VIRTUAL CISO SERVICES FOR OT

Cyber leadership for SCADA systems, ICS and critical infrastructure

OT systems were built for uptime – not cyber resilience.

Our OT-focused vCISO services provide strategic cybersecurity leadership for critical infrastructure environments. We help you manage cyber risk, align with compliance requirements, and safeguard the systems that keep your services running.

What Is an OT vCISO?

A Virtual CISO for OT environments is a cybersecurity leader who understands the unique risks and constraints of Operational Technology systems — including SCADA, PLCs, telemetry, and control networks.

Unlike IT-centric vCISOs, we bring a risk-informed, engineering-aware approach to cyber governance, helping you:

- Assess and manage threats to critical OT assets
- Bridge the gap between IT and OT teams
- Align with ACSC OT Security Principles, ISM, IEC 62443, or PSPF
- Respond to SoCI Act obligations or Essential Eight guidance
- Improve cyber resilience without disrupting uptime

Our Tiered OT vCISO Packages

We offer fixed-cost packages tailored to OT environments and engineering teams:

BRONZE: OT Cyber Health Check

Understand your current risk landscape and next steps.

- One-time OT risk and architecture review
- Includes SCADA, PLC, or telemetry environments
- Gap analysis against ACSC OT Security Principles or ISM
- Executive-ready summary of top risks
- Recommended 6–12 month remediation roadmap

AUD $2,000–$3,500

SILVER: Ongoing OT Cyber Oversight

Monthly governance and compliance support for OT environments.

- Monthly/quarterly virtual check-in with OT-aware consultant
- OT risk register & vendor risk reviews
- Support for policy development tailored to engineering teams
- IT/OT segmentation & remote access guidance
- Compliance alignment (ACSC, PSPF, Essential Eight, IEC 62443)

AUD $3,500–$5,500/month

GOLD: Embedded OT vCISO Partnership

Strategic OT cyber leadership for critical environments.

- All Silver services plus:
- OT incident response planning & tabletop exercises
- OT/ICS lifecycle cyber risk reviews (design → decommission)
- OT cyber awareness briefings for engineers/operators
- On-site walkthroughs (quarterly, if required)
- 6–10 hrs/month engagement

AUD $6,000–$9,000/month

Outcomes You Can Expect

- ✔ Clear visibility into your OT cyber risks
- ✔ A practical security roadmap aligned to real-world constraints
- ✔ Improved compliance with ACSC, ISM, or IEC 62443
- ✔ Safer remote access, vendor integration, and zone segmentation
- ✔ Risk-aware cyber governance embedded into operations
- ✔ A single point of leadership across IT and OT

What Our Clients Say

"The OT security review helped us identify weaknesses we didn't know existed. Their team gave practical, actionable recommendations — not just generic reports."

ICT Manager, Water Utility Provider

vCISO.One cybersecurity consulting & advisory

29/97 Creek Street, Brisbane City QLD 4000 ☎ 1300 067 003 ✉ info@vciso.one 💻 vciso.one

VIRTUAL CISO SERVICES FOR OT

Cyber leadership for SCADA systems, ICS and critical infrastructure

🏆 Completed Projects

We've worked with a number of councils and critical infrastructure operators across Australia and the U.S. to deliver tailored OT cybersecurity outcomes — from architecture reviews to governance uplift programs of work.

OT Security Architecture Review

City of Las Vegas, NV

Reviewed and assessed the network and security architecture of a council-operated industrial control system to identify segmentation gaps, legacy risks, and improvement opportunities aligned with IEC 62443.

OT Visibility Standardisation

California Dept of Transport (CalTrans)

Developed a common OT asset taxonomy and visibility framework across multiple departments to support consistent inventory, monitoring, and risk reporting in alignment with NIST CSF.

OT Readiness Assessment & Policy Development

Local City Council, Queensland

Conducted an OT cybersecurity maturity assessment and developed tailored governance policies to prepare a regional authority for Essential Eight and Australian ISM uplift and future compliance obligations.

⚠️ Why OT Cyber Needs a Different Approach

OT systems:

- Can't always be patched or rebooted
- Often use insecure protocols (Modbus, DNP3, IEC 60870-5-104)
- Rely on vendor-managed devices and long life cycles
- Prioritise safety and uptime over confidentiality

We work with these realities — not against them — to design governance, monitoring, and response models that make sense for OT.

👷 Who Is This For?

- **Local councils** managing SCADA, smart city, or water infrastructure
- **Energy, transport, or manufacturing operators** under the SoCI Act
- **Critical infrastructure owners** needing governance uplift
- **Engineering teams** without internal cybersecurity support
- **Organisations** struggling to bridge the OT/IT divide

Let's Talk OT Security

We speak both "engineer" and "cyber." If you're looking for risk-aware cybersecurity leadership that understands SCADA, PLCs, and control systems — we're ready to help.

Schedule a FREE Discovery Call

vCISO.One cybersecurity consulting & advisory

29/97 Creek Street, Brisbane City QLD 4000 ☎ 1300 067 003 ✉ info@vciso.one 💻 vciso.one