OPERATIONAL TECHNOLOGY **AUDIT**

Secure Your Operations, Protect Your Future.

Digital innovation has brought significant changes to the way businesses operate. One of the most significant impacts has been the integration of IT and operational technology (OT), which has allowed for greater efficiency and improved decision-making capabilities. However, this integration has also created new cybersecurity risks. With OT systems increasingly relying on IT networks and software, they are vulnerable to cyber-attacks that could disrupt operations, cause physical harm, or lead to financial loss. As a result, organizations need to take proactive steps to secure their OT systems and ensure that they are protected from cyber threats.

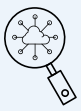
WHAT IS OPERATIONAL TECHNOLOGY AUDIT?

Operational technology (OT) systems are used to control and monitor critical infrastructure such as power plants, water treatment facilities, next-generation distribution centres, the energy sector, oil and gas and transportation. A cyber-attack on the OT environment could cause serious physical damage along with disruption of essential services.

Cybersecurity is crucial for both ICT and OT environments. It safeguards critical infrastructure, maintains safety, prevents financial loss, and meets regulations while protecting intellectual property.

- Maintaining safety
- Preventing financial losses
- Meeting regulatory compliance
- Safeguarding intellectual property

HOW IT WORKS?

PHASE 1		IDENTIFY THE SCOPE
PHASE 2		DETERMINE AUDIT OBJECTIVES
PHASE 4		CONDUCT WORKSHOP
PHASE 4		REVIEW DOCUMENTATION
PHASE 5		SITE VISIT
PHASE 6		EVALUATE SECURITY CONTROLS
PHASE 7		IDENTIFY VULNERABILITIES
PHASE 8		DETERMINE RISK LEVELS
PHASE 9		DEVELOP RECOMMENDATIONS
PHASE 10		FINALISE AUDIT REPORT

BENEFITS

An operational technology audit is a comprehensive assessment of an organisations industrial control systems (ICS). Supervisory control, data acquisition, (SCADA) systems and other operational technology infrastructure identifies not only vulnerabilities, but also evaluates security controls, assesses compliance, improves operational efficiency, enhances risk management, and increases stakeholder confidence. By conducting an OT audit, organisations will gain valuable insights into potential risks and vulnerabilities in its operational technology infrastructure and respond appropriately to mitigate those risks. The audit can help identify areas where operational technology infrastructure can be improved, reduce downtime, and improve productivity. It can also ensure that organisations meet legal requirements and regulatory obligations which reduces the risk of penalties.

WHY ORETA?

Oreta has a team of certified cyber security specialists who are dedicated to helping organisations stay secure in the digital age. With years of experience in the industry, Oreta has the knowledge and expertise needed to provide effective cyber security advisory services.

Oreta's services include everything from vulnerability assessments and penetration testing to security strategy development and incident response planning. Whether you're a small business or a large enterprise, Oreta can help you identify potential security risks and develop a plan to mitigate them.

At Oreta, we understand that every organisation has unique security needs. That's why we take a personalised approach to our services. Our team works closely with each client to understand their specific requirements and develop a customised solution that meets their needs.

For more information about how you can benefit from our services, please contact:

sales@oreta.com.au

Oreta.com.au/security-services

Linkedin.com/company/oreta/

ORETA

Taking you further...

ABOUT ORETA

Empowering business outcomes through advisory, delivery and managed services using network, cloud, security, and analytics technologies since 2015.

- Trusted by 250+ Businesses
- Scale and flexibility on demand
- Time given back to internal IT
- Invested in your success
- Partnership for now and the future