OT SECURITY READINESS

OT Security Readiness Checklist

23 audit points to evaluate the security maturity of your industrial OT environment — organized around the six controls that most reduce cyber financial loss.

Top 6 Effective OT Cyber Controls · **DeRISK Platform**

Work through each point. Mark the checkbox for every YES, then total your score using the guide at the end. Points marked ◆ are cyber risk quantification signals — gaps here are leading drivers of financial loss in an OT cyber incident.

FOUNDATION

Governance & Asset Visibility

☐ **F1** Does the organization have a documented, ICS/OT-specific cybersecurity policy, separate from the IT security policy?

◆ ***Cyber risk quantification signal:*** *Absence of an OT-specific policy is a leading indicator of governance gaps across every other control area.*

☐ **F2** Is a single accountable role at enterprise level responsible for ICS/OT cyber risk, with critical security functions (patching, access control, monitoring, incident response) formally assigned to specific roles?

◆ ***Cyber risk quantification signal:*** *Role clarity directly affects mean time to detect and contain — two primary drivers of loss magnitude.*

☐ **F3** Has a formal asset inventory been completed for all ICS/OT cyber assets — controllers, RTUs, HMIs, historian servers?

◆ ***Cyber risk quantification signal:*** *Asset count and discovery maturity are foundational to modeling financial exposure; you cannot protect or quantify what you cannot see.*

☐ **F4** Is physical access to OT environments controlled and monitored through cameras, guards, or a Security Operations Center?

CONTROL 1

Defensible Architecture

☐ **A1** Is the ICS/OT network logically segmented from the corporate IT network, with a DMZ architected between them?

◆ ***Cyber risk quantification signal:*** *IT/OT segmentation is the highest-impact single control for limiting lateral movement — it directly reduces modeled blast radius.*

☐ **A2** Is an electronic perimeter enforced with controlled access points (firewalls and/or data diodes) governing all ingress and egress, and are control-, safety-, and configuration-related data flows identified and audited?

☐ **A3** Has the basic process control system (BPCS) been segmented and separated from the safety instrumented system (SIS)?

CONTROL 2

Secure the Perimeter & External Access

- ☐ **P1** Have all connectivity points, remote-access paths, and conduits into the ICS/OT system been visually inspected and documented within the last 12 months?
  ◆ ***Cyber risk quantification signal:*** *Undocumented access points are unmodeled attack paths — they inflate uncertainty in quantified exposure.*

- ☐ **P2** Are direct remote-access protocols (RDP, VNC, Telnet, SSH) blocked from internet exposure, with remote access permitted only through a secure intermediary (VPN/DMZ) that enforces MFA and terminates in the DMZ rather than on OT assets?
  ◆ ***Cyber risk quantification signal:*** *Internet-exposed remote access is the most common initial-access vector in documented OT incidents.*

- ☐ **P3** Is identity and access management enforced (unique identities, least privilege), with default passwords changed on all ICS/OT assets and administrative credentials separated from day-to-day operational credentials?

- ☐ **P4** Is there an authorization process for all transient devices (laptops, USB drives, portable media) before connection to ICS/OT networks?

- ☐ **P5** Is the percentage of end-of-life ICS/OT assets (no vendor support, no patch availability) known, tracked, and actively reduced through prioritized remediation or compensating controls?
  ◆ ***Cyber risk quantification signal:*** *End-of-life assets expand unpatched attack surface and vulnerability exposure in loss models.*

CONTROL 3

Secured Data & Configuration Backups

- ☐ **B1** Are ICS/OT system and data backups scheduled, encrypted, stored offsite, and immutable so they survive a ransomware attack?

- ☐ **B2** Are backups restoration-tested at least annually for each asset type, with a documented last-known-good configuration baseline (including critical configs and security data such as Active Directory, certificates, and license keys)?

CONTROL 4

Logging, Monitoring & IR/DR

- ☐ **L1** Is logging and auditing enabled, retained, centralized, and protected from tampering on all OT assets that support it?

- ☐ **L2** Are network communications monitored for industrial protocols (Modbus, DNP3, PROFINET) in addition to standard IT traffic, with endpoint detection and response (EDR) deployed on supported OT workstations and servers?
  ◆ ***Cyber risk quantification signal:*** *Without OT protocol monitoring, rogue control commands go undetected — a key scenario in ransomware-pivot attacks.*

- ☐ **L3** Are OT-specific incident response (IR) and disaster recovery (DR) plans documented, rather than relying on IT-only playbooks?

☐ **L4** Are mean time to detect (dwell time) and mean time to contain measured and tracked against defined targets?

◆ ***Cyber risk quantification signal:*** *Dwell time and containment time are primary drivers of loss magnitude — longer dwell means a larger blast radius, and slower containment extends downtime and third-party response costs.*

CONTROL 5

Harden Shared Infrastructure

☐ **S1** Have shared and intermediary services (Active Directory, IAM, PKI, DNS, NTP, virtualization, remote-access services) been identified and hardened under a high-security policy — continuous vulnerability scanning, prioritized patching, and disabled weak ports, services, and protocols?

◆ ***Cyber risk quantification signal:*** *The majority of OT attacks are detectable in shared intermediary systems; hardening them shrinks the window before detection.*

☐ **S2** For higher-security environments, is application whitelisting (AWL) deployed on intermediary and DMZ assets?

CONTROL 6

IT–OT Dependency & Failure Resilience

☐ **D1** Has a Crown Jewels assessment been completed, identifying assets whose compromise produces the highest operational and financial impact?

◆ ***Cyber risk quantification signal:*** *Crown Jewels mapping is required to model worst-case scenario financial loss accurately.*

☐ **D2** Has a business impact assessment (BIA) and system-of-systems dependency analysis been performed to identify where OT relies on IT services?

☐ **D3** Has OT been validated, through testing, to operate safely in isolation or a degraded mode during an IT-network attack, and under manual control during a direct OT attack?

◆ ***Cyber risk quantification signal:*** *Validated OT isolation caps production downtime — the largest single loss component in many OT incidents.*

HOW TO INTERPRET YOUR SCORE

Score one point for each YES across all 23 items.

19–23 YES	**Strong baseline —** Most controls in place. Proceed to a full quantified risk assessment.
12–18 YES	**Moderate gaps —** Meaningful exposure remains. Prioritize the unchecked items — especially segmentation, remote access, and backups.
0–11 YES	**Significant exposure —** More than half of controls are missing. Immediate review recommended.

Any unchecked ◆ item carries disproportionate weight. These map to the controls our research identifies as the most effective at reducing OT cyber financial loss — a gap in any of them is a material loss driver in an OT cyber incident.