SECURITY ARCHITECTURE ASSESSMENTS

Designing resilient networks, systems and environments from the ground up

Your architecture is the foundation of your cyber resilience.

Our Security Architecture Assessments help you validate and improve your network, cloud, application, and OT environments. Whether you're reviewing an existing design or planning a new system, we assess your security posture through the lens of practical risk.

🔍 What Is a Security Architecture Assessment?

A **Security Architecture Assessment** evaluates how well your IT and OT systems are designed to prevent, detect, and respond to cyber threats — before you spend time or money deploying the wrong solution.

We assess architectural components across:

- Network topology and segmentation
- Cloud and hybrid environments
- SCADA and industrial control systems
- Web apps, APIs, and third-party integrations
- Identity and access pathways

We don't just focus on theory — we look at how your systems are actually used and advise accordingly.

🔎 Key Focus Areas

Network & Infrastructure

- Internal segmentation and trust boundaries
- DMZ design and remote access paths
- Firewall and IDS/IPS placement
- Redundancy, failover, and isolation of critical systems

Cloud & Hybrid Environments

- Microsoft 365, Azure, AWS, Google Cloud
- Identity federation, authentication, and RBAC
- Secure configuration baselines
- Multi-tenancy and SaaS application risks

OT & ICS Environments

- Mapping of zones (Purdue Model, Level 0–5)
- Unsecured protocol analysis (Modbus, DNP3, etc.)
- OT/IT separation and access control
- Visibility into field devices and vendor pathways

Application & Data Flows

- API design and authentication
- Data flow and classification review
- Encryption and secure storage practices
- Third-party service dependencies

⚠️ Common Issues We Identify

- Flat internal networks with no segmentation
- Poorly managed cloud identity and permissions
- Shared credentials for vendor remote access
- Visibility gaps in hybrid IT/OT environments
- App/API designs that leak sensitive data

vCISO.One cybersecurity consulting & advisory
29/97 Creek Street, Brisbane City QLD 4000
☎ 1300 067 003
✉ info@vciso.one
vciso.one

SECURITY ARCHITECTURE ASSESSMENTS

Designing resilient networks, systems and environments from the ground up

👷💼 Who This Is For

- **IT teams** planning or reviewing a new system or cloud migration
- **Councils and utilities** deploying or integrating smart systems
- **Organisations** undergoing cybersecurity uplift or maturity reviews
- **Projects** requiring secure-by-design principles or architecture sign-off
- **Critical infrastructure providers** complying with ISM, SoCI, or PSPF

💬 What Our Clients Say

"vCISO.One provided us with a clear view of where our architecture was putting us at risk — and helped us redesign it before implementation. They gave us real-world feedback, not academic theory."

— Digital Transformation Lead, Local Government Organisation

🎯 Deliverables You Can Expect

- ✔ Architecture diagram review and mark-up
- ✔ Written recommendations aligned to risk and compliance needs
- ✔ Secure architecture principles and reference patterns
- ✔ Design validation prior to procurement or deployment
- ✔ Integration support with GRC, vCISO, or MSS offerings

📦 Optional Add-Ons

- Threat modelling and secure-by-design workshops
- Architecture updates with remediation guidance
- Policy and standards development (e.g., secure build baselines)
- Pre-implementation risk assessments for new systems
- Collaboration with vendors and integrators during design phase

---

Build Security Into the Blueprint

Don't bolt security on at the end. Let us review your architecture and help you build a secure foundation that supports your goals — without slowing you down.

Book a Security Architecture Assessment

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