Security Maturity Assessment

Do you know the current status of your cybersecurity? Understanding your information security level is essential to decide where to act next. With our Security Maturity Assessment, you get a clear picture, based on proven frameworks, to support strategic decision making.

A Security Maturity Assessment gives you:

Clear insight

Understand where your organization stands today on cybersecurity.

Standards-based view

See how your security aligns with frameworks like ISO 27001, NIST CSF, and IEC 62443.

Actionable advice

Get clear next steps to strengthen your security posture.

Why Security Maturity matters

Cybersecurity is not static. As threats evolve and systems grow more complex, staying ahead means knowing where you stand. This assessment gives you that clarity. It shows the effectiveness of your information security management systems and current controls. If gaps exist, our remediation advice will prepare you for today's risks. Whether you are managing regulatory pressure, preparing for audits, or improving internal governance, this service supports sound decision-making.

Assessments are based on internationally recognized frameworks, such as ISO/IEC 27001, the NIST Cybersecurity Framework (CSF) and the IEC62443 family. These standards help benchmark your organization's capabilities and guide structured improvements.

Depending on your needs, we offer different levels of assessment, from a one-day workshop to a full audit and improvement plan.

How it works: step-by-step approach

1 ESTABLISHING CONTEXT

The assessment starts with understanding your unique environment, drivers, challenges and goals. The context of the assessment ill be determined through an intial kick-off and a high-level risk assessment.

2 SECURITY MATURITY REVIEW

We assess your organization's maturity based on the five levels of the Capability Maturity Model (CMM). This is achieved through interviews, documentation review and expert validation.

3 SECURITY MATURITY AUDIT

For organizations seeking a deeper assessment, we offer a full audit. This service follows a similar approach to the review but includes verification of the effectiveness of existing controls.

OPTIONAL SERVICES

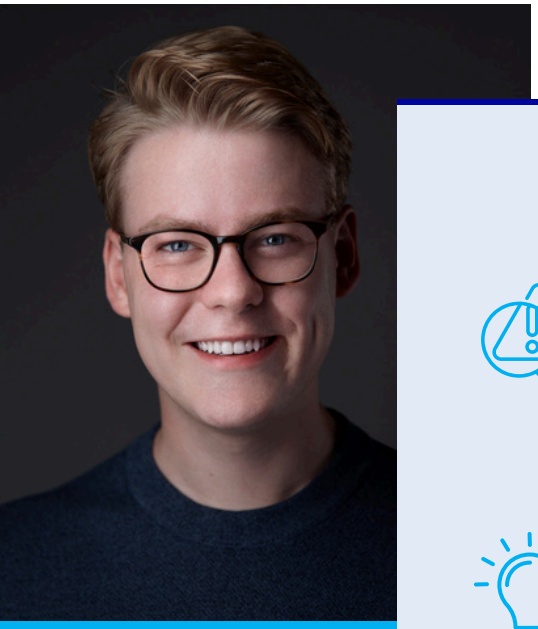
Detailed Risk Assessment
Performed before the maturity assessment, using ISO/IEC 27005. Assists with establishing a clear security target.

Custom Roadmap
After the assessment, we deliver a prioritized roadmap to ensure efficient and effective remediation of the gaps.

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.



Example case | Security Maturity Assessment

What problem did the client have?

A US-based renewable energy provider had grown rapidly through acquisitions but lacked a unified view of its cybersecurity maturity across business units. Leadership needed clarity to prepare for upcoming audits and prioritize cybersecurity investments to minimize operational risk.

Result

We conducted a Security Maturity Assessment using the NIST Cybersecurity Framework. Through interviews, document review, and a structured maturity analysis, we identified inconsistent risk management practices and gaps in incident response readiness. The client used the results to align its security roadmap across units, address key deficiencies, and prioritize improvements based on risk.

Interested?
Contact us today:

cybersecurity@bureauveritas.com
cybersecurity.bureauveritas.com