datacentrix

Operational Technology

Cybersecurity Baseline Assessment

Confidential
This document is confidential and intended for the use of the distribution parties only. Any copying or dissemination of this document is strictly prohibited.
© 2026 Datacentrix (Pty) Ltd

The Operational Technology (OT) cybersecurity baseline assessment is a strategic enabler – reducing operational risk, strengthening governance, guiding investment decisions and supporting digital transformation. It provides leadership with the clarity needed to protect the business today and build resilient, competitive industrial operations for the future.

AN OVERVIEW OF OT CYBERSECURITY BASELINE ASSESSMENTS

1. Purpose

Datacentrix conducts structured OT cybersecurity baseline assessments. The objective is to establish a clear, evidence-based view of a customer's OT security posture and provide a strategic roadmap for improving resilience, system integrity and operational continuity.

2. Why This Matters?

OT environments face rapidly increasing cyber risk due to aging infrastructure, converging IT/OT networks and heightened threat activity targeting industrial operations. Robust OT security is now central to protecting:

- The safety of people and equipment
- Production uptime and operational continuity
- Product quality and process reliability
- Business resilience and regulatory expectations

This assessment offers a practical, low-disruption approach to understanding vulnerabilities before they affect operations.

3. Our Approach

Datacentrix aims to be the "how to" GRC partner, aligning OT and IT through maturity-based control assessments, building a unified strategic cybersecurity framework that works across all standards. Datacentrix applies a proven methodology aligned with to global recognised standards and frameworks, integrating globally recognised frameworks such as:

- National Institute of Standards and Technology (NIST) risk management framework: Guides how we assess controls through a structured life-cycle process.
- **NIST cybersecurity framework:** Defines the capability outcomes we measure and report against.

The process focuses on establishing a realistic OT baseline – not assessing every control – prioritising what matters most for industrial environments aligned to the business' strategic intent.

4. Assessment Structure – Three Phases

4.1 Preparation and context framing

- Understand operational priorities, risks and critical processes
- Review existing documentation and OT governance
- Define system boundaries and preliminary asset lists
- Schedule on-site workshops and assessments

4.2 On-site assessment and discovery (per site)

- Workshops with engineering and operations teams
- Network scanning and physical walk-downs
- Detailed OT asset inventory creation
- Mapping network topology and data flows
- Categorising systems as low/moderate/high impact

4.3 Analysis, maturity scoring and reporting

- Correlation of all evidence collected
- Maturity scoring aligned with IEC 62443 levels (ML1–ML4)
- Identification of control gaps and strengths
- Development of a prioritised improvement roadmap

5. General Domains Assessed

- Security governance and program management
- Asset and configuration management
- Access control and identity management
- Network and communications security
- Monitoring and incident response
- System integrity and life cycle management
- Compliance and continuous improvement

6. Expected Outcomes

Customers receive a unified, enterprise-wide view of the OT cyber maturity and a practical, phased plan to improve resilience. This positions operations for safer, more efficient and more secure industrial performance. Deliverables include the following:

- Executive summary with primary findings and recommendations
- OT system categorisation and baseline assessment

- Maturity scorecard across the identified domains
- Evidence-based observations and control gap analysis
- A prioritised, actionable roadmap to enhance OT cybersecurity maturity relevant to the business' planning.

STRATEGIC SIGNIFICANCE OF OT CYBERSECURITY BASELINE ASSESSMENTS

Operational Technology (OT) environments are now central to business resilience, product quality, and safe, continuous production. As cyber threats increasingly target industrial systems, organisations must ensure their OT environments are secure, dependable and aligned with broader enterprise risk and performance objectives. The OT cybersecurity baseline assessment provides management with a clear, evidence-based understanding of current maturity and the strategic actions required to strengthen operational resilience.

1. Safeguarding Operational Continuity

Downtime in industrial operations has immediate financial and reputational impact. The assessment identifies vulnerabilities across plants, networks and legacy systems that could disrupt production – transforming unknown risk into actionable insight.

Business impact: Protects revenue, throughput and customer delivery commitments.

2. Strengthening Enterprise Risk Management (ERM)

Executives and boards are increasingly accountable for cyber risk. The assessment establishes a defensible maturity baseline aligned to NIST and IEC 62443 standards, enabling management to govern OT risk with the same rigor as financial or operational risk.

Business impact: Enhances governance, oversight and risk transparency.

3. Informing Investment and Budget Prioritisation

OT cyber spending is often ad hoc without clarity on priorities. This assessment produces a capability-based roadmap, ensuring funding is directed to the highest-value controls with the greatest impact on resilience.

Business impact: Ensures cost-effective, strategically aligned investment decisions.

4. Supporting Compliance and Customer Requirements

Regulators, auditors and large customers increasingly demand proof of OT cyber controls. The assessment highlights timeous compliance gaps and supports audit readiness across safety, quality and cybersecurity domains.

Business impact: Maintains license to operate and strengthens supply chain confidence.

5. Protects People, Assets and the Environment

Cyber incidents in OT can cause physical harm, equipment failure and environmental risks. The assessment identifies weaknesses in safety systems, change management and configuration control.

Business impact: Improves worker safety, asset reliability and environmental protection.

6. Enabling Digital Transformation and Industry 4.0

Smart manufacturing, automation and data-driven operations require secure and stable OT foundations. The assessment ensures the OT environment can support modernisation without increasing risk.

Business impact: Accelerates innovation while maintaining operational security.

7. Key Outputs for Management

- Enterprise-wide maturity baseline across all plants
- Asset visibility and formal system categorisation
- Maturity scorecard aligned to NIST and IEC 62443
- Prioritised roadmap for cyber resilience and long-term capability development
- Clear operational and financial justification for relevant future investment

8. Fortify Your Operational Resilience

Establish a clear, evidence-based view of your OT security posture and ensure an effective, strategic roadmap for improving resilience, system integrity and operational continuity with Datacentrix. Contact our industrial cybersecurity specialists today to discuss how we can help you accelerate innovation while maintaining operational security for your OT environment.

Email Karina Geyser, Business Unit Manager: Infrastructure Solutions and Operational Technology at Datacentrix on kgeyser@datacentrix.co.za.

9. National Contact Details

Corporate office
Tel: +27 87 741 5000

Corporate Park North
238 Roan Crescent, 1685
Old Pretoria Road, Midrand

PO Box 50722
Randjiesfontein
Midrand, 1683

Logistics centre
Tel: +27 12 657 5000

26 Landmarks Avenue
Kosmosdal, Extension 11
Samrand, Midrand

PO Box 50722
Randjiesfontein
Midrand, 1683

Coastal

Cape Town office
Tel: +27 21 529 0700

18 Oxbow Crescent
The Estuaries
Century City, 7441

PO Box 181
Century City
Cape Town, 7446

East London office
Tel: +27 43 705 8000

Suite 2, 11 Cavendish Road
Vincent
East London, 5217

PO Box 19066
Tecoma
East London, 5214

Gqeberha office
Tel: +27 41 391 0200

Southern Life Gardens
Ground Floor, Block B, 70 2nd Avenue
Newton Park, Gqeberha

PO Box 63657
Greenacres, 6057

Durban office
Tel: +27 31 389 0500

1st Floor, 30A The Boulevard
Dawncliffe, Westville
Durban, 3629

PO Box 1645
Westville, Durban, 3630

Middle East

Doha office
Tel: +974 4007 1793

Eighteen Tower
Zone 69, Street 303, Building 230
19th Floor, Office 1972
Lusail, Doha, Qatar
PO Box 23107

Rest of Africa

Datacentrix deploys technologies and provides support services to customers across 45 countries in the rest of Africa.

www.datacentrix.co.za