Secura
A BUREAU VERITAS COMPANY

Security Maturity Assessment

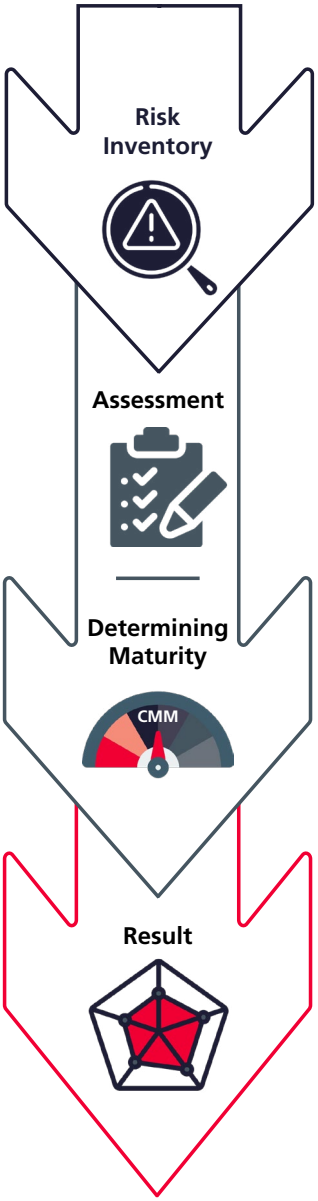
Cybersecurity risks are becoming increasingly important to organizations. The sophistication and number of digital attacks is ever growing. A major factor is the professionalization of criminal enterprises as well as the increasing dependence on digital resources and data. A hack, data breach or at worst a **ransomware attack**, can have a huge impact on business continuity. The consequences can range from reputation damage, fines and losing valuable and sensitive data to the costly affair of restoring business operations. Long downtime due to problems with digital infrastructure can sometimes even be fatal for a company. **How do you determine if your organization is resilient to these cybersecurity risks?**

The Need for Cybersecurity

In the last decade, cyber-attacks have become a daily affair and an existential threat for most companies. In combatting this threat, many companies struggle to have a full overview of the status of their digital security, the maturity of information security or the cyber resilience of the organization. The lack of this insight prevents organizations from answering the question to management on "how secure are we?" and structurally working on reducing cybersecurity risks.

To help organizations to get insight into their digital security Secura has developed the **Security Maturity Assessment** (SMA). The SMA will help your organization setting a baseline of the current information security maturity, identify both security risks and areas of improvement and monitor its progress over time. The SMA considers the three major pillars of cybersecurity: **people, process, and technology.** As the SMA is based on **(inter)national standards and frameworks**, it allows your organization to compare information security maturity to other organizations in a repeatable and independent manner.

SMA Methodology



GETTING ACQUAINTED

To deliver the most value, Secura consultants first need to get to know your organization. In this phase, variables like company size, goals, complexity, and the scope of the assessment are determined. By means of **a customized risk inventory**, the most important risks of the organizations are mapped out with a top-down (more general) or bottom-up (more detailed) approach, depending on the goals of the organization. This can be used to apply weights to certain controls or chapters.

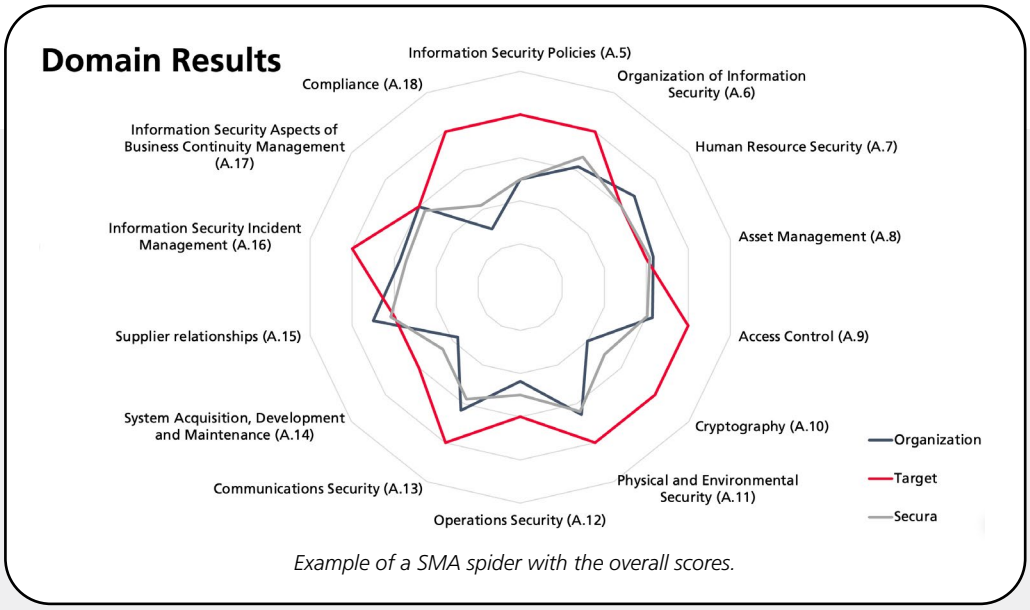
If desired and with the help of a Secura consultant, you can do a **self-assessment** based on the applicable standard or framework. The results of your self-assessment will be compared and challenged by the professional judgement of Secura in the later stages of the assessment to see how well the state of the information security is known by yourself.

EXECUTION

To assess maturity in a structured, repeatable, and independent manner, metrics are defined for each control of **one of the several (inter)national frameworks** offered (see bottom of page 3 for a list of these frameworks), which incorporate the qualities of **design, implementation**, and **operational effectiveness.** These metrics are used to assign one of five maturity levels to each control, which are based on the **Capability Maturity Model (CMM)**. The consultant will initially use evidence based on the documentation requested in the first phase to start assigning maturity levels to individual controls. If further information is required, documents will be requested, and relevant individuals will be interviewed.

RESULTS

When the assessment is done, you will receive a report and the SMA tool containing both the results of the optional self-assessment and maturity as determined by Secura. The report contains a management summary that describes the most important issues identified, the gaps in relation to the desired maturity and the overall score. The rest of the report goes into detail on our findings. Both the report and the tool contain dashboards, offering clear insight into the information security maturity of your organization. If desired, a plan of approach for increasing maturity can be drafted by the Secura consultant.



Example of a SMA spider with the overall scores.

Our SMA Services

The SMA approach consists of three levels: the Security Workshop, the Security Maturity Review and the Security Maturity Audit. Every assessment starts with a workshop to get to know the organization. Depending on your needs, this can be extended to a review or full audit. Optional extras like a full risk assessment and the creation of plan-of-approach after the assessment are available.

SECURITY **WORKSHOP** 1 DAY

During this workshop, variables like company size, goals, complexity, and the scope of the assessment are determined. A **quick scan** will be performed based on the selected standard or framework. After half a day of interviews and reviewing some key documentation, an **initial estimate of the information security maturity** will be given. A compact report with key recommendations will be provided.

SECURITY MATURITY **REVIEW** 2-10 DAYS

After the workshop, a maturity review can be initiated. An **expert review of the organizational maturity** is performed through documentation-review and interviews and can optionally be compared to a self-review. The maturity is determined **based on the five CMM levels of maturity**, where Secura has provided metrics for each level and control that incorporate the qualities of **design and implementation**. The quality of **operational effectiveness** is checked by doing spot checks with the help of the client. As a result of this assessment, a report and the SMA tool will be provided. These contain the outcome and the details of the assessment, as well as dashboards to visualize the results.

SECURITY MATURITY **AUDIT** 10-20 DAYS

Instead of a review, a full audit can be performed after the workshop. The process is largely the same, but the quality of **operational effectiveness** will be **verified more in-depth by the Secura consultants**. More time will also be spend verifying the maturity of individuals controls, which makes it ideal for larger organizations or organizations which are already at a high level of maturity.

OPTIONAL: RISK ASSESSMENT 2-5 DAYS

The SMA will start with a risk-assessment based on the ISO/IEC 27005:2018 standard.

OPTIONAL: IMPROVEMENT PLAN 2-5 DAYS

A prioritized list of concrete action items will be provided after the assessment.

By default, Secura offers the SMA on the following frameworks and standards. However, bespoke assessments can be carried out after consultation.

- ISO/IEC 27001 (2013 and 2022)
- NIST Cyber Security Framework (CSF)
- NIST CSF – Ransomware Resilience (RR)
- IEC62443 for OT environments
- NEN7510 for Medical environments
- BIO for Dutch Municipalities

Our Related Services

Secura's Security Maturity Assessment is designed to provide a wide variety of customers in various market sectors actionable insight into their information security maturity. However, every customer's challenge is unique. Related services that can be relevant to get in control of your digital security are:

IMPLEMENTATION SUPPORT

In addition to helping identify gaps and risks, Secura also offers implementation support for a wide range of standards and frameworks.

INTERNAL AUDIT

Preparing for certification? Secura can provide an internal audit, evaluating and offering potential improvements for effectiveness of risk management, control, and governance processes.

CISO-AS-A-SERVICE

Secura's CISO-As-A-Service opens the opportunity for small and midsize companies on execution and prioritization of cyber security management by a professional, without having to find and employ dedicated staff. This service can help you by managing security challenges as a result of the rapid and ever-changing risk landscape.

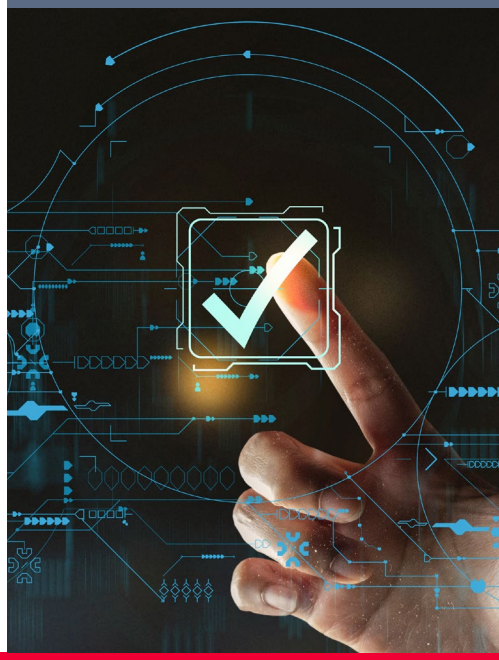
THREAT MODELING

The SMA offers insight into the maturity of your organization's information security. However, to inspect the digital resilience of your network architecture, a Threat Modeling session can be held. The service identifies the biggest technical weaknesses in your network design and offers actionable advice on mitigation.

Secura
A BUREAU VERITAS COMPANY

About Secura

Secura is a leading expert in digital security. We help our customers - from government and healthcare to finance and industry - to **raise their cyber resilience**. You can expect high quality security advice, testing, training and certification services from our experts. We believe in an **integrated approach to cybersecurity**: people, process and technology are equally important. Since 2021, Secura is part of the international Bureau Veritas Group.



Secura
A BUREAU VERITAS COMPANY

Interested?

Contact us today:

Follow us:

+31 88 888 31 00
info@secura.com
secura.com

BUREAU VERITAS
1828

Shaping a World of Trust