The OT Cyber Readiness Checklist

How resilient is your pharma OT environment?

In the world of pharma production, protection reigns supreme.
From external threat actors to internal legacy infrastructure, securing systems and shopfloors remains mission critical. But OT cybersecurity isn't just about protecting assets. It's about safeguarding product integrity, ensuring regulatory compliance and preserving public trust.

The question is: **how ready are you?**

Helping OT and cybersecurity leaders assess the maturity of their current approach across five critical focus areas, this readiness checklist will give you the answer. Identify strengths and critical improvement areas as you score your current OT security posture—and prioritise your next strategic initiative.

How it works

Read each statement and score your current readiness on a scale of **0–3**:

- **0** Not in place
- **1** Planning stage
- **2** Partially implemented
- **3** Fully implemented

At the end of each section, total your score and review your resilience level.

Downtime & Operational Resilience

Why it matters: Unplanned OT downtime can halt batch production, trigger costly revalidations and delay patient access to potentially life-saving treatments. This section assesses how prepared your organisation is in minimising disruption and recovering at speed.

Statement	Score (0–3)
We have mapped our OT systems and identified critical assets most vulnerable to downtime.	
We have real-time visibility into OT operations and system performance.	
We have incident response plans that include coordinated OT-specific playbooks.	
We monitor and test our downtime recovery processes regularly.	

Subtotal	Score ___/12

Resilience Level:

- **0–4** Reactive
- **5–8** Developing
- **9–12** Operationally Resilient

Legacy System Risk Mitigation

Why it matters: Pharmaceutical manufacturing relies on legacy systems that can't be easily replaced; nor do they necessarily need to be with the right solutions in place. Securing these assets without disrupting validated processes is critical for sustained compliance and uptime. This section explores your ability to manage legacy systems while driving future innovation, without compromising security standards.

Statement	Score (0-3)
We maintain a full inventory of legacy systems running unsupported or soon-to-be-unsupported software (e.g. Windows 10).	
We have compensating security controls in place to protect vulnerable endpoints.	
We segment legacy systems from wider networks wherever possible.	
We segment legacy systems from wider networks wherever possible.	

Subtotal **Score ___/12**

Resilience Level: **0–4** At risk **5–8** Improving **9–12** Secure and Sustained

Regulatory & Compliance Readiness

Why it matters: With directives such as NIS2 and GMP Annex 11 raising the bar on OT accountability, proactive compliance is no longer optional. It's business critical. This section evaluates your ability to demonstrate control, traceability and audit readiness.

Statement	Score (0-3)
We meet the requirements of EU GMP Annex 11 and NIS2 for OT and IT systems.	
We can demonstrate clear separation between validated and non-validated systems.	
We conduct regular internal audits and are prepared for third-party scrutiny.	
We can produce compliance reports showing visibility, control, and traceability of system access and changes.	

Subtotal **Score ___/12**

Resilience Level: **0–4** Exposed **5–8** Compliance-aware **9–12** Audit-ready

Product Integrity & Patient Safety

Why it matters: Tampered dosing, mislabelled packaging or contaminated batches can erode public trust and put lives at risk, both for employees and end users. This section ensures that cyber resilience is directly supporting your production quality and patient safety goals.

Statement	Score (0-3)
We understand how OT system compromise could affect drug formulation, contamination risk, or packaging accuracy.	
We have measures in place to detect and prevent data tampering in production environments.	
We've implemented end-to-end integrity checks on batch production data.	
We regularly train staff on the cybersecurity risks that could impact patient safety.	

Subtotal **Score ___/12**

Resilience Level: **0–4** Vulnerable **5–8** Aware **9–12** Trusted and transparent

Security Architecture & Endpoint Protection

Why it matters: Strong OT security depends on visibility, segmentation and tailored controls at every network edge. This section focuses on the core technical capabilities that support continuous protection across your OT environment.

Statement	Score (0-3)
We have adopted OT-native security tools purpose-built for industrial environments.	
Our security architecture follows Zero Trust principles across both IT and OT.	
We've secured remote and third-party access points into OT systems.	
Our endpoint protection includes host-based intrusion prevention (HIPS) capabilities without disrupting operations.	

Subtotal **Score ___/12**

Resilience Level: **0–4** Fragmented **5–8** Baseline Secure **9–12** Proactively Managed

Your Total Score	Score ___/60

0–15	Critical Risk	Your OT environment is highly vulnerable to threats. Foundational capabilities are missing and downtime, compliance breaches or integrity failures are likely. Immediate action is required.
16–30	Developing	Some progress has been made but significant gaps remain—especially around your legacy systems, visibility and regulatory readiness. There's a clear exposure threat that requires a structured improvement plan.
31–45	Baseline Secure	Core controls are in place and some risk mitigation is evident. However, your general resilience is inconsistent and could be undermined by evolving threats or audits. Now is the time to commit to strengthening and scaling proactive defences.
46–55	Operationally Resilient	Core controls are in place and some risk mitigation is evident. However, your general resilience is inconsistent and could be undermined by evolving threats or audits. Now is the time to commit to strengthening and scaling proactive defences.
56–60	Trusted Leader	You're achieving best-in-class OT cyber resilience. Your posture is proactive, as regulatory-proof as it can be and tightly integrated across people, process and technology. You're a model for secure pharmaceutical operations. Congratulations.

Want to go deeper?

Download our eBook on **'Prescribing Cyber Resilience'** or speak with a TXOne expert to map your next steps to OT readiness.

Download