

INDUREVIA

OT Cyber Risk. Operational Resilience.

GUIDED OT READINESS ASSESSMENT

Public Sample Customer Report

Organization	Riverton Precision Components (Fictional)
Facility / Site	Main Manufacturing Plant
Assessment Date	October 8, 2026
Prepared By	Indurevia
Assessment Version	Guided Assessment v1.0

PUBLIC SAMPLE - FICTIONAL ORGANIZATION - DEMONSTRATION DATA

Know your plant's cyber risk — before it becomes downtime.

A practitioner-led review of OT cybersecurity readiness, evidence, operational risk, and prioritized improvement actions.

SAMPLE NOTICE This document is a fictional demonstration of the deliverable provided with an Indurevia Guided OT Readiness Assessment. Riverton Precision Components is not a real customer, and all scores, findings, evidence, and operational details are fabricated for demonstration purposes.

00 Report Contents

Public sample structure for the Guided OT Readiness Assessment

Section	Content
01	Executive Summary
02	Assessment Scope & Methodology
03	Manufacturing Environment Profile
04	Validated Readiness Results
05	Notable Strengths
06	Executive Priority Findings
07	Detailed Validated Findings
08	Evidence & Validation Summary
09	30/60/90-Day Improvement Roadmap
10	Longer-Term Considerations
11	Management Decisions & Next Steps
12	Framework Alignment
13	Assessment Limitations & Disclaimer

01 Executive Summary

A concise management-level interpretation of validated OT cybersecurity readiness

Validated Score	Readiness Band	Risk Status	Applicable Questions
45/100	Established	CRITICAL	25/25

Overall Readiness

Riverton Precision Components achieved a validated OT Readiness Score of 45/100, placing the assessed plant in the Established band. Core practices are present, particularly in backup operations, named-account use, and assigned OT ownership, but implementation is inconsistent across several risk-critical controls. The overall maturity score should not be interpreted as low risk: the assessment identified a Critical compound exposure involving remote access, along with High-priority weaknesses in incident response, vulnerability management, monitoring coverage, and recovery validation.

Principal Risk Story

The principal risk theme is that trusted remote-access paths are not governed consistently enough to prevent or contain misuse. If a remote or vendor credential were compromised, uneven MFA/session controls and limited internal OT monitoring could delay detection and increase the chance of production impact. A second theme is recovery confidence: backups are generally established, but restoration has not been sufficiently exercised and recovery sequencing remains incomplete.

Recommended Management Focus

- Standardize all OT remote-access pathways, MFA, jump-host use, vendor enablement, and recurring access review.
- Define OT-specific incident authority, escalation, and communications, then exercise the playbook.
- Validate recovery through a controlled restoration test and document process dependencies/restoration order.
- Plan phased monitoring and segmentation improvements around engineering capacity and production windows.

02 Assessment Scope & Methodology

How the Guided Assessment was performed and how results should be interpreted

Assessment Approach

The Indurevia Guided OT Readiness Assessment is a practitioner-led review of cybersecurity readiness across seven OT domains. It uses a consistent 25-question scoring model, guided interview prompts, targeted evidence review, practitioner observations, compound-risk logic, and a prioritized improvement roadmap.

- Customer responses were preserved as the initial assessment position.
- The assessor used structured follow-up questions to clarify how controls operate in practice.
- Available documents, records, diagrams, screenshots, or other reasonable evidence were reviewed where appropriate.
- Validated answers were used to calculate the final readiness score and domain results.
- Automated severity was kept separate from practitioner priority so operational context could inform sequencing without changing the scoring engine.

Validation Levels

Validation Level	Meaning
Self-reported — Unverified	Based primarily on the customer statement; no meaningful supporting evidence was reviewed.
Interview validated	Structured probing produced a coherent and credible description of how the control operates.
Document reviewed	A relevant policy, diagram, inventory, record, report, or similar artifact supported the response.
Technical evidence validated	Technical evidence was reviewed for the specific question. This does not imply exhaustive technical testing.

03 Manufacturing Environment Profile

Operational context used to interpret cybersecurity readiness and remediation feasibility

Industry / Manufacturing	Precision manufacturing / automotive supplier	Employees at Site	100–249
Manufacturing Sites	1	Approx. OT Assets	500–999
Production Schedule	3 shifts	Tolerable Downtime	1–4 hrs
OT / Controls Staffing	Dedicated controls/engineering staff	Cybersecurity Staffing	No dedicated OT cybersecurity staff
Remote Support Model	Central VPN/jump-host for most users; vendor exceptions remain	Primary OT Vendors	Rockwell Automation, Siemens, FANUC (mixed)
Assessment Scope	One manufacturing plant / defined OT environment	Evidence Basis	Five supporting artifacts reviewed; interview validation used where evidence was unavailable

Critical Production Processes

#	Critical Process	Tolerable Downtime	Primary Business Impact
1	Automated assembly lines	1–4 hrs	Production loss / delivery
2	CNC machining cells	4–8 hrs	Production loss / quality
3	Final inspection / machine vision	1–4 hrs	Quality / delivery

Operational Context

The plant operates three shifts and depends on automated assembly, CNC machining, and machine-vision inspection with limited tolerance for production interruption. A small IT team supports the site alongside plant controls/engineering personnel, while several vendors retain remote-support pathways. The environment includes mixed modern and legacy Windows systems. Limited maintenance windows, incomplete OT monitoring coverage, and vendor dependencies constrain how quickly some improvements can be implemented.

04 Validated Readiness Results

Validated maturity across the seven Indurevia OT readiness domains

Validated Score	Readiness Band	Risk Status	Applicable Questions
45/100	Established	CRITICAL	25/25

Domain Results

Domain	Score	Band	Executive Interpretation
Governance & Ownership	58	Established	Ownership exists and enterprise practices provide a foundation, but OT-specific policy and recurring risk governance remain inconsistent.
Asset Visibility & Criticality	50	Established	Useful inventory and network information exists, but portable/vendor-connected assets and dependency mapping need better reconciliation.
Network Architecture & Access	40	Developing	Basic IT/OT separation exists, but remote-access controls and internal segmentation are the largest architecture-related concerns.
System & Account Protection	50	Established	Account controls are generally workable; the largest weakness is an inconsistent, case-by-case OT vulnerability and patch-risk process.
Monitoring & Detection	42	Established	Logging and boundary monitoring provide partial visibility, but several production segments remain blind and alert handling needs stronger OT context.
Incident Response	33	Developing	Enterprise response capability exists, but OT-specific decision

Domain	Score	Band	Executive Interpretation
			authority, communications, and exercise maturity are underdeveloped.
Backup, Recovery & Resilience	42	Established	Backups are a relative strength; restoration testing and dependency-based recovery sequencing require validation.

How to Read the Score

The readiness score reflects implementation maturity across applicable questions. Risk status is evaluated separately because a plant can show moderate overall maturity while still having a small number of critical weaknesses that materially affect operational resilience.

Score	Band	General Interpretation
0–20	Initial	Foundational OT cybersecurity practices are limited or inconsistent.
21–40	Developing	Some controls exist, but significant gaps or inconsistent implementation remain.
41–60	Established	Core practices are present, with material opportunities to improve coverage and consistency.
61–80	Managed	OT cybersecurity practices are broadly managed, with targeted gaps and improvement needs.
81–100	Resilient	Strong, broadly implemented practices with continued focus on validation, sustainability, and resilience.

05 Notable Strengths

Practices that materially support OT cybersecurity readiness and operational resilience

Strength	Established backup routine
Evidence / Observation	EV-005 confirmed recurring backups of critical PLC/HMI programs, engineering files, and supporting data.
Why It Matters	Provides a meaningful recovery foundation and reduces dependence on rebuilding critical configurations from scratch.

Strength	Named-account practices on supported systems
Evidence / Observation	Interview validation confirmed individual accounts are used on most Windows and engineering platforms, with shared accounts mainly limited to legacy/vendor constraints.
Why It Matters	Improves accountability and reduces risk associated with unmanaged shared credentials.

Strength	Assigned OT cybersecurity ownership
Evidence / Observation	Plant Engineering has clear day-to-day responsibility and coordinates with IT Security when enterprise controls or incidents require support.
Why It Matters	Creates a practical decision point for governance, remediation ownership, and cross-functional coordination.

Strength	Existing enterprise/OT boundary controls
Evidence / Observation	EV-002 confirmed firewall separation between enterprise IT and OT networks and documented the major production network paths.
Why It Matters	Provides a useful architectural foundation that can be refined toward least-required communications and stronger internal zoning.

06 Executive Priority Findings

The issues requiring the clearest management attention and coordinated action

The findings below represent the most consequential risk themes identified through validated responses, compound-risk logic, evidence review, and manufacturing context. Priority reflects both cybersecurity significance and potential operational consequence.

Finding	Uncontrolled Remote Access
Priority	Executive Priority — Critical
Operational impact	Inconsistent MFA, jump-host use, and vendor-session controls leave a credible path for unauthorized remote access to production systems. A compromised vendor or remote account could disrupt automated assembly and CNC operations.
Tailored recommendation	Inventory every OT remote-access pathway and account, eliminate unapproved paths, require MFA and the controlled jump-host path for all feasible access, apply time-bounded vendor enablement, and establish quarterly access review.
Target horizon	0–30 days

Finding	Incident Response Breakdown
Priority	Executive Priority — High
Operational impact	OT-specific decision authority and coordination are underdefined. During a cyber event, delays in deciding whether or how to isolate production assets could extend downtime or create unsafe recovery pressure.
Tailored recommendation	Create an OT incident playbook defining isolation/shutdown authority, plant/IT/security/vendor roles, escalation criteria, communications, and recovery handoffs; then validate it through a tabletop exercise.
Target horizon	31–60 days

Finding	Restore Testing
Priority	Executive Priority — High
Operational impact	Backups exist, but unproven restoration increases the chance that a real outage or ransomware event will reveal missing files, dependencies, tools, or procedures when recovery time matters most.
Tailored recommendation	Perform a controlled restore test for at least one critical PLC/HMI configuration and one supporting OT server or engineering-data set; record timing, dependencies, failures, lessons learned, and corrective actions.
Target horizon	61–90 days

06 Executive Priority Findings — Continued

Finding	Vulnerability & Patch Management
Priority	High
Operational impact	Known OT weaknesses may remain unresolved without documented patch/defer decisions, compensating controls, ownership, or management awareness.
Tailored recommendation	Establish a risk-based OT vulnerability workflow covering vendor advisories, affected assets, operational testing constraints, patch/defer decisions, compensating controls, owners, and target dates.
Target horizon	31–60 days

Finding	OT Network Monitoring
Priority	High
Operational impact	Limited monitoring coverage creates blind spots across CNC and assembly areas, reducing the plant's ability to identify unexpected devices, lateral movement, or anomalous communications early.
Tailored recommendation	Prioritize passive monitoring coverage for critical production segments, define who reviews alerts, and reconcile observed devices/communications against the asset inventory and approved network paths.
Target horizon	61–90 days

Priority Interpretation

The roadmap is intentionally sequenced around dependencies. Remote-access inventory and asset reconciliation come first because they establish ownership and visibility needed for later control improvements. Incident-response and vulnerability-management work follow once those baselines are clearer. Monitoring expansion and recovery validation move into the 61–90 day window because they require technical preparation, cross-functional coordination, and in the case of restoration testing, a controlled maintenance opportunity.

07 Detailed Validated Findings

Supporting findings selected for inclusion in the customer report

Key	Finding	Severity	Priority	Horizon	Evidence	Tailored Action
CR-01	Uncontrolled Remote Access	Critical	Exec Priority	0–30 days	EV-003	Standardize remote access: MFA, approved jump-host, time-bounded vendor access, and quarterly review.
CR-05	Incident Response Breakdown	High	Exec Priority	31–60 days	EV-004	Define OT incident authority, escalation, communications, and exercise the playbook.
Q24	Restore Testing	High	Exec Priority	61–90 days	EV-005	Perform and document a controlled OT restore test.
Q15	Vulnerability / Patch Mgmt.	High	High	31–60 days	Interview	Create a risk-based OT vulnerability/patch workflow with documented defer decisions.
Q18	OT Network Monitoring	High	High	61–90 days	EV-004	Expand passive monitoring on critical CNC and assembly segments.
Q25	Recovery Priorities	High	High	61–90 days	EV-005	Document recovery dependencies, downtime, required tools, and restore order.
Q4	OT Asset Inventory	Moderate	Medium	0–30 days	EV-001	Add engineering laptops and temporary/vendor assets to the inventory.
Q8	IT/OT Segmentation	Moderate	Medium	90+ days	EV-002	Tighten broad IT/OT flows and phase stronger zone/conduit segmentation.

08 Evidence & Validation Summary

What supported the assessment and where important limitations remain

Evidence Items	Reviewed	Follow-up Needed	Score-Impacting
5	5	5	5

Evidence Reviewed

- EV-001 — OT asset inventory spreadsheet and sample asset records
- EV-002 — High-level IT/OT network diagram and production VLAN overview
- EV-003 — Remote-access procedure, VPN/jump-host overview, and vendor account sample
- EV-004 — SOC alert escalation procedure and sample OT-boundary alert
- EV-005 — Backup procedure, recent backup job history, and available restore documentation

Important Limitations

Five supporting evidence items were reviewed. Several governance, account-management, removable-media, vulnerability-management, and incident-exercise conclusions remained primarily interview validated or self-reported. No active scanning, system login, firewall-rule audit, configuration audit, or exhaustive technical testing was performed. The network diagram was not fully current, and restoration evidence did not demonstrate an end-to-end OT recovery exercise.

Evidence Handling

Indurevia records what evidence was reviewed and what it supported. Sensitive customer documents should not be reproduced in this report unless necessary. Credentials, passwords, private keys, and authentication secrets are outside the scope of the Guided Assessment and should not be provided.

09 30/60/90-Day Improvement Roadmap

A practical sequence for reducing risk while respecting manufacturing constraints

The roadmap prioritizes actions that can materially improve readiness without forcing outage-dependent, capital-intensive, or architecture-heavy work into unrealistic deadlines.

0–30 Days	Immediate risk reduction, ownership, inventory, access cleanup, procedural gaps, and preparatory work.
Actions	• Inventory every OT remote-access pathway/account and retire or formally approve exceptions. • Require MFA and the controlled jump-host path for all feasible OT remote/vendor access. • Reconcile the OT asset inventory to include engineering laptops and temporary/vendor-connected assets.
Success measures	All remote paths/accounts have an owner and approved disposition; supported access uses MFA/approved path; critical production areas are reconciled in the asset inventory.
31–60 Days	Coordinated implementation requiring approvals, vendor input, moderate engineering, or process change.
Actions	• Implement a risk-based OT vulnerability and patch-decision workflow. • Create an OT-specific incident playbook with isolation authority, contacts, escalation thresholds, and vendor coordination.
Success measures	Open vulnerability/patch decisions have owners and documented dispositions; an approved OT incident playbook and call tree define decision authority and communications.
61–90 Days	Validation, exercises, restore testing, monitoring expansion, segmentation improvement, or planned operational windows.
Actions	• Expand passive OT monitoring to critical CNC and automated-assembly segments. • Perform a controlled restoration test for representative critical OT configurations and data. • Document recovery dependencies and restoration sequence for the three highest-impact production processes.
Success measures	Critical segments have defined monitoring coverage; representative OT restoration is successfully tested and documented; top processes have approved dependency/recovery sequences.

10 Longer-Term Considerations

Improvements requiring strategic planning beyond the initial 90-day roadmap

Some risk-reduction activities depend on capital planning, lifecycle replacement, major architecture changes, extended vendor coordination, or production outages. These items should be tracked explicitly rather than treated as failed 90-day commitments.

Strategic Item	Business Rationale	Dependency	Likely Window	Decision Owner
Phased zone/conduit segmentation	Reduce unnecessary lateral movement and improve containment.	Architecture design, firewall review, production windows	2027 planning cycle	IT Infrastructure / Engineering
Legacy Windows lifecycle strategy	Reduce unsupported-platform exposure while preserving vendor compatibility.	Asset criticality, OEM support, capital budget	2027–2028	Engineering / Management
Vendor remote-access consolidation	Reduce exception pathways and standardize MFA, logging, and account lifecycle.	Vendor agreements, access architecture	2027	IT / Cybersecurity
Broader passive OT monitoring	Extend visibility beyond initial critical segments.	Sensor placement, network design, alert ownership	2027	Cybersecurity / IT
Recurring OT risk governance cadence	Sustain ownership, remediation tracking, and reassessment.	Management sponsorship, risk register	Quarterly	Plant Engineering / Cybersecurity

Architectural / Lifecycle Themes

The most important longer-term themes are segmentation maturation, legacy operating-system lifecycle planning, consolidation of vendor remote-access paths, broader passive monitoring coverage, and a recurring plant-level OT cyber risk governance cadence. These items may require capital, vendor coordination, architecture design, or planned production windows and should therefore be managed as strategic work rather than treated as overdue 90-day actions.

11 Management Decisions & Next Steps

Decisions that require leadership attention, cross-functional ownership, or resource commitment

Decision / Next Step	Why Leadership Attention Is Needed	Recommended Timing	Owner
Approve a plant-wide remote-access control standard and exception owner.	Cross-functional authority is needed to remove inconsistent vendor pathways and enforce MFA/jump-host expectations.	Within 30 days	Plant/IT leadership
Assign ownership for the OT incident playbook and isolation/shutdown decision roles.	Operational and cybersecurity teams need predetermined authority before an incident creates time pressure.	Within 45 days	Plant management / Cybersecurity
Provide a maintenance window for a controlled OT restoration exercise.	Recovery confidence cannot be established through backup-job success alone.	Within 90 days	Operations / Engineering
Sponsor a phased monitoring and segmentation improvement plan.	Broader visibility and least-required communications require engineering coordination and potentially capital planning.	90+ days	IT / Engineering leadership
Establish a quarterly OT risk and roadmap review.	Sustains ownership and prevents one-time assessment findings from becoming stale.	Quarterly	Plant Engineering / Cybersecurity

Suggested Follow-Up

- 30-day checkpoint: confirm remote-access inventory/control cleanup and OT asset reconciliation progress.
- 90-day checkpoint: review monitoring expansion, restore-test results, recovery sequencing, and incident-playbook readiness.
- Consider a formal reassessment in 6–12 months or after major architecture/change initiatives.
- Executive-priority risks that cannot be remediated on schedule should be documented with an owner, compensating controls, and accepted target date.

12 Framework Alignment

Informative alignment to widely used OT cybersecurity guidance

Indurevia uses public cybersecurity frameworks and guidance to inform assessment structure and recommendations. Framework references in this report are provided for orientation and planning; they do not constitute certification, attestation, or a determination of compliance.

Assessment Domain	NIST CSF 2.0	NIST SP 800-82	CISA CPG / Other
Governance & Ownership	GV (Govern); ID.RA	OT cybersecurity program and risk-management guidance	Governance, accountability, training and risk-management practices
Asset Visibility & Criticality	ID.AM; ID.RA	Asset inventory, system characterization and risk-assessment guidance	Asset inventory and device visibility practices
Network Architecture & Access	PR.PS; PR.IR	Network architecture, segmentation and remote-access guidance	Network segmentation, secure remote access and MFA practices
System & Account Protection	PR.AA; PR.PS	Access control, patch/vulnerability management and removable-media guidance	MFA/access control and vulnerability-management practices
Monitoring & Detection	DE.CM; DE.AE	Logging, monitoring and anomaly-detection guidance	Logging, centralized monitoring and alerting practices
Incident Response	RS.MA; RS.AN; RS.CO; RS.MI	Incident-response planning and coordination guidance	Incident-response planning, communications and exercises
Backup, Recovery & Resilience	RC.RP; RC.CO; PR.IR	Backup, recovery and contingency-planning guidance	Backups, recovery testing and resilience practices

13 Assessment Limitations & Disclaimer

Important boundaries for interpreting this report

Public Sample Status

Riverton Precision Components, its manufacturing environment, evidence items, scores, findings, priorities, and roadmap are fictional and were created solely to demonstrate the structure and depth of an Indurevia Guided OT Readiness Assessment. No real customer information is represented in this sample.

Nature of the Service

The Indurevia Guided OT Readiness Assessment is a point-in-time readiness review based on the assessment scope, customer-provided information, practitioner interview, and evidence available during the engagement. It is intended to support risk prioritization and operational resilience planning.

What This Assessment Is Not

- A penetration test, vulnerability scan, red-team exercise, or technical security test.
- An exhaustive audit of every OT asset, network path, configuration, account, or security control.
- A certification, compliance attestation, legal opinion, or guarantee that the environment is secure.
- Authorization for Indurevia to modify, connect to, or operate customer production systems.
- A substitute for engineering, safety, legal, regulatory, insurance, or other specialized professional advice where those disciplines are required.

Customer Responsibility

The customer remains responsible for evaluating recommendations in the context of safety, production, quality, change management, vendor requirements, regulatory obligations, and operational risk before implementation. Changes to OT environments should follow appropriate engineering and change-control processes.

Evidence & Future Change

Results may be affected by incomplete, unavailable, or inaccurate information. OT environments also change over time; new assets, network paths, software, vendors, threats, and business requirements may alter risk after the assessment date.

INDUREVIA

Understand Risk. Strengthen Resilience.

This fictional sample illustrates the structure, evidence depth, prioritization, and roadmap a customer can expect from an Indurevia Guided OT Readiness Assessment.

Contact

support@indurevia.com
www.indurevia.com

Ready to Assess Your Plant?

Start with the free OT Risk Snapshot at www.indurevia.com, or request a Guided Assessment for practitioner-led validation, evidence review, prioritized remediation, a 30/60/90-day roadmap, and a 30-minute readout.

OT Cyber Risk. Operational Resilience.