TXONE NETWORKS

11 Steps to Stable OT Systems Without Interrupting Production

Same-Week Action Checklist

Executive Summary

Guide 1 gave your OT team the reasoning. Guide 2 gave your IT Security Leader the architecture. This is the action list both teams share. Eleven steps. Each one completable without stopping a line. Each one with a named owner, a testable acceptance criterion, and an audit-folder evidence artifact.

Steps 1 through 5 are same-week governance moves. No procurement. No new technology. Steps 6 through 9 are 30-day technology accelerators on top of the governance baseline. Steps 10 and 11 are 60-to-90-day foundational deployments worth scheduling this week. The checklist a brewery peer would hand you with the cover note "start here."

> **22%** of OT organizations reported a cybersecurity incident in the past year, and **40%** of those caused operational disruption [1]. **19%** of incidents take more than a month to remediate fully [1].

> Sites under mandatory compliance experienced **approximately 50% fewer financial losses and safety impacts** than peers [1]. The eleven steps below are the operational reading of that finding.

How to use this checklist

Every step uses the same five-field contract:

- **Step.** One verb-forward sentence.
- **Owner.** One primary owner with decision authority, named by role. A co-signer where cross-functional sign-off is required; the primary owns the outcome.
- **Acceptance criterion.** The observable, testable outcome that says "done." A status meeting is not an acceptance criterion.
- **Evidence artifact.** The specific output that belongs in the audit folder at step close.
- **Risk of skipping.** One line, in brewery operational terms.

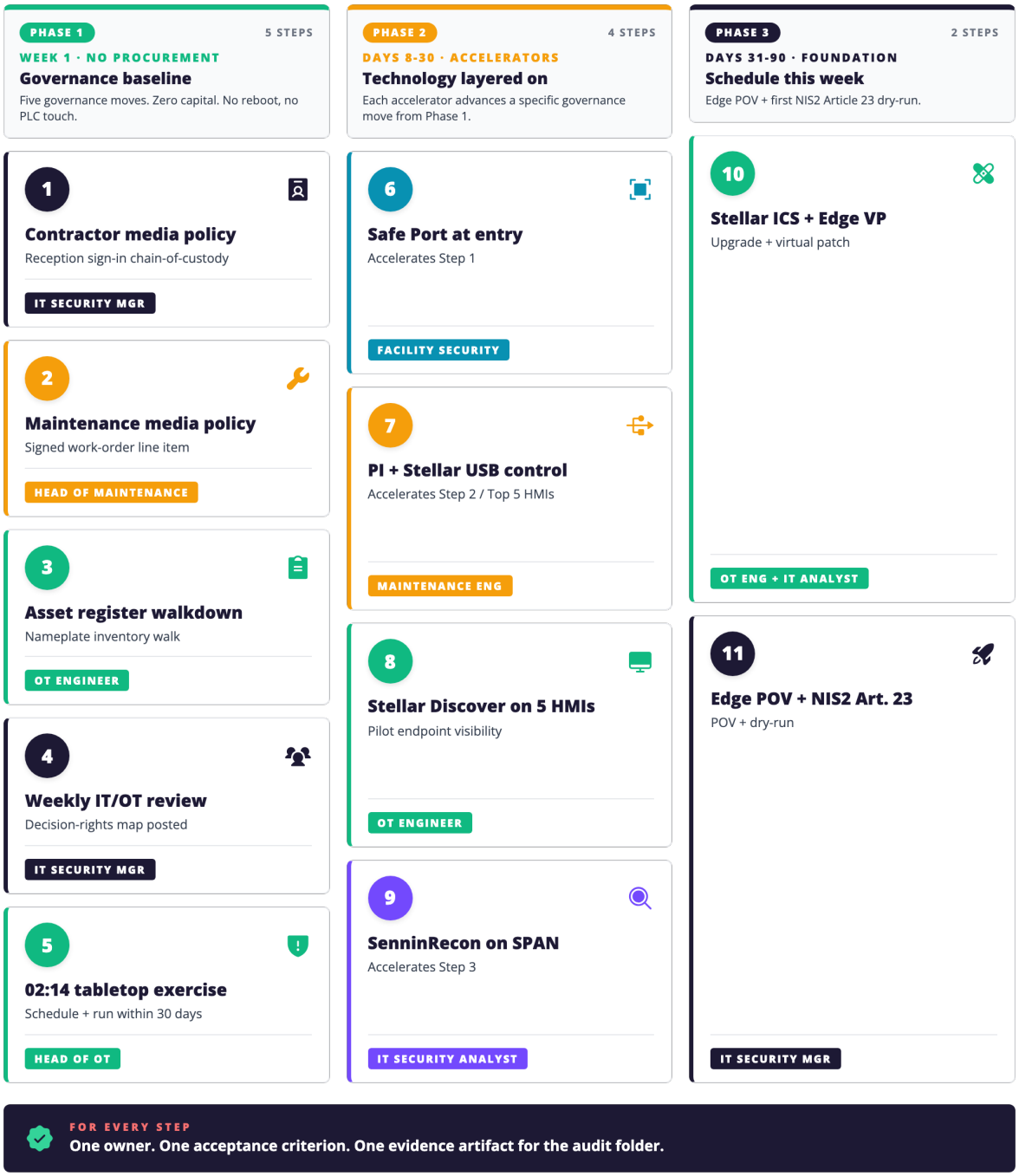
Start here, this week. The five governance steps cost nothing you do not already have and close the gaps an auditor would flag tomorrow.

Each step carries a sequencing flag and cross-references the Guide 1 Tip and Guide 2 Way it advances. Assign owners by name. Post the list on the OT Leader's wall. Recheck at the weekly IT/OT review (Step 4). Every step is completable inside one CIP maintenance window or entirely outside the line.

The 11 Steps

Governance first. Then technology. Then foundation.

Every step has one named owner, one acceptance criterion, and one evidence artifact for the audit folder.



Three phases: governance leads, technology accelerates, foundation sustains.

WEEK 1 · NO PROCUREMENT

STEP 01

Publish the contractor media policy and add it to the reception sign-in flow.

Owner (primary): IT Security Manager. **Co-signer:** Head of OT.

Acceptance criterion: policy published, signed by both owners, posted at reception. Reception sign-in carries a declared-media field (device serial, target system, time). Reception and shift supervisors briefed. First three contractor sign-ins carry the field complete.

Evidence artifact: signed policy PDF; sign-in template; first three completed declarations as chain-of-custody record.

Risk of skipping: 25% of top OT security incidents are triggered by USB plug-and-play events [2]. The undeclared device is the device the auditor will ask about.

SEQUENCING

This week. No-procurement. Brief reception on shift handover.

25%

of top OT security incidents triggered by USB plug-and-play events [2]

WEEK 1 · NO PROCUREMENT

STEP 02

Publish the maintenance-window media policy and the signed work-order line item.

Owner (primary): Head of Maintenance. **Co-signer:** IT Security Manager.

Acceptance criterion: policy published, signed, added to maintenance standard procedures. Work-order template carries a media line item (device serial, owner, target system, insertion/ removal times, two signatures). Escort rule briefed. Next three work orders close with the line complete.

Evidence artifact: signed policy PDF; updated work-order template; first three completed work orders with media line and escort signature.

Risk of skipping: 10.5% of USB-based suspicious activity in OT environments is classified as malicious USB devices [3]. The reception kiosk (Step 6) does not catch the laptop already badged in at 02:00 on a Saturday.

SEQUENCING

This week. No-procurement. Update maintenance team standard procedures.

10.5%

of USB-based suspicious activity in OT classified as malicious USB devices [3]

STEP 03

Walk the brewery and write down the asset register.

Owner (primary): OT engineer. **Co-signer:** Head of OT.

Acceptance criterion: every PLC, HMI, switch, engineering workstation, and brewhouse PC has a row in a shared spreadsheet with vendor, model, firmware, location, owner, Purdue level, primary process, and "talks to" column. Date stamped. Signed by the Head of OT. Quarterly refresh on the calendar.

Evidence artifact: signed asset register (PDF export); refresh-cadence calendar invitation.

Risk of skipping: 30% of IR cases were discovered because "something seemed wrong," not by detection tools [4]. Until the register exists, the OT team is defending assets it cannot enumerate.

SEQUENCING

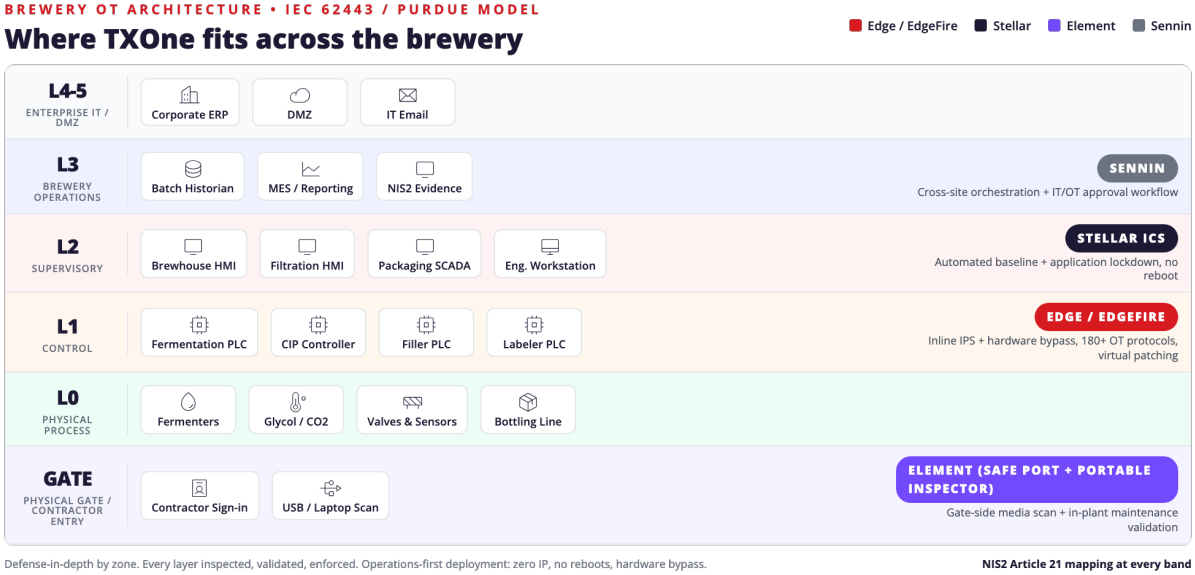
This week. Two-person walkdown completes a 50 to 200-asset site in a day or two.

30%

of IR cases discovered because "something seemed wrong"
[4]

BREWERY OT ARCHITECTURE • IEC 62443 / PURDUE MODEL

Where TXOne fits across the brewery



Walk the register by Purdue zone.

WEEK 1 · NO PROCUREMENT

STEP 04

Stand up the weekly IT/OT review and post the decision-rights map.

Owner (primary): IT Security Manager. **Co-chair:** Head of OT.

Acceptance criterion (week 1): a recurring 30-minute IT/OT review is on both calendars with named site attendees. Standing agenda published (open incidents, planned maintenance, pending vulnerabilities, NIS2 evidence-folder status, step-list progress). Decision-rights map (segmentation rule changes, endpoint policy changes, emergency stops) signed and posted. **By day 21:** three consecutive reviews held with notes captured.

Evidence artifact: notes from the first three reviews; signed decision-rights map; recurring calendar invitation.

Risk of skipping: 33% of security incidents occur at IT/OT integration points [5]. Without a standing handoff, the IT/OT boundary is negotiated in ad-hoc calls during incidents instead of designed in advance.

SEQUENCING

Cadence in place this week. Notes captured at every review.

33%

of security incidents occur at IT/OT integration points [5]

WEEK 1 · NO PROCUREMENT

STEP 05

Schedule and run the first brewery tabletop on the 02:14 scenario.

Sequencing: schedule this week, run within 30 days. No procurement.

Owner (primary): Head of OT. **Co-signer:** IT Security Manager.

Acceptance criterion: a 90-minute tabletop is on the calendar with production lead, maintenance engineer, IT security analyst, SOC representative, quality lead, and legal advisor confirmed. Scenario: ransomware on the bottling line during a Saturday CIP window, delivered via contractor USB. Runs within 30 days. Outcomes recorded: time-to-contain, time-to-notify, time-to-restore.

Evidence artifact: calendar invitation with confirmed attendees; after-action report; updated runbook; RACI snapshot.

Risk of skipping: 88% of tabletop exercises reveal degraded detection capability [4]. Just 14% of OT organizations felt fully prepared for emerging threats [1]. The first time you run the scenario should not be at 02:14 on a real Saturday.

SEQUENCING

Schedule this week. Run within 30 days. Re-run quarterly.

88%

of tabletop exercises reveal degraded detection capability [4]

STEP 06

Install Safe Port at the facility entry to convert the contractor-media policy into a structured event stream.

Sequencing: 30 days. Technology accelerator on Step 1.

Owner (primary): Facility security lead or reception supervisor. **Co-signer:** IT Security Analyst (SIEM forwarding).

Acceptance criterion: kiosk powered, networked, integrated into reception sign-in. At least five visitor devices scanned in the first operational day. LED pass/fail visible from the desk. Scan results forward into the IT SIEM.

Evidence artifact: ElementOne scan log (PDF); SIEM forwarding configuration screenshot.

Risk of skipping: Step 1's policy deters but does not enforce. The kiosk closes the gap without adding security-team headcount.

TECHNOLOGY ACCELERATOR

Layers Safe Port over the Step 1 policy. Powered, networked, integrated into reception within 30 days.

7,200

files per minute scanned by Safe Port at the gate

10

STEP 07

Put a Portable Inspector in every maintenance kit and turn on Stellar USB device control on the top 5 HMIs.

Sequencing: 30 days. Technology accelerator on Step 2.

Owner (primary): Maintenance engineer. **Co-signer:** IT Security Analyst.

Acceptance criterion: every maintenance kit contains one Portable Inspector. The last three work orders since deployment closed with a "media scanned" line alongside the Step 2 signed-log line. Stellar USB device control enabled on the top 5 HMIs; only approved-list devices can mount; unknown-device attempts produce a block event in the Stellar log.

Evidence artifact: work-order close-outs with media-scan line; Portable Inspector scan reports; Stellar device-control policy PDF; first week of block-event logs.

Risk of skipping: 81.9% of USB-based suspicious activity in OT environments is file transfers [3]. Step 2 catches the routine case; Stellar USB control catches the laptop that bypassed it; Portable Inspector catches the device that has not been to the kiosk yet.

TECHNOLOGY ACCELERATOR

Layers Stellar USB control + Portable Inspector over the Step 2 maintenance-window policy.

81.9%

of USB-based suspicious activity in OT environments is file transfers [3]

STEP 08

Deploy Stellar Discover on 5 pilot HMIs to validate compatibility before commitment.

Sequencing: 30 days. Technology accelerator (no governance prerequisite).

Owner (primary): OT engineer assigned to the pilot brewery. **Co-signer:** IT Security Analyst.

Acceptance criterion: Stellar Discover sensors run on 5 HMIs. Each installed in 1 minute, zero reboots, zero operator-reported stability issues. First asset-health assessment report delivered to the OT Leader.

Evidence artifact: StellarOne assessment PDF (software inventory, USB activity, active malware status).

Risk of skipping: 100% of surveyed organizations operate legacy Windows in OT; 51% of European organizations had a legacy Windows incident in the past 12 months [6]. Until Discover is on these HMIs, the OT team cannot see software-level activity on the assets it is defending.

TECHNOLOGY ACCELERATOR

1-minute install per HMI. Zero reboot. Compatibility validation before any ICS upgrade.

100%

of surveyed organizations operate legacy Windows in their OT environment [6]

STEP 09

Run SenninRecon on one SPAN port to overlay live discovery on the manual asset register.

Sequencing: 30 days. Technology accelerator on Step 3.

Owner (primary): IT security analyst.

Acceptance criterion: SenninRecon receiving mirrored traffic from at least one segment (ideally IT/OT DMZ). First asset inventory report produced. VSAR scoring ranks the top 10 vulnerabilities by operational context. Zero agents, zero inline deployment, zero PLC touches. Output reconciled against the Step 3 register; gaps recorded and assigned in the IT/OT review (Step 4).

Evidence artifact: SenninRecon asset inventory; VSAR top-10 list (PDF); reconciliation note against the Step 3 register.

Risk of skipping: 67% of OT teams struggle with unified IT/OT visibility [5]. The manual register ages between refreshes; SenninRecon keeps it current and surfaces vulnerabilities the walkdown cannot.

TECHNOLOGY ACCELERATOR

Layers SenninRecon over the Step 3 manual register. Zero agents. Zero inline. Zero PLC touches.

67%

of OT teams struggle with unified IT/OT visibility [5]

60 TO 90 DAYS · FOUNDATIONAL

STEP 10

Upgrade Discover-validated endpoints to Stellar ICS, and virtual-patch one exposed controller via Edge.

Owner (primary): OT engineer (Stellar) and IT Security Analyst (Edge virtual patching). **Co-signer:** Head of OT (operator sign-off on the Stellar upgrade).

Acceptance criterion: every Step-8 Discover-validated endpoint has been upgraded to Stellar ICS via one-click remote activation from StellarOne, typically under 5 minutes per endpoint with no local engineer and no reboot. Zero production interruption. Pilot-brewery shift supervisor has signed off operations unchanged. A virtual-patch rule is active on Edge for the highest-priority unpatched controller; the blocked-exploit counter is non-zero or demonstrably tested via red-team verification; the vulnerability moves from "open" to "compensating-control-active" in the NIS2 vulnerability register.

Evidence artifact: StellarOne upgrade audit log; signed operator sign-off; EdgeIPS policy file; CVE-to-rule mapping; one week of traffic log showing block count or test record.

Risk of skipping: Stellar Discover reports activity; Stellar ICS stops it. **26% of CISA ICS advisories offered no patch and 18% had no patch and no documented mitigation** [7]; the unpatched controller during peak season is the textbook reason virtual patching exists.

FOUNDATIONAL

Stellar ICS upgrade in under 5 minutes per endpoint, no reboot. Edge virtual patch on the highest-priority unpatched controller.

26% / 18%

of CISA ICS advisories had no patch / no patch and no mitigation

[7]

60 TO 90 DAYS · FOUNDATIONAL

STEP 11

Run the 60-minute Edge POV on the highest-risk conduit, then run the NIS2 Article 23 tabletop dry-run.

Owner (primary): IT Security Manager. **Co-signer (Article 23):** Legal counsel. **Readiness sign-off:** Business Leader.

Acceptance criterion: a 60-minute Proof of Value on EdgeIPS has completed at the highest-risk conduit; live traffic observed; policies applied; hardware-bypass demonstrated on a controlled test. POV report confirms inline blocking; OT engineer countersigned zero operational impact. Within the same window, the NIS2 Article 23 dry-run has run with production, OT, IT security, SOC, quality, legal, and communications. The scenario exercises all three Article 23 reporting windows (24-hour early warning, 72-hour notification, 1-month final report). First-pass drafts of each report produced with evidence from the Sennin-to-SIEM pipeline. Results and gap list recorded.

Evidence artifact: EdgeOne POV report; OT engineer sign-off; go/no-go memo for the first production Edge deployment; Article 23 readiness report; the three reporting-window draft templates; open-gap list.

Risk of skipping: 82% of observed attacks abuse exposed VNC clients on internet-facing CPS assets [8]; without inline enforcement at the conduit, detection remains documentation. NIS2 administrative fines for essential entities reach the higher of **€10 million or 2% of global annual turnover**; for important entities, **€7 million or 1.4%** (NIS2 Directive (EU) 2022/2555, Article 34). The first time you run the Article 23 timeline should not be during the real incident.

NIS2 ARTICLE 23

60-minute Edge POV plus Article 23 dry-run inside the same 60-90 day window. The rehearsal that surfaces the gaps is the gating item.

82%

of observed attacks abuse exposed VNC clients on internet-facing CPS assets [8]

How Carlsberg runs a version of this list

Context. Carlsberg Group, originating in Denmark. A global brewing company with 140+ brands. OT security treated as a distinct discipline from IT.

Challenge. Close the legacy endpoint coverage gap (Windows XP HMIs on packaging lines, and similar) where enterprise EPP fell short, without operational disruption. Multi-site scale: replacing the lines was financially infeasible at millions of euros per line.

Response. TXOne Stellar deployed via a third-party service partner roughly three years ago. Stellar analyzes the processes running on each asset and locks them in place; no active scanning. Phased, region-by-region rollout. The governance equivalents of Steps 1 through 5 were already in place.

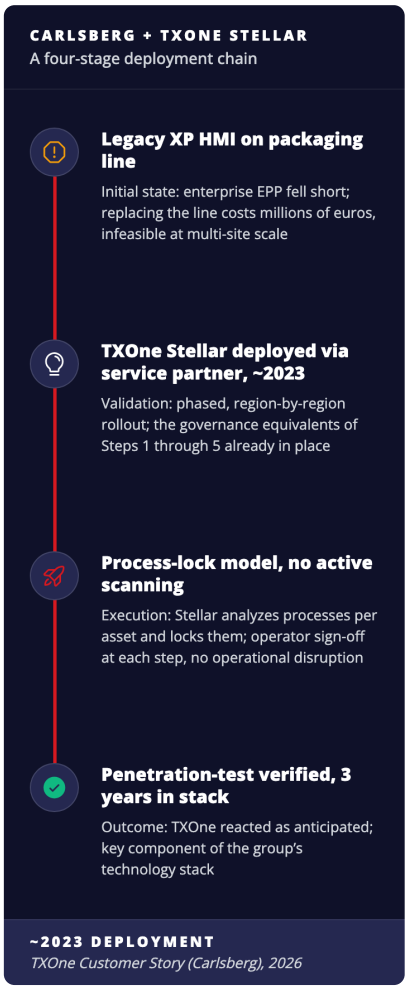
Result. A penetration test at one brewery confirmed the technology reacted as anticipated. Stellar is now a key component of the group's technology stack.

> **"TXOne Networks gives me confidence that it won't disrupt my operations." — Chris Thompson, Director of Brewery OT Security, Carlsberg Group** [9]

The most audit-defensible action was the simplest: a Stellar agent that locks the processes already running on each legacy asset, without active scanning, without an enterprise EPP rollout. The most underrated action was the work that came before it: the policies, the asset register, and the IT/OT cadence that gave the deployment somewhere to land.

3 yrs

TXOne Stellar in Carlsberg's group technology stack; legacy endpoint coverage where enterprise EPP fell short [9]



Carlsberg: Stellar locks the processes, without active scanning.

What you will have produced

The audit folder fills in three checkpoints. Day 7 carries the brewery if the auditor arrives early; Day 30 and Day 90 carry the next program review. Each column below is cumulative.

DAY 7 / 30 / 90 AUDIT FOLDER

What is in the audit folder at each milestone

Evidence accumulates. Each column is cumulative: Day 30 includes Day 7. Day 90 includes Day 30.

DAY 7 STEPS 1-5 CLOSED

Same-week evidence

- **ElementOne scan log**
  Safe Port kiosk scan log (PDF) with timestamps, device types, pass/fail per visitor device.
- **Portable Inspector reports**
  Per-device scan reports plus AES-256 chain-of-custody logs (PI Pro kits) and work-order close-outs with "media scanned" line item.
- **StellarOne pilot assessment**
  PDF covering 5 HMIs: software inventory, USB activity, active malware status.
- **SenninRecon asset inventory**
  Segment asset report plus VSAR top-10 vulnerability list exported as PDF. Zero agents installed.
- **USB device-control policy**
  Stellar policy file plus first week of block-event logs from the 5 HMIs.

DAY 30 STEPS 6-9 CLOSED

Day 7 + foundations

- **StellarOne upgrade audit**
  One-click Discover-to-ICS upgrade log for every validated endpoint plus shift-supervisor sign-off that operations are unchanged.
- **Virtual-patch artifacts**
  EdgeIPS policy file, CVE-to-rule mapping, one week of traffic log with block count or red-team test record.
- **Tabletop after-action**
  02:14 ransomware scenario after-action report plus RACI snapshot plus updated incident response runbook.
- **IT/OT review minutes**
  Three consecutive weekly review minutes plus VSAR priority list at each review.

DAY 90 STEPS 10-11 CLOSED

Day 30 + deployment

- **EdgeOne POV report**
  60-minute Proof of Value report plus OT-engineer-countersigned zero-operational-impact statement.
- **Edge go/no-go memo**
  First production Edge deployment go/no-go memo, signed by IT Security Manager and Head of OT.
- **NIS2 Article 23 readiness**
  120-minute Article 23 tabletop report covering 24-hour, 72-hour, and 1-month reporting windows.
- **Article 23 draft templates**
  First-pass drafts of all three reporting-window forms, extracted from the Sennin-to-SIEM pipeline plus open-gap list.

AT DAY 90

Audit-ready evidence for NIS2 Article 21 (asset management, incident handling, supply chain, business continuity, vulnerability management) and Article 23 (reporting readiness). Zero operational interruption caused by the steps.

At Day 90 the brewery holds an audit-ready evidence set for NIS2 Article 21 (asset management, incident handling, supply chain, business continuity, vulnerability management) and Article 23 (reporting readiness). Zero operational interruption caused by the steps.

Take the Next Step

- **Primary:** book a 60-minute brewery readiness review. A TXOne OT specialist will walk one cell of one brewery with the OT Leader, assign the first three step owners, and get Steps 1 through 5 on the wall this week.
- **Secondary:** share Guide 1 with the OT Leader for the full reasoning behind these steps: "11 Practical Tips for Breweries to Avoid Production Downtime Due to OT Risks."
- **Tertiary:** share Guide 2 with the IT Security Leader for the NIS2 and IEC 62443 architecture behind these steps: "11 Proven Ways IT Managers in Breweries Secure Production."

Ready to run the checklist?

Contact your TXOne Networks partner or visit txone.com to schedule a 60-minute brewery readiness review.

Book a Brewery Readiness Review

The first five steps can be finished inside this week. They cost nothing you do not already have, and they close the loudest gaps an auditor would flag tomorrow. Steps 6 through 9 are the technology layer that accelerates them. Steps 10 and 11 are the foundation everything else sits on. In that order.

Sources

1 SANS State of ICS/OT Security Survey, 2025.

2 Honeywell 2025 Cyber Threat Report.

3 Nozomi Networks 1H 2025 OT/IoT Security Report, p. 22.

4 Dragos 9th Annual OT/ICS Cybersecurity Year in Review, 2026.

5 TXOne Networks / Omdia OT Security Survey, 2023.

6 TXOne Legacy OT Cybersecurity Report, 2026.

7 Gartner CPS Security Requires Specialized Vulnerability and Patch Management, 2025, citing Claroty.

8 Claroty Team82 Threat Intelligence Report, 2026, p. 5.

9 TXOne Customer Story (Carlsberg), 2025.

10 TXOne Product Documentation, 2026.

About TXOne Networks

TXOne Networks specializes in OT-native cybersecurity for critical infrastructure and industrial control systems. Our solutions are deployed across energy, manufacturing, water, food and beverage, and transportation sectors globally.

As the operations-first OT security partner, TXOne helps industrial organizations protect critical operations, securely extend asset life, and build security programs without operational disruption. This guide is part of the European Brewery OT Security series.

Visit txone.com

© 2026 TXOne Networks, Inc. All rights reserved. TXOne and the TXOne logo are trademarks of TXOne Networks. Claroty, Dragos, Honeywell, and Nozomi Networks are trademarks of their respective owners. All external statistics remain the property of their respective publishers (Claroty, Dragos, Gartner, Honeywell, Nozomi Networks, Omdia, SANS); they are cited here for illustrative reference and are not reproduced in full. Gartner does not endorse any vendor referenced in this e-book. NIS2 Directive (EU) 2022/2555 reproduced under EU public-document conventions. This document is for informational purposes only.