

01 · EXPOSE — RISK ANALYSIS

The Score Isn't the Problem. The Gaps You Didn't Know Were Driving It Are.

Every environment has more gaps than it can close at once. The question isn't whether you have risk — it's which risk matters most, where the score comes from, and what to act on first.

ConsoleWorks traces every score to the specific measurement that drove it — and puts the fix path one click away.

WHERE THIS PICKS UP

Asset Intelligence Built the Inventory. Now ConsoleWorks Acts on It.

Asset Intelligence built the unified, authoritative inventory. Measurement Questions ran against every asset. Every asset returned a Pass or Fail. Those binary results are the inputs. Risk Analysis is what ConsoleWorks does with them — aggregating through the Secure Controls Framework (SCF) hierarchy, surfacing gaps ranked by organizational impact, and generating a continuously updated posture that traces from fleet level down to the specific measurement that drove it.

A device not in the inventory cannot be measured. A measurement that cannot be traced cannot be trusted. Risk Analysis depends entirely on the accuracy of the inventory beneath it — and extends that accuracy upward into a posture that security, compliance, and operations teams can all work from simultaneously.

Fully Traceable

Fleet score → domain → control → sub-control → measurement → asset → collection event. The chain is unbroken.

Continuously Updated

Scores update on every measurement cycle — on schedule, automatically. Posture reflects the latest run, not last quarter's assessment.

Gaps Ranked by Impact

You define asset weights. ConsoleWorks applies them. The highest-impact gaps surface first — with a direct fix path included.

Evidence Generated

Every cycle produces NERC CIP, NIST, IEC 62443, CMMC, and SOC 2 evidence — stored, timestamped, ready on demand.

THREE LENSES. ONE DATA SET.

One Measurement. Three Ways to Act on It.

The same Pass/Fail result means something different depending on who's reading it. ConsoleWorks surfaces the same measurement data through three operational lenses — so each team sees exactly what they need, without translating from a platform built for someone else. One measurement engine. Three conversations.

Security — Are controls in place and working?

A continuously updated posture traced to actual device measurements — with trend data showing improvement or degradation. No black-box algorithms. Zero Trust architectures require continuous verification of control state — ConsoleWorks provides the measurement-driven foundation that Zero Trust enforcement depends on.

Compliance — Does the posture map to the framework?

Every measurement maps to SCF sub-controls, which crosswalk to NERC CIP, NIST 800-53, IEC 62443, CMMC, SOC 2, and 100+ frameworks simultaneously. When a control passes, it satisfies requirements across every applicable framework at once — with timestamped evidence already stored.

Operations — What's broken, and where?

Failed measurements ranked by operational impact — with a Fix button that opens a Secure Remote Access session directly from the gap, under Least Privilege controls. Works across IT and OT environments with the same workflow. The score updates when the fix is verified, not when the ticket is closed.

Reporting Scope — How much of your environment is scoring?

A risk score based on 847 of 1,200 expected assets is a fundamentally different number than one based on 1,200 of 1,200. ConsoleWorks surfaces Reporting Scope alongside every score — so you always know what the number represents, and where measurement hasn't yet reached.

MEASUREMENT QUESTIONS

The Language of Risk: Pass/Fail, Every Asset, Every Cycle.

Risk Analysis begins with Measurement Questions — configurable Pass/Fail checks that ConsoleWorks evaluates against every asset in the inventory. Each question tests one specific condition on one or more device types. Questions are organized into three categories — Operational, Security, and Compliance — reflecting the three lenses through which posture is assessed. Organizations configure which questions apply to which assets; a PLC running EcoStruxure is measured against a different set of questions than a Windows Server in the corporate network, even though both contribute to the same posture hierarchy.

Measurement Questions are not static checklists. They run on every cycle — continuously evaluating current device state against the organization’s defined requirements. If state changes between cycles — a patch goes uninstalled, a configuration drifts, a new account appears — the next cycle surfaces it. The score reflects what is true now.

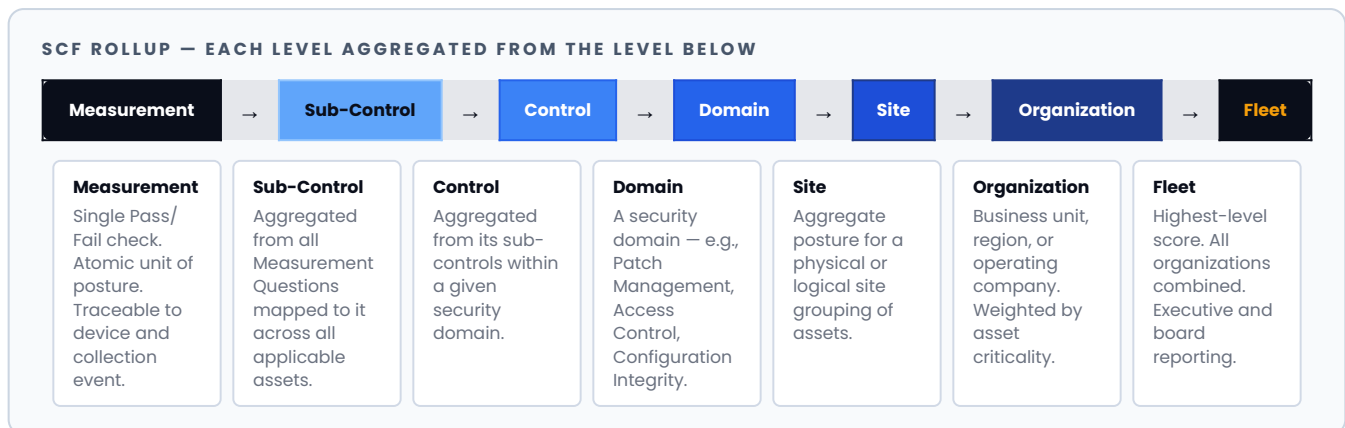
Operational	Security	Compliance
<ul style="list-style-type: none"> Running approved firmware version Configuration within defined policy baseline No unauthorized software detected Services and open ports within baseline Communication paths match expected profile 	<ul style="list-style-type: none"> Latest known vulnerabilities addressed Patches applied within required window Antivirus definitions current (where applicable) No unmitigated high-severity CVEs No default or shared credentials detected 	<ul style="list-style-type: none"> Specific NERC CIP control requirement met IEC 62443 security level satisfied Continuous logging and audit trail active Access control policy enforced per framework Session monitoring requirements in place

Organizations configure which Measurement Questions apply to which assets — ensuring OT devices like PLCs, RTUs, and protective relays are held to the right standards, not forced into IT templates that don’t reflect their operational reality. An RTU that lacks antivirus because none exists for its platform is not a failed measurement — it’s a correctly scoped one.

THE SCF HIERARCHY

From a Single Device Measurement to Organizational Risk Posture

Every Measurement Question maps into the Secure Controls Framework (SCF) — a structured rollup that aggregates Pass/Fail results into a continuously updated posture score at every level of the organization. A single failed measurement on one device affects every level above it. The magnitude depends on asset weight and domain priority settings configured by the organization.

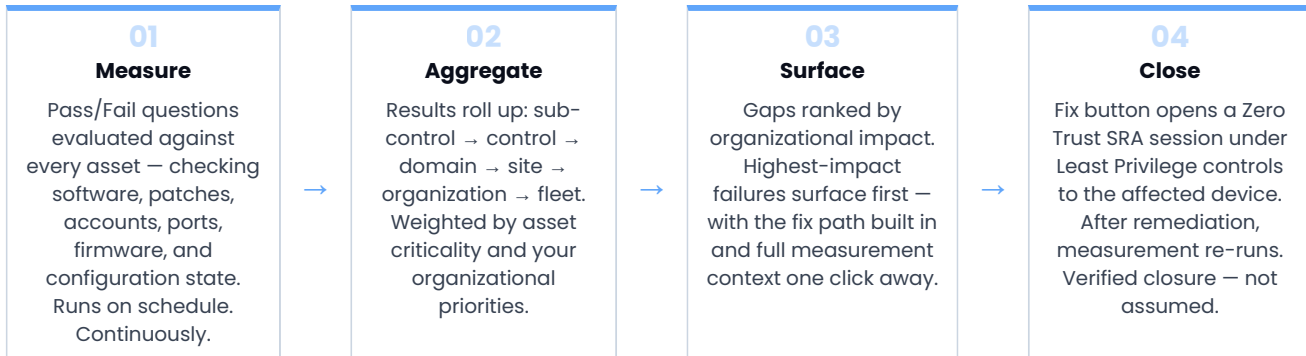


A drop at the Domain level points to the Control. The Control points to the Sub-Control. The Sub-Control points to the Measurement. The Measurement points to the asset — and from there, you can open a session and fix it. ConsoleWorks doesn’t require you to trace that chain manually. Every level is a click into the next. Zero Trust policies are only as strong as the posture data behind them — a continuously verified, measurement-driven score gives enforcement policies something real to act on.

HOW SCORING WORKS

Measure → Aggregate → Surface → Close

You define the asset groups that mirror your organization. You define the weightings that reflect your priorities. ConsoleWorks calculates and aggregates continuously – rolling measurement results up through sub-controls, controls, domains, and your full organizational hierarchy. One failed measurement on one device affects every level above it. The impact depends on asset weight and domain priority settings you control. Every level is recalculated on the next measurement cycle.

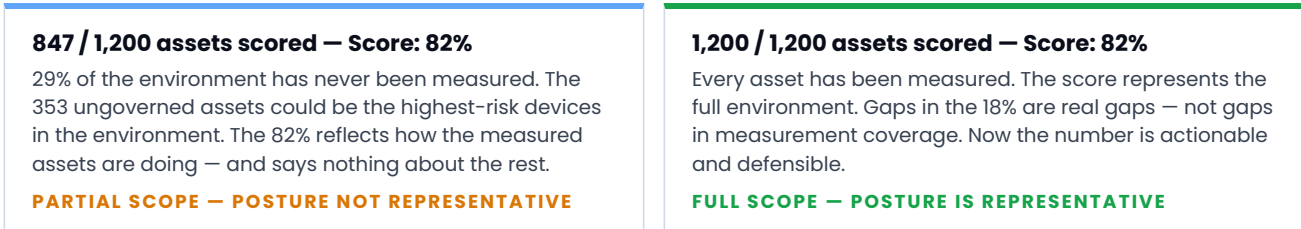


The score is the signal – not the destination. The rollup exists to direct attention. Zero Trust policies are only as strong as the posture data behind them – a continuously verified, measurement-driven score gives enforcement policies something real to act on.

REPORTING SCOPE

The Score Tells You How Well. Scope Tells You How Much.

A risk score only means something if you know what it's based on. An organization with 1,200 assets in its inventory that has measured 847 of them doesn't have a risk score – it has a partial one. The remaining 353 assets are unmeasured, unmeasured, and invisible to the posture calculation. ConsoleWorks surfaces Reporting Scope alongside every score at every level of the hierarchy.



Scope gaps are treated as a category of finding in their own right – surfaced alongside measurement failures so that coverage and posture are both managed explicitly. Expanding measurement scope is itself a risk reduction activity.

HOW IT COMPARES

Not All Risk Scores Are Created Equal

Most risk tools produce a score from estimates or periodic assessments. ConsoleWorks produces one from actual measurements – traceable to the device, continuously updated, with a direct fix path built in.

Capability	ConsoleWorks	Risk Platforms	GRC / Compliance Tools
Score Traceability	✓ Fleet → asset → measurement → collection event	Partial — score to control, not to measurement	Based on manual inputs — not live measurements
Three Lenses	✓ Security, Compliance, Operations from one data set	Security only — compliance requires separate tool	Compliance only — security requires separate tool
Posture Currency	✓ Updates on every measurement cycle	Partial — depends on scan frequency	Point-in-time — updated manually or on assessment
OT Coverage	✓ Native OT — PLCs, RTUs, HMIs, protective relays	Limited — IT-centric; OT requires add-on	IT scope only — no native OT measurement
Fix Path	✓ SRA session opens directly from failed measurement	Alert only — remediation in a separate tool	No remediation capability
Verified Closure	✓ Measurement re-runs — score updates when gap is closed	Score updates on next scan cycle	Score updated manually — no automated verification
Audit Evidence	✓ Generated every cycle — 100+ frameworks auto-mapped	Partial — some evidence, limited framework mapping	Strong evidence — requires manual data entry

ONE MEASUREMENT. 100+ FRAMEWORKS.

Compliance Evidence Isn't Assembled Pre-Audit. It Accumulates Every Cycle.

Most organizations maintain separate compliance programs for each framework they operate under — NERC CIP here, NIST 800-53 there, IEC 62443 for the OT team, CMMC for the defense side. Each demands its own evidence. The result is redundant effort, reconciliation between overlapping requirements, and a sprint every time an audit begins.

ConsoleWorks eliminates that fragmentation through the SCF crosswalk. Every Measurement Question maps to SCF sub-controls. Every SCF sub-control crosswalks automatically to every applicable framework it satisfies. When a Measurement Question passes, it satisfies requirements across every mapped framework simultaneously — without additional configuration, without re-running assessments, and without building a separate evidence package for each auditor.

EXAMPLE: SINGLE MEASUREMENT QUESTION → MULTIPLE FRAMEWORK CONTROLS SATISFIED SIMULTANEOUSLY
Measurement Question: Antivirus definitions current on all applicable assets

Pass/Fail · Security + Compliance · Applicable to IT and OT endpoints with AV capability

Framework	Specific Control Satisfied	Primary Sector
NERC CIP-007 R3	Malicious Code Prevention — AV definition currency requirement	Energy & Utilities
NIST 800-53 SI-3	Malicious Code Protection — mechanism currency requirement	Federal / Defense
IEC 62443 SR 3.2	Malicious code protection — prevention and detection	Industrial / OT
NIST CSF PR.DS-1	Data-at-rest protection — integrity maintained	Cross-sector
SOC 2 CC6.8	Logical and physical access controls — malware prevention	Enterprise / Service
ISO 27001 A.12.2	Protection from malware — detection and prevention controls	Cross-sector

Every Measurement Question runs on every cycle. Every cycle generates timestamped evidence automatically mapped to all applicable frameworks. When an audit begins — for any framework — the evidence is already there. No sprint. No last-minute data collection.

IT AND OT — ONE RISK NUMBER, NOT TWO

The Boundary Isn't Clean. The Risk Program Shouldn't Pretend It Is.

Most security tools treat IT and OT as separate domains — because they were built for one or the other. IT risk platforms don't know what to do with a PLC that has no OS agent and responds only over native protocols. OT security tools don't see the

Windows historian sitting at the boundary, or the corporate laptop connected to the control network. Each tool maintains its own view — and the gaps between them are where the real risk lives.

ConsoleWorks manages IT and OT assets in a single inventory, under a single measurement program, producing a single organizational risk posture. An engineering workstation, a SCADA server, and a Schneider RTU on the same site are all governed by the same hierarchy — measured against the requirements applicable to each, weighted by their operational criticality, and contributing to the same domain and site scores that leadership reviews. There is one number — and it represents the environment as it actually operates.

IT Assets Under OT Risk

Engineering workstations, data historians, HMIs running standard operating systems, and corporate systems with connections to control networks are IT in form — but OT in risk profile. A historian with a direct path to a PLC network is not measured as an enterprise endpoint. It is weighted and measured as the operational risk surface it actually is.

OT Assets Without Agent Constraints

PLCs, RTUs, and protective relays that cannot support agents or tolerate active scanning — responding only over Modbus, DNP3, or IEC 61850 — are still manageable under Zero Trust Least Privilege access controls and direct configuration collection. ConsoleWorks reaches them without disruption, and measures them against requirements appropriate to their device class.

PLATFORM INTEGRATION

Risk Analysis Connects to the Full ConsoleWorks Platform.

Risk Analysis is not a standalone scoring engine. It is the output of an integrated measurement program — built on the inventory that Asset Intelligence assembled, acted on through Secure Remote Access, sustained by the Configuration & Change Management cycle, and enforced by continuous measurement under the Enforce mandate. The posture score reflects the environment as it is right now — because every layer of the platform keeps it current.

RISK ANALYSIS ACROSS THE CONSOLEWORKS PLATFORM

Scoped by Asset Intelligence

Inventory accuracy is score accuracy — a device not in the inventory cannot be measured, scored, or fixed. Asset classification, criticality weights, and site assignments flow directly from the inventory into the risk calculation.

Fixed Through SRA

The Fix button opens a Zero Trust SRA session under Least Privilege controls, fully logged keystroke-by-keystroke. The same infrastructure that collected the data closes the gap. No tool switch. No ticket. No assumed closure.

Monitored by CCM

Configuration & Change Management captures device state before and after every session — and detects drift between sessions. Gaps that reopen between cycles are caught. Configuration changes that introduce new risk are logged and surfaced.

Sustained by Enforce

Measurements re-run on schedule. Gaps that reopen surface on the next cycle. Compliance evidence accumulates continuously. The posture you see today will still be accurate tomorrow — because ConsoleWorks never stops measuring.

RISK VIEW — AMARILLO-RTU-04 · IMPACT-RANKED GAPS

[Fix → SRA](#)

SECURITY SCORE 61 / 100	COMPLIANCE SCORE 74 / 100	OPERATIONS SCORE 79 / 100	REPORTING SCOPE 1,200 / 1,200
TOP GAP · DOMAIN Patch Mgmt — 3 Critical Fails	NERC CIP MAPPING CIP-007 R2 · Partial Pass	FIRMWARE v3.1.2 — Drift Detected	LAST MEASURED Today · 06:14 AM

WHAT THIS DELIVERS

A Risk Program Built on Measurement, Not Estimation.

Most organizations don't have a risk visibility problem — they have a risk credibility problem. Scores from estimates or manual inputs create arguments, not decisions. When the CISO, the compliance team, and operations are all looking at different numbers — or the same number with no idea what's behind it — risk management stalls. ConsoleWorks changes the foundation: every score is generated from actual measurements, traced to a specific device and collection event, and updated on every cycle.

A Posture You Can Defend

Every score is traceable. Every gap has a source. When an auditor, a board member, or an incident responder asks why the score is what it is, the answer is a click away — not a spreadsheet exercise. ConsoleWorks produces the evidence-backed posture that Zero Trust governance frameworks require: verified, timestamped, continuously current.

Evidence Without the Audit Sprint

Every measurement cycle generates timestamped evidence automatically mapped to NERC CIP, NIST, IEC 62443, CMMC, SOC 2, and 100+ frameworks simultaneously. When an audit begins, the evidence is already there. No sprint. No last-minute collection. No reconciling what the tool said against what was submitted last quarter.

One Number Everyone Agrees On

Security, compliance, and operations teams often run separate tools and arrive at different conclusions — then spend cycles reconciling. ConsoleWorks eliminates that friction. Because every team works from the same measurement data through their own lens, the conversation shifts from whose number is right to what to do about it.

A Fix Path, Not Just a Finding

Most risk tools end at the alert. ConsoleWorks closes the loop. The Fix button opens a Zero Trust SRA session under Least Privilege controls to the affected device — the same session infrastructure that collected the data. After remediation, the measurement re-runs and the score updates. No ticket. No lag. No assumed closure.

THE PLATFORM BEHIND THE SCORE

Risk Analysis Is the Signal. The Platform Is the Response.

A risk score that ends at a dashboard is a report. A risk score that triggers a fix — and then verifies the fix closed the gap — is a program. ConsoleWorks is built around the latter. The score is not the deliverable. The reduction in exposure is.

From Score to Session in One Step

Every failed measurement carries a Fix button. That button opens a Zero Trust Secure Remote Access session under Least Privilege controls — directly to the device that failed. The same infrastructure that collected the measurement handles the remediation. There is no ticket queue, no out-of-band coordination, no assumed closure. The score updates when the next collection cycle confirms the gap is gone.

Configuration Drift Is a Risk Event

Most risk programs treat configuration as static — set once, audited periodically. ConsoleWorks treats it as a continuous signal. When a device drifts from its approved baseline, the measurement fails, the score reflects it, and Configuration & Change Management can restore the baseline state automatically. Drift becomes a visible, closeable risk event — not a hidden accumulation between audits.

The three solutions in the ConsoleWorks platform — Asset Intelligence, Risk Analysis, and Configuration & Change Management — are not independent modules. They are phases of the same continuous loop: build the inventory, score the posture, close the gaps. Each cycle through the loop produces better data, tighter baselines, and a more defensible posture. Zero Trust governance is not a destination — it is what the loop looks like when it is running well.

01 - Expose

Risk Analysis surfaces every gap — ranked by impact, traced to the measurement, with a direct path to remediation across IT and OT environments.

02 - Eliminate

Configuration & Change Management closes gaps at scale — detecting drift and restoring baseline state before risk accumulates between measurement cycles.

03 - Enforce

Secure Remote Access enforces Zero Trust session controls — ensuring every fix happens under verified, Least Privilege access with a complete session record.

“When every score traces back to a measurement on a real device, you stop debating risk and start managing it.”

— Risk & Compliance Manager, Critical Infrastructure Operator