

OT Cyber Risk Starter Assessment

Riverton Precision Components

Fictional U.S. precision manufacturer | ~180 employees | One production facility

SAMPLE REPORT - FICTIONAL ORGANIZATION - DEMONSTRATION DATA

42 / 100	ESTABLISHED	CRITICAL
OT Cyber Readiness Score	Readiness Band	Critical Risk Status

Assessment basis: Self-reported - Unverified

Assessment version: Starter demonstration profile v1.0

Scoring engine: Indurevia v1.0.0

OT Cyber Risk. Operational Resilience.

This sample illustrates the type of prioritized, customer-facing output produced by the Indurevia Starter Assessment. It is not a penetration test, vulnerability scan, certification, compliance audit, or independent validation of controls.

01 Executive Summary

Riverton Precision Components achieved an OT Cyber Readiness Score of **42/100 (Established)**. The assessment indicates that foundational cybersecurity practices are present, including basic system hardening, backup practices, network separation, and some security logging. However, several OT-specific controls remain inconsistently implemented.

More importantly, the assessment identified **three compound Critical risks** involving remote access, OT visibility, and incident response. These risks arise from combinations of control weaknesses that may create greater operational exposure than any individual deficiency considered alone.

Priority message: Improve remote-access governance, OT asset visibility and monitoring, and OT-specific incident response before pursuing broader maturity improvements.

What the score means

The readiness score reflects maturity across the applicable assessment questions. The Critical Risk Status is separate: it highlights high-consequence combinations of weaknesses that deserve attention even when the overall maturity score is higher.

Compound Critical Risks	3	Compound High Risks	1
Applicable Questions	25	Readiness Band	Established

02 Readiness by Domain

Domain	Score	Band
Governance	58%	Established
Asset Visibility	38%	Developing
Network & Access	35%	Developing
System & Account Protection	50%	Established
Monitoring	33%	Developing
Incident Response	33%	Developing
Backup & Recovery	50%	Established

Interpretation

Riverton's strongest areas are Governance and basic System/Account Protection and Backup/Recovery practices. The most material maturity gaps are concentrated in Monitoring, Incident Response, Network/Access governance, and Asset Visibility. These weaknesses interact with one another, which is why the compound-risk analysis elevates several issues to Critical.

03 Framework Alignment

Indurevia uses established OT cybersecurity guidance to organize the assessment and recommendations. The mappings below are informative alignments, not certifications or assertions of control equivalence.

Priority Area	NIST CSF 2.0 Alignment	NIST SP 800-82 / OT Theme
Remote access governance	PR.AA, PR.PS	Remote access control; least privilege; protected access paths
Asset visibility & monitoring	ID.AM, DE.CM	Asset identification; network monitoring; detection
OT incident response	RS.MA, RS.CO	Incident procedures; roles; communications and escalation
Vulnerability management	ID.RA, PR.PS	Risk-based patching; compensating controls; vendor guidance
Recovery dependencies	RC.RP	Backup, restoration, recovery sequencing and operational dependencies

Additional reference points may include CISA Cross-Sector Cybersecurity Performance Goals and selected IEC 62443 concepts where useful to the recommendation. Indurevia's framework references are intended to help customers understand direction and priority; they do not represent certification, attestation, or formal compliance determination.

04 Top Five Priority Findings

1. Uncontrolled Remote Access	CRITICAL
Observed condition Multiple remote-access methods are not centrally governed, MFA is not consistently required, and third-party access is not strongly controlled.	
Recommended action Inventory every OT remote-access pathway. Remove unnecessary access and prioritize MFA, controlled jump/access paths, least privilege, logging, and periodic review.	
2. Blind OT Environment	CRITICAL
Observed condition The OT asset inventory is incomplete while network/security monitoring coverage is limited, reducing confidence in what is connected and what activity is occurring.	
Recommended action Establish a baseline OT asset inventory and monitoring coverage for critical segments. Reconcile observed assets against the inventory.	
3. Incident Response Breakdown	CRITICAL
Observed condition OT-specific response procedures and roles are immature, and alert review/escalation is not formally established.	
Recommended action Define OT-specific response procedures, decision authority, escalation paths, and communications across operations, engineering, IT/security, management, and relevant third parties.	
4. Vulnerability Exposure	HIGH
Observed condition OT vulnerability and patch management is largely reactive, while the incomplete asset baseline makes it harder to determine exposure consistently.	
Recommended action Establish a trustworthy OT asset baseline, then implement a risk-based vulnerability process covering identification, vendor guidance, patch evaluation, compensating controls, and documented risk decisions.	
5. Recovery Dependencies & Sequencing	HIGH
Observed condition Backups exist, but recovery dependencies, acceptable downtime, and restoration sequencing are not sufficiently documented.	
Recommended action Document critical production dependencies, define acceptable downtime, establish recovery order, and validate restoration procedures through controlled testing.	

05 Recommended 30-Day Actions

The first 30 days should reduce the most immediate exposure and establish reliable visibility. These actions are prioritized for operational practicality rather than theoretical completeness.

1. Inventory remote access

Identify VPNs, remote desktop paths, vendor tools, cellular/modem access, cloud gateways, jump hosts, and other mechanisms that can reach OT.

2. Require stronger remote-access controls

Prioritize MFA and named accounts for remote access where technically feasible; remove dormant or unnecessary pathways.

3. Establish an OT asset baseline

Create or reconcile an inventory of critical PLCs, HMIs, robots, drives, engineering workstations, servers, network devices, and other production-connected assets.

4. Define OT incident contacts

Document who makes containment decisions, who contacts production leadership, and how IT/security, engineering, operations, and vendors coordinate.

5. Identify critical recovery dependencies

Document which systems must be restored first and what network, identity, application, configuration, and vendor dependencies are required.

06 Recommended 90-Day Roadmap

Timeframe	Objective	Practical outcome
Days 1-30	Contain immediate exposure	Remote-access inventory; stronger authentication; initial OT asset baseline; incident con
Days 31-60	Improve visibility and governance	Expand monitoring on critical OT segments; document permitted IT/OT pathways; forma
Days 61-90	Validate response and recovery	Run an OT incident tabletop; test selected restorations; document recovery sequence; r

Suggested success measures

- All known OT remote-access paths have an owner and documented business purpose.
- Critical OT assets have a reconciled baseline inventory.
- Critical OT network areas have defined monitoring coverage and alert ownership.
- OT incident roles and escalation paths have been exercised at least once.
- At least one representative critical restoration has been tested and recovery sequencing documented.

07 Existing Strengths to Build On

Basic system hardening

Default credentials are generally changed and baseline hardening occurs.

Backup practices

Backups exist for many important systems and configurations.

Network separation

IT and OT are separated at a basic level, providing a foundation for more deliberate segmentation.

Security logging

Some OT systems generate useful security logs that can support expanded monitoring.

General security awareness

The organization already has general security-awareness practices that can be extended to OT-specific scenarios.

Why this matters: Riverton does not need to build an OT cybersecurity program from zero. The recommended roadmap focuses first on connecting and strengthening existing practices around the risks most likely to affect operational resilience.

08 Methodology & Important Limitations

The Indurevia Starter Assessment is a structured, questionnaire-based OT cybersecurity readiness assessment. Responses are scored using a deterministic maturity model, domain scoring, question-level priority logic, and compound-risk rules designed to surface combinations of weaknesses that may create elevated operational exposure.

This Starter report is based on information supplied through the assessment. Unless otherwise stated, responses are **self-reported and unverified**. Indurevia does not connect to the customer's network, install software, scan production systems, perform penetration testing, or independently validate technical controls as part of the Starter Assessment.

Scores and recommendations are decision-support information. They should be considered alongside operational requirements, safety constraints, vendor guidance, system criticality, change-management requirements, and qualified technical judgment before implementation.

Framework references are informative alignments intended to help organize improvement work. They do not constitute certification, attestation, regulatory advice, or a formal compliance determination.

Indurevia

OT Cyber Risk. Operational Resilience.

support@indurevia.com

SAMPLE REPORT - FICTIONAL ORGANIZATION - DEMONSTRATION DATA

Ready to assess your own OT environment?

Complete the Indurevia Starter OT Cyber Risk Assessment to receive your organization's prioritized readiness report and 30/90-day improvement roadmap.

Starter Assessment | \$149

25 questions • Seven OT domains • About 10 minutes

No network connection, scanning, or software installation required.

www.indurevia.com

OT Cyber Risk. Operational Resilience.