OT Site Assessment

Many organizations recognize that Operational Technology (OT) cybersecurity is becoming increasingly important, but struggle to determine where to start. Questions such as "How vulnerable are we?", "Which risks matter most?", and "What should we improve first?" are common.

Our OT Site Assessment provides a practical and cost-effective first step for improving OT Cybersecurity.

The OT Site Assessment gives you:

Understand your exposure

Identify which OT systems matter most to operations and where connectivity, remote access, or security gaps create risk.

Validate your controls

Review and test organizational, physical, and technical protections to see how they support the security of your OT environment.

Prioritize improvement

Focus investments and improvement work in order to build resilience, and align with industry good practices and regulatory expectations

Why choose the OT Site Assessment?

In just a few days on-site, we help organizations understand their current security posture, identify the most important risks, and establish a prioritized roadmap for improvement without disrupting operations. Designed for organizations at any stage of their OT cybersecurity journey, the assessment combines business, operational, physical, and technical perspectives to provide a clear view of your OT cybersecurity risks and improvement opportunities. Extensive documentation or a mature OT security program is not a prerequisite. All testing is coordinated with site personnel, with operational continuity and safety as priorities.

Our Modular Approach

Four complementary modules that can be delivered independently or combined to match your objectives and maturity level.

MODULE 0

OT criticality and exposure snapshot

A focused workshop examines your dependence on OT, potential business impact, external connectivity, remote access, and attack surface. The resulting profile helps you understand your site's criticality and exposure, and identify where improvement efforts should focus.

MODULE 1

OT maturity indicator

Interviews and available documentation examine governance, responsibilities, and operational processes. We review asset management, network security, access management, vulnerability management, monitoring, and incident response. A maturity indicator highlights areas to improve.

MODULE 2

Site tour and physical security review

An on-site review examines facility access, operator and server rooms, critical OT assets, and visitor management to identify gaps that could allow unauthorized access or tampering. Optional wireless survey. A passive wireless survey identifies unknown or unauthorized devices, checks approved inventories, and assesses potential wireless risks.

MODULE 3

Technical testing

Targeted reviews and testing validate controls, identify vulnerabilities, and assess the OT security architecture, based on the agreed scope and earlier findings.

IT/ OT perimeter: We assess IT/OT boundaries, including network segmentation, firewalls, remote access and data flows, to identify potential pathways for threats between business and operational networks.

Configuration reviews: We review selected OT systems and infrastructure for secure configurations, hardening, access controls, software versions and alignment with OT security best practices.

Selective probing and testing: Depending on the agreed scope, targeted testing may include protocol security checks, vulnerability identification, network service validation and system security testing.

Why choose Bureau Veritas

Bureau Veritas Cybersecurity is your expert partner in cybersecurity. We help organizations identify risks, strengthen defenses and comply with cybersecurity standards and regulations. Our services cover people, processes and technology, ranging from awareness training and social engineering to security advice, compliance and penetration testing.

We operate across IT, OT and IoT environments, supporting both digital systems and connected products. With over 300 cybersecurity professionals worldwide, we combine deep technical expertise with a global presence. Bureau Veritas Cybersecurity is part of the Bureau Veritas Group, a global leader in testing, inspection and certification.

Deliverables

The OT Site Assessment provides a clear and actionable overview of your current OT cyber-security posture, including:

- Executive management summary
- OT criticality and exposure profile
- Maturity indicator results
- Physical and technical security findings
- Prioritized remediation recommendations

Interested?

Contact us today:

cybersecurity@bureauveritas.com

cybersecurity.bureauveritas.com