 0        | 5          | 20         | 11         | 55.0        | Partial implementation        |
| F Network and detection           | 5         | 0        | 5          | 20         | 10         | 50.0        | Partial implementation        |
| G Third party                     | 5         | 0        | 5          | 20         | 9          | 45.0        | Early development             |
| H Incident response and recovery  | 6         | 0        | 6          | 24         | 9          | 37.5        | Early development             |
| I Secure engineering              | 5         | 1        | 4          | 16         | 11         | 68.8        | Partial implementation        |
| J Assurance                       | 5         | 0        | 5          | 20         | 11         | 55.0        | Partial implementation        |
| <b>Total</b>                      | <b>54</b> | <b>1</b> | <b>53</b>  | <b>212</b> | <b>115</b> | <b>54.2</b> | <b>Partial implementation</b> |

Arithmetic: domain D, for example, has 7 applicable questions, so the maximum is  $7 \times 4 = 28$ ;  $13 \div 28 \times 100 = 46.4$ . Overall:  $115 \div 212 \times 100 = 54.2$ . The overall score pools points; it is not the mean of the ten domain percentages (54.9), and the small difference is expected because domains have different question counts.

**HOW TO READ THE EXAMPLE**

**Overall 54.2 sits in “Partial implementation”.** One N/A (question I5, no separate test environment on site) was approved with a rationale and removed from the denominator: 53 questions are applicable.

**Two critical gaps override the headline.** Remote access (D2) scored 1 and restoration testing (H4) scored 1. Both are ▲ questions, so they lead the executive summary. They would still lead it if the overall score were 80.

**Evidence mix across the 53 applicable questions:** Unverified 19, Documented 22, Observed 8, Tested 4. More than a third of the answers are still assertions, so the score is a starting point for verification, not a result to quote.

## SECTION 6

## Assessment worksheets, Domains A–J

Score each question for the scope you defined. ▲ marks a critical-control question (see the override in Section 3). Evidence codes: **U** Unverified, **D** Documented, **O** Observed, **T** Tested. Owner and next-action columns hold suggestions; overwrite them with your own. Use the notes column to record what you saw and where the evidence is held, not the sensitive evidence itself.

Scope assessed: \_\_\_\_\_ Assessor: \_\_\_\_\_ Date: \_\_\_\_\_ Reviewer: \_\_\_\_\_

| DOMAIN A Governance and Security Management <small>Indicative IEC 62443 alignment (part level): 2-1 (security programme); 2-4 for service providers</small> |                                                                                                                                                                                                                                    |                                                                    |                                                          |                         |                    |                                                                           |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------|----------------------------------------------------------|-------------------------|--------------------|---------------------------------------------------------------------------|
| #                                                                                                                                                           | Question and why it matters                                                                                                                                                                                                        | Examples of acceptable evidence                                    | Score (top) and evidence label (bottom): circle one each | Accountable owner       | Notes and findings | Next action if score ≤ 2 or unverified                                    |
| A1                                                                                                                                                          | <b>Is accountability for OT cybersecurity assigned to a named role with authority across IT, OT engineering and operations?</b><br><i>Why: Without one accountable owner, gaps fall between IT, engineering and safety teams.</i>  | Org chart or RACI; role description; appointment record            | 0 · 1 · 2 · 3 · 4 · N/A<br>U · D · O · T                 | CISO / plant leadership |                    | Name the accountable owner and publish a RACI.                            |
| A2                                                                                                                                                          | <b>Is there an approved OT security policy and programme that covers the defined scope?</b><br><i>Why: Policy is the authority behind every control, exception and escalation.</i>                                                 | Signed policy; programme charter; approval and review dates        | 0 · 1 · 2 · 3 · 4 · N/A<br>U · D · O · T                 | CISO                    |                    | Draft an OT-specific policy with engineering and safety sign-off.         |
| A3                                                                                                                                                          | <b>Is the programme scope documented (sites, systems, exclusions) with a rationale?</b><br><i>Why: A score only means something against a defined scope; unscoped systems are unassessed risk.</i>                                 | Scope statement; site and system list; exclusion rationale         | 0 · 1 · 2 · 3 · 4 · N/A<br>U · D · O · T                 | Programme owner         |                    | Write the scope statement and list exclusions with reasons.               |
| A4                                                                                                                                                          | <b>Are risk acceptance and escalation paths defined, with named approvers and expiry dates?</b><br><i>Why: Undocumented exceptions become permanent and invisible.</i>                                                             | Risk acceptance register; approval records; exceptions with expiry | 0 · 1 · 2 · 3 · 4 · N/A<br>U · D · O · T                 | Risk / asset owner      |                    | Create a register; set an expiry and review date for each entry.          |
| A5                                                                                                                                                          | <b>Do IT security, OT engineering, operations and safety coordinate through a working forum or joint procedures?</b><br><i>Why: OT incidents and changes cross team boundaries; coordination has to exist before it is needed.</i> | Forum charter; minutes; joint change or incident procedures        | 0 · 1 · 2 · 3 · 4 · N/A<br>U · D · O · T                 | OT security manager     |                    | Set a standing joint forum with an agreed agenda and escalation route.    |
| A6                                                                                                                                                          | <b>Does management review programme performance and set measurable improvement objectives at defined intervals?</b><br><i>Why: Reviews turn a programme from activity into managed improvement.</i>                                | Management review minutes; objectives with targets; KPI pack       | 0 · 1 · 2 · 3 · 4 · N/A<br>U · D · O · T                 | Executive sponsor       |                    | Schedule recurring reviews and agree three to five measurable objectives. |

| DOMAIN B Asset Inventory and System Understanding <small>Indicative IEC 62443 alignment (part level): 2-1; 3-2 (system under consideration)</small> |                                                                                                                                                                                                                                                            |                                                                         |                                                          |                                    |                    |                                                                            |
|-----------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------|----------------------------------------------------------|------------------------------------|--------------------|----------------------------------------------------------------------------|
| #                                                                                                                                                   | Question and why it matters                                                                                                                                                                                                                                | Examples of acceptable evidence                                         | Score (top) and evidence label (bottom): circle one each | Accountable owner                  | Notes and findings | Next action if score ≤ 2 or unverified                                     |
| ▲ B1                                                                                                                                                | <b>Is there a current inventory of OT assets (controllers, HMIs, servers, engineering workstations, network devices) with owner and criticality?</b><br><i>Why: You cannot protect or assess what you cannot name; every other domain depends on this.</i> | Inventory export with owner and criticality fields; last-validated date | 0 · 1 · 2 · 3 · 4 · N/A<br>U · D · O · T                 | OT engineering                     |                    | Baseline assets for the highest-consequence processes first.               |
| B2                                                                                                                                                  | <b>Does the inventory capture hardware, software and firmware versions where obtainable, and flag unsupported or end-of-life components?</b><br><i>Why: Exposure and compensating controls cannot be judged without version and support status.</i>        | Version fields; unsupported-asset list; vendor support statements       | 0 · 1 · 2 · 3 · 4 · N/A<br>U · D · O · T                 | OT engineering / vendor management |                    | Add version and support-status fields; start with controllers and servers. |

| <b>DOMAIN B Asset Inventory and System Understanding</b> Indicative IEC 62443 alignment (part level): 2-1; 3-2 (system under consideration) |                                                                                                                                                                                                  |                                                                        |                                                          |                              |                    |                                                                                 |
|---------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------|----------------------------------------------------------|------------------------------|--------------------|---------------------------------------------------------------------------------|
| #                                                                                                                                           | Question and why it matters                                                                                                                                                                      | Examples of acceptable evidence                                        | Score (top) and evidence label (bottom): circle one each | Accountable owner            | Notes and findings | Next action if score ≤ 2 or unverified                                          |
| B3                                                                                                                                          | <b>Are network architecture and communication paths documented and consistent with reality?</b><br><i>Why: Undocumented paths are unmanaged paths.</i>                                           | Current logical and physical diagrams with revision dates; flow matrix | <b>0 · 1 · 2 · 3 · 4 · N/A</b><br><b>U · D · O · T</b>   | OT network engineering       |                    | Reconcile diagrams against observed or configured flows.                        |
| B4                                                                                                                                          | <b>Is there visibility of engineering workstations, remote access points and external connections?</b><br><i>Why: These are the points where administrative control meets the outside world.</i> | Engineering workstation list; connection register; discovery results   | <b>0 · 1 · 2 · 3 · 4 · N/A</b><br><b>U · D · O · T</b>   | OT security                  |                    | Build a register of every external and remote path into OT.                     |
| B5                                                                                                                                          | <b>Is inventory accuracy validated on a defined cycle and after change, using methods that are safe for the process?</b><br><i>Why: A stale inventory gives false assurance.</i>                 | Validation records; reconciliation reports; site walk-down notes       | <b>0 · 1 · 2 · 3 · 4 · N/A</b><br><b>U · D · O · T</b>   | OT engineering / OT security |                    | Set a validation cycle; prefer document review, walk-downs and passive methods. |

| <b>DOMAIN C OT Risk Assessment and Security Architecture</b> Indicative IEC 62443 alignment (part level): 3-2 (risk assessment, zones and conduits); 3-3 |                                                                                                                                                                                                                                                                             |                                                                                |                                                          |                          |                    |                                                                              |
|----------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------|----------------------------------------------------------|--------------------------|--------------------|------------------------------------------------------------------------------|
| #                                                                                                                                                        | Question and why it matters                                                                                                                                                                                                                                                 | Examples of acceptable evidence                                                | Score (top) and evidence label (bottom): circle one each | Accountable owner        | Notes and findings | Next action if score ≤ 2 or unverified                                       |
| C1                                                                                                                                                       | <b>Is there a documented OT cybersecurity risk assessment for a defined system, reviewed within your policy interval?</b><br><i>Why: Risk assessment is what turns generic controls into priorities for your system.</i>                                                    | Risk assessment report; method statement; review date                          | <b>0 · 1 · 2 · 3 · 4 · N/A</b><br><b>U · D · O · T</b>   | OT security / risk       |                    | Scope one system and complete a documented assessment.                       |
| ▲ C2                                                                                                                                                     | <b>Are critical processes, their dependencies and the consequences of compromise or loss of availability documented, including safety-related dependencies?</b><br><i>Why: Consequence, not asset count, decides what must be protected first.</i>                          | Process dependency maps; consequence ratings agreed with operations and safety | <b>0 · 1 · 2 · 3 · 4 · N/A</b><br><b>U · D · O · T</b>   | Operations / safety      |                    | Run a consequence workshop with operations and safety for the top processes. |
| ▲ C3                                                                                                                                                     | <b>Are security zones and conduits (or equivalent segments and boundaries) defined, with permitted communications documented?</b><br><i>Why: Defined boundaries limit how far a compromise can travel.</i>                                                                  | Zone and conduit model; approved flow matrix; justified firewall rules         | <b>0 · 1 · 2 · 3 · 4 · N/A</b><br><b>U · D · O · T</b>   | OT network architect     |                    | Define zones for the highest-consequence area; document permitted flows.     |
| C4                                                                                                                                                       | <b>Are dependencies on enterprise IT, cloud services and suppliers identified and assessed?</b><br><i>Why: Shared services (directory, patching, historians, remote support) carry risk into OT.</i>                                                                        | Dependency register; shared-service list; assessment notes                     | <b>0 · 1 · 2 · 3 · 4 · N/A</b><br><b>U · D · O · T</b>   | IT / OT architecture     |                    | List shared services and the OT functions that rely on each.                 |
| C5                                                                                                                                                       | <b>Are target security requirements (for example target security levels, where used) approved on the basis of risk and consequence, not attacker profile alone?</b><br><i>Why: Targets set without consequence analysis are either over-engineered or under-protective.</i> | Approved targets per zone with rationale and sign-off                          | <b>0 · 1 · 2 · 3 · 4 · N/A</b><br><b>U · D · O · T</b>   | Risk owner / OT security |                    | Record the rationale for each target and obtain owner approval.              |

**DOMAIN D Identity, Privileged Access and Remote Access** Indicative IEC 62443 alignment (part level): 2-1; 3-3 (identification, authentication and use control)

| #    | Question and why it matters                                                                                                                                                                                                           | Examples of acceptable evidence                                                   | Score (top) and evidence label (bottom): circle one each | Accountable owner               | Notes and findings | Next action if score ≤ 2 or unverified                                    |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|----------------------------------------------------------|---------------------------------|--------------------|---------------------------------------------------------------------------|
| ▲ D1 | <b>Are privileged and engineering accounts individually accountable, with shared credentials removed or tightly controlled?</b><br><i>Why: Shared administrative accounts remove accountability and make investigation difficult.</i> | Privileged account list; shared-account exceptions; vault or access configuration | 0 · 1 · 2 · 3 · 4 · N/A<br>U · D · O · T                 | IAM / OT security               |                    | List all privileged accounts; remove or compensate for shared ones.       |
| ▲ D2 | <b>Is remote access to OT controlled with appropriate authentication and approved paths only?</b><br><i>Why: Remote access is a primary route between outside networks and process systems.</i>                                       | Remote access architecture; authentication configuration; approved access list    | 0 · 1 · 2 · 3 · 4 · N/A<br>U · D · O · T                 | OT security / network           |                    | Inventory remote paths; close unapproved ones; strengthen authentication. |
| ▲ D3 | <b>Are third-party access paths approved, time-bound and monitored?</b><br><i>Why: Vendor access is legitimate by design, which makes misuse harder to spot.</i>                                                                      | Vendor access register; session approvals; access logs                            | 0 · 1 · 2 · 3 · 4 · N/A<br>U · D · O · T                 | Vendor management / OT security |                    | Require approval and an end time for each vendor session.                 |
| D4   | <b>Are access provisioning and removal triggered by joiner, mover, leaver and contract-end events?</b><br><i>Why: Stale access accumulates quietly, especially for contractors.</i>                                                   | Provisioning tickets; leaver records; a sampled test                              | 0 · 1 · 2 · 3 · 4 · N/A<br>U · D · O · T                 | IAM / HR                        |                    | Link removal to HR and contract events; sample-test quarterly.            |
| D5   | <b>Are access rights reviewed periodically, with evidence that excess access was removed?</b><br><i>Why: A review without removals is a ritual, not a control.</i>                                                                    | Review sign-offs; before-and-after access lists                                   | 0 · 1 · 2 · 3 · 4 · N/A<br>U · D · O · T                 | System owners                   |                    | Run a first review on the most privileged accounts.                       |
| D6   | <b>Are privileged and remote sessions logged, and are the logs reviewed?</b><br><i>Why: Logging without review does not detect anything.</i>                                                                                          | Log configuration; review records; sample investigations                          | 0 · 1 · 2 · 3 · 4 · N/A<br>U · D · O · T                 | OT security / SOC               |                    | Define who reviews logs, how often and what triggers escalation.          |
| D7   | <b>Are emergency (break-glass) access procedures safe, controlled, tested and audited?</b><br><i>Why: Emergency access must work in a crisis without becoming a standing back door.</i>                                               | Break-glass procedure; test record; post-use audit                                | 0 · 1 · 2 · 3 · 4 · N/A<br>U · D · O · T                 | OT operations / OT security     |                    | Document and test the procedure; review every use afterwards.             |

**DOMAIN E Vulnerability and Configuration Management** Indicative IEC 62443 alignment (part level): 2-1; 2-3 (patch management, technical report); 3-3

| #  | Question and why it matters                                                                                                                                                                                                                   | Examples of acceptable evidence                                                   | Score (top) and evidence label (bottom): circle one each | Accountable owner            | Notes and findings | Next action if score ≤ 2 or unverified                                        |
|----|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|----------------------------------------------------------|------------------------------|--------------------|-------------------------------------------------------------------------------|
| E1 | <b>Is there an OT-aware vulnerability management process that weighs exploitability and operational consequence before action?</b><br><i>Why: Generic severity scores ignore process impact and the limits of what can be changed safely.</i> | Procedure; vulnerability register with consequence notes; advisory intake         | 0 · 1 · 2 · 3 · 4 · N/A<br>U · D · O · T                 | OT security / engineering    |                    | Define intake and triage with engineering; record the decision for each item. |
| E2 | <b>Are configuration baselines documented for critical systems and checked for drift?</b><br><i>Why: You cannot spot unauthorised change without a known-good reference.</i>                                                                  | Baseline documents; configuration backups; comparison reports                     | 0 · 1 · 2 · 3 · 4 · N/A<br>U · D · O · T                 | OT engineering               |                    | Baseline the most critical systems first.                                     |
| E3 | <b>Are changes approved, assessed for operational risk, tested where feasible and traceable, including emergency changes?</b><br><i>Why: Uncontrolled change is both a safety risk and a security risk.</i>                                   | Change records; approval minutes; rollback plans                                  | 0 · 1 · 2 · 3 · 4 · N/A<br>U · D · O · T                 | OT change authority          |                    | Extend the change process to OT with an agreed emergency route.               |
| E4 | <b>Is patching decided on risk, with compensating controls documented where patching is not feasible?</b><br><i>Why: Indiscriminate patching or active scanning of live OT can itself cause disruption; decisions need engineering input.</i> | Patch decision log; compensating-control records; vendor compatibility statements | 0 · 1 · 2 · 3 · 4 · N/A<br>U · D · O · T                 | OT engineering / OT security |                    | Create a decision log; require a recorded rationale for deferral.             |

**DOMAIN E Vulnerability and Configuration Management** Indicative IEC 62443 alignment (part level): 2-1; 2-3 (patch management, technical report); 3-3

| #  | Question and why it matters                                                                                                                                                                                      | Examples of acceptable evidence                                 | Score (top) and evidence label (bottom): circle one each | Accountable owner            | Notes and findings | Next action if score ≤ 2 or unverified                                       |
|----|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------|----------------------------------------------------------|------------------------------|--------------------|------------------------------------------------------------------------------|
| E5 | <b>Are unsupported systems and vendor constraints tracked with an owner, compensating controls and a lifecycle plan?</b><br><i>Why: Unsupported components are normal in OT; unmanaged ones are the problem.</i> | Unsupported-asset register; exception approvals; lifecycle plan | 0 · 1 · 2 · 3 · 4 · N/A<br>U · D · O · T                 | OT engineering / asset owner |                    | Register each unsupported asset with a compensating control and review date. |

**DOMAIN F Network Security and Threat Detection** Indicative IEC 62443 alignment (part level): 3-3 (restricted data flow, timely response to events); 3-2

| #    | Question and why it matters                                                                                                                                                                         | Examples of acceptable evidence                                | Score (top) and evidence label (bottom): circle one each | Accountable owner               | Notes and findings | Next action if score ≤ 2 or unverified                           |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------|----------------------------------------------------------|---------------------------------|--------------------|------------------------------------------------------------------|
| ▲ F1 | <b>Are IT/OT and external communications controlled, justified and documented at defined boundaries?</b><br><i>Why: Unnecessary or undocumented flows widen the attack surface and hide misuse.</i> | Boundary rulebase review; flow justifications; DMZ design      | 0 · 1 · 2 · 3 · 4 · N/A<br>U · D · O · T                 | Network security                |                    | Review boundary rules; remove or justify each permitted flow.    |
| F2   | <b>Are critical conduits monitored, with visibility of the industrial protocols in use?</b><br><i>Why: Visibility of process-relevant traffic is the basis for detection.</i>                       | Monitoring architecture; coverage map; protocol list           | 0 · 1 · 2 · 3 · 4 · N/A<br>U · D · O · T                 | OT security                     |                    | Map monitoring coverage against critical conduits.               |
| F3   | <b>Can you detect unauthorised communications, new devices and configuration or logic changes?</b><br><i>Why: Detection is only credible if it has been demonstrated.</i>                           | Detection use cases; alert samples; validation results         | 0 · 1 · 2 · 3 · 4 · N/A<br>U · D · O · T                 | OT security / SOC               |                    | Define detection use cases and test them against safe scenarios. |
| F4   | <b>Is logging adequate for investigation, with synchronised time and defined retention?</b><br><i>Why: Investigations stall without consistent timestamps and retained logs.</i>                    | Log source list; time synchronisation design; retention policy | 0 · 1 · 2 · 3 · 4 · N/A<br>U · D · O · T                 | OT security / IT infrastructure |                    | List log sources and gaps; agree time source and retention.      |
| F5   | <b>Are alerts triaged jointly with OT engineering, and are monitoring blind spots identified and tracked?</b><br><i>Why: An alert about a controller means little without engineering context.</i>  | Triage runbooks; escalation records; blind-spot register       | 0 · 1 · 2 · 3 · 4 · N/A<br>U · D · O · T                 | SOC / OT engineering            |                    | Agree who triages what, and record blind spots with owners.      |

**DOMAIN G Third-Party and Supply-Chain Security** Indicative IEC 62443 alignment (part level): 2-4 (service providers); 2-1; 4-1 and 4-2 for product suppliers

| #  | Question and why it matters                                                                                                                                                                             | Examples of acceptable evidence                              | Score (top) and evidence label (bottom): circle one each | Accountable owner                 | Notes and findings | Next action if score ≤ 2 or unverified                                   |
|----|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------|----------------------------------------------------------|-----------------------------------|--------------------|--------------------------------------------------------------------------|
| G1 | <b>Is there an inventory of critical OT suppliers and service providers, with the systems and sites each supports?</b><br><i>Why: You cannot manage supplier risk without knowing who touches what.</i> | Supplier register; criticality rating; escalation contacts   | 0 · 1 · 2 · 3 · 4 · N/A<br>U · D · O · T                 | Procurement / OT engineering      |                    | Build the register from maintenance contracts and access lists.          |
| G2 | <b>Are security requirements defined for external parties in contracts and onboarding?</b><br><i>Why: Requirements that are not agreed cannot be enforced later.</i>                                    | Contract clauses; supplier questionnaires; assurance reports | 0 · 1 · 2 · 3 · 4 · N/A<br>U · D · O · T                 | Procurement / legal / OT security |                    | Draft standard OT security clauses; request supplier assurance evidence. |
| G3 | <b>Is vendor maintenance activity approved, supervised and recorded?</b><br><i>Why: Maintenance is a routine route for change and for compromise.</i>                                                   | Work permits; maintenance logs; post-work verification       | 0 · 1 · 2 · 3 · 4 · N/A<br>U · D · O · T                 | Plant maintenance / OT security   |                    | Require a permit and a post-work check for each vendor visit.            |

**DOMAIN G Third-Party and Supply-Chain Security**

Indicative IEC 62443 alignment (part level): 2-4 (service providers); 2-1; 4-1 and 4-2 for product suppliers

| #  | Question and why it matters                                                                                                                                                                                         | Examples of acceptable evidence                                   | Score (top) and evidence label (bottom): circle one each | Accountable owner         | Notes and findings | Next action if score ≤ 2 or unverified                               |
|----|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------|----------------------------------------------------------|---------------------------|--------------------|----------------------------------------------------------------------|
| G4 | <b>Are integrity checks required for software, firmware and engineering tools (trusted source, hash or signature verification)?</b><br><i>Why: Tampered or untrusted updates enter through legitimate channels.</i> | Procedure; verification records; approved source list             | 0 · 1 · 2 · 3 · 4 · N/A<br>U · D · O · T                 | OT engineering            |                    | Define approved sources and a verification step before installation. |
| G5 | <b>Do suppliers have incident-notification obligations, and are shared-service dependencies reviewed?</b><br><i>Why: Supplier incidents can become your incident before you hear about them.</i>                    | Notification terms; supplier incident contacts; dependency review | 0 · 1 · 2 · 3 · 4 · N/A<br>U · D · O · T                 | Procurement / OT security |                    | Add notification terms and test the contact route.                   |

**DOMAIN H Incident Response and Recovery**

Indicative IEC 62443 alignment (part level): 2-1; 3-3 (timely response, resource availability)

| #    | Question and why it matters                                                                                                                                                                                                                                                 | Examples of acceptable evidence                                          | Score (top) and evidence label (bottom): circle one each | Accountable owner                 | Notes and findings | Next action if score ≤ 2 or unverified                             |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------|----------------------------------------------------------|-----------------------------------|--------------------|--------------------------------------------------------------------|
| ▲ H1 | <b>Is there an OT-specific incident response plan with named roles across security, operations, engineering and safety?</b><br><i>Why: IT playbooks assume actions (isolation, reboot) that can be unsafe on live processes.</i>                                            | OT incident response plan; role assignments; contact tree                | 0 · 1 · 2 · 3 · 4 · N/A<br>U · D · O · T                 | OT security / operations          |                    | Adapt the IT plan with operations and safety; name roles.          |
| H2   | <b>Is decision authority for containment actions (for example isolating IT/OT links) agreed in advance with operations and safety?</b><br><i>Why: Delays in authority cost time during an incident.</i>                                                                     | Decision matrix; pre-approved containment actions                        | 0 · 1 · 2 · 3 · 4 · N/A<br>U · D · O · T                 | Operations / safety / OT security |                    | Agree who can authorise isolation, and under what conditions.      |
| ▲ H3 | <b>Are backups of controller logic, configurations and engineering project files current, protected from the production network, and complete for critical systems?</b><br><i>Why: Recovery depends on having known-good engineering assets that survived the incident.</i> | Backup schedule and logs; storage location and protection; coverage list | 0 · 1 · 2 · 3 · 4 · N/A<br>U · D · O · T                 | OT engineering                    |                    | Confirm coverage for critical systems; separate at least one copy. |
| ▲ H4 | <b>Has restoration been tested for critical systems against the required recovery time?</b><br><i>Why: An untested backup is an assumption.</i>                                                                                                                             | Restoration test report; timings; issues log                             | 0 · 1 · 2 · 3 · 4 · N/A<br>U · D · O · T                 | OT engineering / operations       |                    | Schedule a safe restoration test on a representative system.       |
| H5   | <b>Are recovery priorities aligned with business and safety requirements, including safe degraded or manual operation where feasible?</b><br><i>Why: Recovery order should follow consequence, and operators need a safe fallback.</i>                                      | Recovery priority list; manual operating procedures; operator drills     | 0 · 1 · 2 · 3 · 4 · N/A<br>U · D · O · T                 | Operations / safety               |                    | Agree recovery priorities; document manual and degraded modes.     |
| H6   | <b>Have realistic OT disruption scenarios been exercised within the last 12 months, with lessons tracked to closure?</b><br><i>Why: Exercises find gaps that documents hide.</i>                                                                                            | Exercise report; action log with closure evidence                        | 0 · 1 · 2 · 3 · 4 · N/A<br>U · D · O · T                 | OT security / operations          |                    | Run a tabletop on a plausible OT scenario with operations present. |

**DOMAIN I Secure Engineering and Change Management**

Indicative IEC 62443 alignment (part level): 2-1; 2-4 (integration and maintenance activities)

| #  | Question and why it matters                                                                                                                                                                                                                              | Examples of acceptable evidence                                                                           | Score (top) and evidence label (bottom): circle one each | Accountable owner              | Notes and findings | Next action if score ≤ 2 or unverified                                               |
|----|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------|----------------------------------------------------------|--------------------------------|--------------------|--------------------------------------------------------------------------------------|
| I1 | <b>Is access to engineering workstations and project files restricted, protected and logged?</b><br><i>Why: Engineering workstations can change process behaviour; they are high-value targets.</i>                                                      | Access lists; repository permissions; logging configuration                                               | 0 · 1 · 2 · 3 · 4 · N/A<br>U · D · O · T                 | OT engineering / OT security   |                    | Restrict and log access; review who can modify controller projects.                  |
| I2 | <b>Are controller logic and configuration changes approved and traceable to a requester and a rationale?</b><br><i>Why: Traceability separates authorised engineering from unauthorised change.</i>                                                      | Change tickets linked to project versions                                                                 | 0 · 1 · 2 · 3 · 4 · N/A<br>U · D · O · T                 | OT engineering                 |                    | Link every logic change to a ticket and a version.                                   |
| I3 | <b>Can you verify that running controller logic and configuration match the authorised version?</b><br><i>Why: Detecting unapproved change depends on a comparison baseline.</i>                                                                         | Comparison or hash reports; periodic verification records                                                 | 0 · 1 · 2 · 3 · 4 · N/A<br>U · D · O · T                 | OT engineering / OT security   |                    | Start with critical controllers; set a verification interval.                        |
| I4 | <b>Are removable media and engineering laptops controlled (authorised, scanned, inventoried)?</b><br><i>Why: Portable media and laptops cross network boundaries by hand.</i>                                                                            | Media procedure; scan records; laptop register                                                            | 0 · 1 · 2 · 3 · 4 · N/A<br>U · D · O · T                 | OT engineering / site security |                    | Introduce a media procedure and a laptop register.                                   |
| I5 | <b>Is system integrity verified after maintenance or change, and are development and test activities separated from production where applicable?</b><br><i>Why: Post-maintenance checks catch unintended change; separation protects live processes.</i> | Post-maintenance checklists; test environment description; N/A rationale where no test environment exists | 0 · 1 · 2 · 3 · 4 · N/A<br>U · D · O · T                 | OT engineering                 |                    | Add a post-maintenance check; document the separation approach or the N/A rationale. |

**DOMAIN J Monitoring, Assurance and Continuous Improvement**

Indicative IEC 62443 alignment (part level): 2-1 (reviews, evaluation and improvement)

| #  | Question and why it matters                                                                                                                                                                                                                                 | Examples of acceptable evidence                                         | Score (top) and evidence label (bottom): circle one each | Accountable owner            | Notes and findings | Next action if score ≤ 2 or unverified                                 |
|----|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------|----------------------------------------------------------|------------------------------|--------------------|------------------------------------------------------------------------|
| J1 | <b>Are OT cybersecurity KPIs and KRIs defined, owned and reported on a regular cadence?</b><br><i>Why: What is not measured is not managed.</i>                                                                                                             | KPI and KRI definitions; dashboards; trend reports                      | 0 · 1 · 2 · 3 · 4 · N/A<br>U · D · O · T                 | OT security manager          |                    | Pick five measures linked to your highest-risk gaps.                   |
| J2 | <b>Is control effectiveness reviewed periodically, not just control existence?</b><br><i>Why: Existence and effectiveness are different findings.</i>                                                                                                       | Review or test plans and results; internal audit reports                | 0 · 1 · 2 · 3 · 4 · N/A<br>U · D · O · T                 | OT security / internal audit |                    | Choose three controls to test for effectiveness this quarter.          |
| J3 | <b>Does every remediation action have an owner, a due date and a tracked status?</b><br><i>Why: Unowned actions do not close.</i>                                                                                                                           | Remediation tracker; status reports                                     | 0 · 1 · 2 · 3 · 4 · N/A<br>U · D · O · T                 | Programme owner              |                    | Create a tracker and assign owners to all critical gaps.               |
| J4 | <b>Is remediation verified after completion, with evidence that the gap is closed?</b><br><i>Why: Closed on paper is not closed in practice.</i>                                                                                                            | Re-test results; evidence of verification; updated scores               | 0 · 1 · 2 · 3 · 4 · N/A<br>U · D · O · T                 | OT security / assessor       |                    | Require evidence before closing any critical gap.                      |
| J5 | <b>Is reassessment triggered by material change (new site, major change, incident), and does reporting connect technical findings to operational risk?</b><br><i>Why: Posture changes when the system does; leaders need findings in operational terms.</i> | Reassessment triggers; reports linking findings to process consequences | 0 · 1 · 2 · 3 · 4 · N/A<br>U · D · O · T                 | OT security / risk           |                    | Define triggers; add a consequence statement to each reported finding. |

## SECTION 7

## Critical-gap identification matrix

Typical gaps found in OT assessments, with the evidence you need and a sensible first step. **These are examples, not a ranking.** Actual severity depends on the system, its exposure, the process consequence, compensating controls and your risk assessment. A gap that is critical in one plant can be minor in another.

| Security domain                   | Example gap                                                                     | Potential operational consequence                                               | Evidence required                                              | Suggested priority (starting point)                              | Accountable owner               | Recommended next step                                                        |
|-----------------------------------|---------------------------------------------------------------------------------|---------------------------------------------------------------------------------|----------------------------------------------------------------|------------------------------------------------------------------|---------------------------------|------------------------------------------------------------------------------|
| <b>B Assets</b>                   | Critical assets are unknown or the inventory is out of date                     | Compromise or failure may go unnoticed; recovery and impact analysis are slowed | Inventory export with owner and criticality; validation record | Often High; depends on process criticality                       | OT engineering                  | Baseline the highest-consequence processes first; set a validation cycle     |
| <b>D Access / G Third party</b>   | Vendor remote access is uncontrolled (permanent, shared or unlogged)            | An external path to process systems; hard to attribute activity                 | Vendor access register; approval records; session logs         | Often High to Critical where reachable from outside              | OT security / vendor management | Inventory paths; require approval, end time and logging per session          |
| <b>F Network / C Architecture</b> | Unnecessary or undocumented IT/OT communications                                | Wider attack surface; compromise in IT may reach OT                             | Approved flow matrix; boundary rule review with justifications | Often High; depends on exposure and compensating controls        | Network security                | Review boundary rules; remove or justify each permitted flow                 |
| <b>B Assets / E Vulnerability</b> | Critical components are unsupported or end-of-life with no compensating control | Known weaknesses cannot be fixed; failure may lack a spare or vendor help       | Unsupported-asset register; compensating-control records       | Varies; High where exposed and process-critical                  | OT engineering / asset owner    | Register each asset; add a compensating control and a lifecycle plan         |
| <b>H Recovery</b>                 | Backups of engineering configurations are unverified or untested                | Slow or failed recovery after an incident or failure                            | Backup coverage list; restoration test report with timings     | Often High for critical systems                                  | OT engineering                  | Confirm coverage; separate a copy; run a safe restoration test               |
| <b>H Incident response</b>        | No OT-specific incident response procedure                                      | Delays or unsafe actions under pressure; unclear authority to isolate           | OT incident response plan; role assignments; exercise report   | Often High; depends on process consequence                       | OT security / operations        | Adapt the IT plan with operations and safety; agree decision authority       |
| <b>I Secure engineering</b>       | Engineering changes cannot be traced or verified                                | Unauthorised or erroneous logic changes may go undetected                       | Change tickets linked to project versions; comparison reports  | High where safety or process logic is affected                   | OT engineering                  | Link changes to tickets; verify running logic against the authorised version |
| <b>F Detection</b>                | Monitoring of critical conduits is incomplete                                   | Intrusion or misuse stays hidden; slower investigation                          | Coverage map; detection use cases; test results                | Medium to High; depends on exposure and other detective controls | OT security / SOC               | Map coverage to critical conduits; track blind spots with owners             |
| <b>D Privileged access</b>        | Shared privileged or engineering accounts                                       | No accountability; weak investigation; wider misuse                             | Privileged account list; shared-account exceptions             | Often High; depends on what the accounts control                 | IAM / OT security               | Remove or tightly control shared accounts; individual accountability         |

## 30-60-90-day improvement plan

A starting template. Begin with every critical gap (▲ scored 0–1), then work by consequence. Question references show where each action comes from.

### First 30 days: establish visibility and contain critical exposure

- Validate the critical asset inventory for the highest-consequence processes (B1, B5)
- Review privileged and remote access: remove stale or shared access, confirm approved paths and authentication (D1–D3)
- List every IT/OT and internet-facing path; close or justify each (F1)
- Identify the largest monitoring blind spots (F2, F5)
- Verify that critical controller and engineering backups exist, are protected and are plausibly restorable (H3)
- Assign an owner and due date to every critical gap (J3)

### Days 31–60: address priority weaknesses

- Document key zones, conduits and permitted communications (C3)
- Formalise supplier access: approval, end time, logging and maintenance permits (D3, G2, G3)
- Establish configuration baselines and change traceability for critical systems (E2, E3, I2)
- Close high-priority control gaps; record compensating controls where closure is not feasible (E4, E5)
- Walk through the OT incident response procedure with operations and safety (H1, H2)

### Days 61–90: validate and institutionalise

- Test restoration for at least one critical system (H4)
- Measure detection effectiveness against agreed use cases (F3)
- Verify remediation with evidence and re-score (J4)
- Update the risk assessment where architecture or dependencies changed (C1)
- Set a recurring management review and reassessment triggers (A6, J5)

|                                             |
|---------------------------------------------|
| <b>A TEMPLATE, NOT A UNIVERSAL SEQUENCE</b> |
|---------------------------------------------|

|                                                                                                                                                                                                                                                                            |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Real priorities depend on operational risk, safety, engineering constraints, system criticality and available resources. Do not apply changes to live systems, including scanning, patching or isolation, without the engineering and safety approvals your site requires. |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

# Executive readiness summary template

**IMPORTANT**  
This summary is a **self-assessment** using a Shieldworkz-designed preliminary methodology. It is **not** an independent audit, a formal certification or a declaration of compliance with IEC 62443 or any other standard.

|                              |               |                 |                                    |
|------------------------------|---------------|-----------------|------------------------------------|
| Organisation                 |               | Assessment date |                                    |
| Assessment scope             |               |                 |                                    |
| Overall preliminary score    | % Band: _____ | N/A questions   | Count: _____ (rationales attached) |
| Evidence mix (applicable Qs) | U __ D O T    |                 |                                    |

| A | B | C | D | E | F | G | H | I | J |
|---|---|---|---|---|---|---|---|---|---|
| — | — | — | — | — | — | — | — | — | — |

| # | Top five identified gaps | Domain | Priority | Owner |
|---|--------------------------|--------|----------|-------|
| 1 |                          |        |          |       |
| 2 |                          |        |          |       |
| 3 |                          |        |          |       |
| 4 |                          |        |          |       |
| 5 |                          |        |          |       |

|                                                                                    |  |
|------------------------------------------------------------------------------------|--|
| Critical gaps requiring management attention (▲ scored 0–1) and verify-first items |  |
| Evidence-quality limitations                                                       |  |
| Immediate actions (next 30 days)                                                   |  |
| Proposed 60-day and 90-day priorities                                              |  |
| Assumptions and exclusions                                                         |  |
| Review owner / next assessment date                                                |  |

## Next step: an evidence-led assessment workflow

### Turn OT security assessment into a structured, evidence-led process.

You now have a way to score readiness, label evidence and flag critical gaps. The slow part is usually gathering scattered documentation, mapping it to requirements and organising findings. That is where an assessment tool can help, and it is why Shieldworkz built OThello Assess.

### What OThello Assess does, per the current product page

- Ingests your existing documentation, maps evidence to relevant security requirements, identifies gaps and organises findings into an assessment.
- Follows a five-step workflow: set up the project and upload documents; review the initial assessment (assets, threats, crown jewels, gaps); configure the risk matrix, confirm zones and conduits and set target security levels; review and confirm risk scores, evidence and remediation plan; generate the report.
- Produces, per its description, an achieved security level for each zone, gaps per zone ranked by severity, a security-level heat map, recommended controls and a remediation plan, with findings traced to source documents.
- States that it generates an IEC 62443 assessment report in **under 24 hours**, with about **85 minutes of human input** across the review steps.
- 

#### WHAT THAT DOES AND DOES NOT MEAN

The 24-hour figure refers to producing the assessment report from the documentation you upload, after your team's review input. Results depend on the quality and completeness of that documentation and on your own judgement. It is not remediation, independent verification, certification or a statement of compliance.

This workbook is a programme-level readiness check. OThello Assess is a separate, system-level assessment workflow against your chosen standard; the two are complementary, not identical.

## Assess Your OT Environment with OThello

*Move from scattered documentation and manual gap identification to a more structured OT security assessment workflow.*

**Try OThello Assess for Free:** <https://shieldworkz.com/othello/assess>

Try your first assessment at no cost (per the current OThello Assess page; confirm terms at sign-up):  
[assess.shieldworkz.com/login](https://assess.shieldworkz.com/login)

Before you upload any documents to any tool, confirm that your data-handling and approval requirements allow it (see Section 4).

### Go deeper with Shieldworkz resources

- **Strategic Implementation of ISA/IEC 62443-3-2** (regulatory playbook): [shieldworkz.com/regulatory-playbooks](https://shieldworkz.com/regulatory-playbooks)
- **OT Security Risk Exposure Calculator Workbook** (remediation guide): [shieldworkz.com/remediation-guides](https://shieldworkz.com/remediation-guides)
- **OT Cybersecurity Threat Landscape Analysis Report 2026**: [shieldworkz.com/reports](https://shieldworkz.com/reports)
- **IEC 62443 Practical Guide for OT/ICS and IIoT security**: [shieldworkz.com](https://shieldworkz.com)
- Prefer to talk it through? **Request a demo or assessment discussion**: [shieldworkz.com/request-a-demo](https://shieldworkz.com/request-a-demo)

---

## About Shieldworkz

Shieldworkz is a specialist OT/ICS cybersecurity firm with an NDR solution and AI-based tools for securing SCADA, PLCs and Cyber Physical Systems. We serve critical infrastructure operators, industrial organisations, and government entities across the energy, oil and gas, manufacturing, utilities, transport, and defence sectors.

Our service areas include OT security assessments (powered by OThello Assess with sub-24-hour assessment cycles), NIS2 and IEC 62443 compliance programmes, OT threat intelligence advisories, OT SOC design and implementation, and regulatory readiness engagements for NCA (Saudi OTCC/ECC), NERC CIP, SOCI, and Singapore Cybersecurity Act obligations.

Reach out to us at [info@shieldworkz.com](mailto:info@shieldworkz.com) for a briefing

**NDR Solution:** [shieldworkz.com/products/ot-security-platform](https://shieldworkz.com/products/ot-security-platform) | **Media Scan:** [shieldworkz.com/products/ot-security-](https://shieldworkz.com/products/ot-security-) | **Othello Assess:** [shieldworkz.com/othello/assess](https://shieldworkz.com/othello/assess) | **Patch Management:** [shieldworkz.com/products/patch-management-solution](https://shieldworkz.com/products/patch-management-solution) | **Regulatory Playbooks:** [shieldworkz.com/regulatory-playbooks](https://shieldworkz.com/regulatory-playbooks) | **Remediation Guides:** [shieldworkz.com/remediation-guides](https://shieldworkz.com/remediation-guides) | **Reports:** [shieldworkz.com/reports](https://shieldworkz.com/reports)



# About Shieldworkz



## ISOC and Honeypot Locations

Honeypot Locations



Security Operations Center



Shieldworkz is a global OT security company founded by top industry experts to protect critical infrastructure using proprietary technology and a leading consulting platform, we partner with businesses to secure assets, networks, and programs across industries. Our services are tailored to each client's cyber risks and backed by the world's largest OT and IoT threat intelligence facility and a global research team.

## Secure Your Industrial Future

Talk to us today!



From OT security assessments covering NIS2, IEC 62443, NERC CIP and other regional requirements to an OT security platform, Shieldworkz covers all compliance and industrial cybersecurity enhancement needs. Talk to us to learn how you can enhance your security posture in 7 easy steps.

# Contact Us



## GERMANY

- 📍 Fritz-Schäffer-Street 1,  
4th floor  
Bonn, 53113, Germany
- ☎ +49 (0) 228 / 929 39210
- ✉ europe@shieldworkz.com

## CANADA

- 📍 396 Old Colony Road  
Richmond Hill,  
ON L4E 5A5 Canada
- ☎ +1 (437) 223-7770
- ✉ americas@shieldworkz.com

## UAE

- 📍 Tenth floor,  
Abu Dhabi,  
United Arab Emirates,  
FAB Business Center
- ☎ +971 56 660 5200
- ✉ middleeast@shieldworkz.com

## INDIA

- 📍 Gopalan Signature Tower,  
No 6, 2nd Floor, Old Madras  
Road, Benniganahalli  
Bengaluru,  
Karnataka 560093
- ☎ +91 9059620557
- ✉ apac@shieldworkz.com

