Security Maturity Review

Cyber risks are increasingly important to organizations. The professionalization of criminal organizations as well as the increasing dependence on digital resources and data play a major role in this. A data breach, hack or worse a **ransomware attack**, can have a huge impact on your organization. The consequences of a cybersecurity attack can be severe. The reputation of your organization, customers or partners can be seriously damaged. Fines may be levied, and restoring business operations can be a costly affair. Business may be lost, sometimes to the extent the business will fail. How to make sure your organization is resilient to these cybersecurity risks?

Secura has worked in information security and privacy for more than two decades. This is why we uniquely understand the challenges that you face like no one else and would be delighted to help you address your information security matters efficiently and thoroughly. We work in the areas of people, processes and technology. We offer a range of security testing services varying in depth and scope.

The Need for Cybersecurity

Many companies have no good overview and no firm grip on the maturity of the information security and cyber resilience within their organization. Often, the comprehensive overview is missing, which prevents organizations to structurally work on reducing security risks. To protect against this growing menace, Secura defined a Security Maturity Review and Assessment model framework, approach and services to help you in providing insight into your security by assessing the maturity of your organization's cybersecurity resilience. The Security Maturity Review and Assessment model is available in 3 flavors based on 3 international standards:

- ISO 27001;
- NIST Cyber Security Framework and
- IEC 62433.

On top of these 3 versions other standards and cross-references are used to strengthen the model and to support customers to dive deeper in certain domains with the knowledge and insight of more specific standards. For Risk Assessment we use ISO 27005, for example.

The Goal of Security Maturity Reviews & Assessments

The goal of the Security Maturity Reviews & Assessments is to provide insight into the security risks and the maturity of your cybersecurity organization in light of those risks. Secura assesses the effectiveness of the (implemented) security controls and measures, identifies deviations and vulnerabilities and provides a clear report and advice for follow up.

Your key benefits are:

- Evidence that you are in control of your cyber risks and measures towards customers and authorities;
- Raising the right security behavior in your organization;
- Risk inventory: Prioritizing the items that matter the most;
- The ability to perform the Maturity Review trough a self-assessment, followed up with an expert review.
- Avoiding fines and losses as a consequence of data leaks and security incidents;
- Cost optimization by improved process control.

The Framework

Secura defined a security framework and approach based on the NIST Cyber Security Framework covering the five security resilience stages, covering people, process and technology. Secura extended this framework with Governance (from the ISO 27001 standard) and Risk Management chapters (from ISO 27005). This framework helps you to assess the cybersecurity maturity and resilience of your organization from a management perspective.

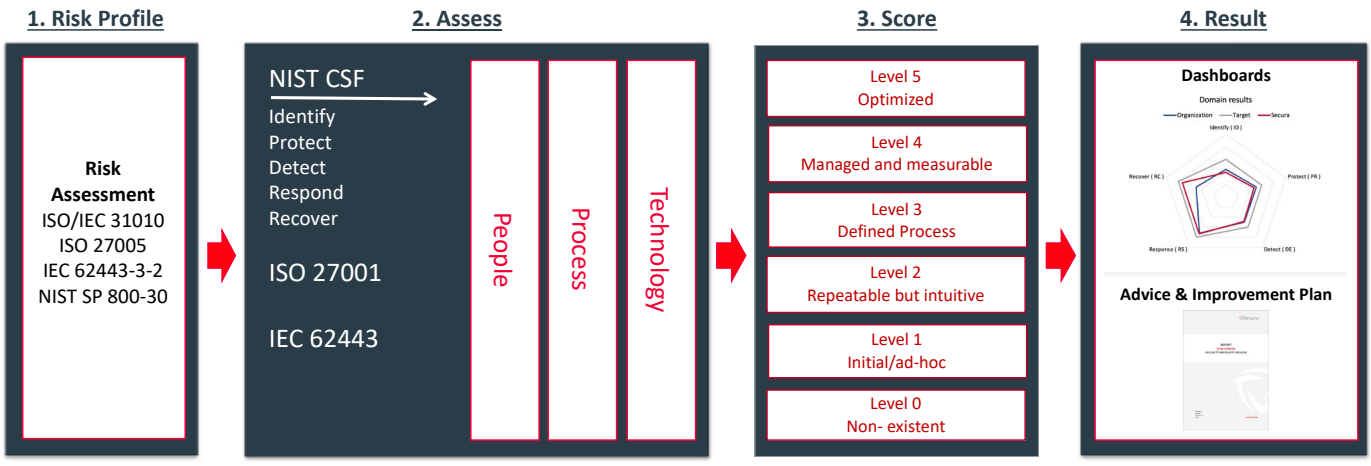


Figure 1. Secura Security Maturity Assessment Framework

Three Levels for Assessing your Organization

Secura developed three levels of services, ranging from a simple Quick Scan to a comprehensive Security Maturity Assessment. Depending on where you stand as an organization and what your needs are, you can select either of these levels, or take a stepwise approach.stepwise approach.

1. Security Maturity Quick Scan

A quick-scan including free reporting and recommendations. On the basis of a workshop with a selection of questions, you will get an initial estimate of the cybersecurity maturity of the organization. Focus for this Quick Scan is to review the design (presence) of the most important security controls linked to the highest risk domains.

1 day

2. Security Maturity Review

The Security Maturity in which all possible types of cyber risks are identified and the maturity of the organization is determined based on the information provided in a self-review and expert review. The self-review is optional. Focus for this Security Maturity Review is to thoroughly review the design and existence of security controls in order to validate the maturity of it, linked to the risks applicable to your organization. The output is a report consisting of:

- The maturity scoring per security objective and chapter;
- Recommendations to strengthen the security controls.

This will be presented in a closure meeting including a management presentation and the main points of attention.

2-9 days

3. Security Maturity Audit

The Security Maturity Audit is a comprehensive audit consisting of the following steps:

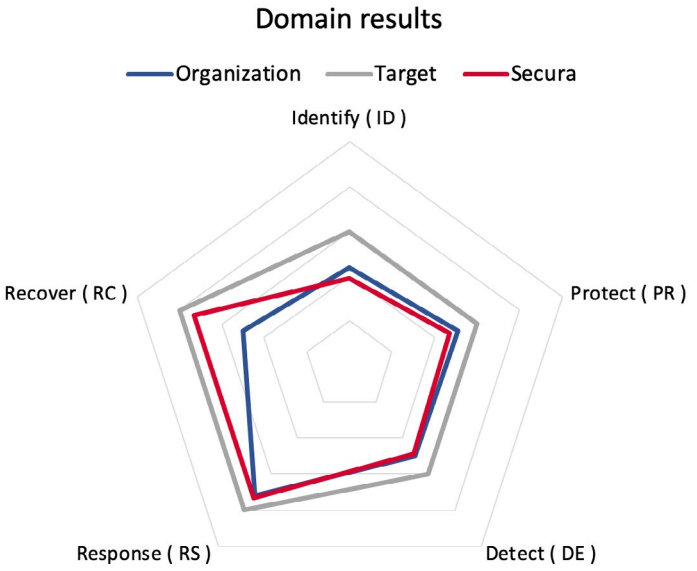
- Determining the risk profile of the organization in order to define the focus areas for the audit;
- The assessment of the organization covering all security controls according to the selected standard, covering people, process and technology; this includes collection of evidence, checks on operating effectiveness, resulting in findings per security objective;
- The maturity scoring per security objective and chapter;
- Recommendations and action plan to strengthen the security controls.

So, the focus of the Security Maturity Audit is the design, existence and the effectiveness of the security controls linked to the defined organizational risk profile.

10-30 days

The Result

The outcome of our Security Maturity Assessment services is clear insight into your current maturity scoring and the points of deviation from your own estimates, including showing the gaps to your desired maturity level.



Why Secura?

Since 2000, Secura has been supporting organizations with high-quality services. Secura has its origin in the technical and audit domain of IT security, which is an extremely complex and rapidly changing field in which a continuous race is going on between digital burglars and security experts.

Based on the technical expertise and knowledge required over the last decades, Secura has developed this Security Framework and the related services. Are you curious about what possibilities we can offer for your organization? Contact us today!

Secura's Security Maturity Assessment Methodology According to NIST CSF

1. Risk Profile

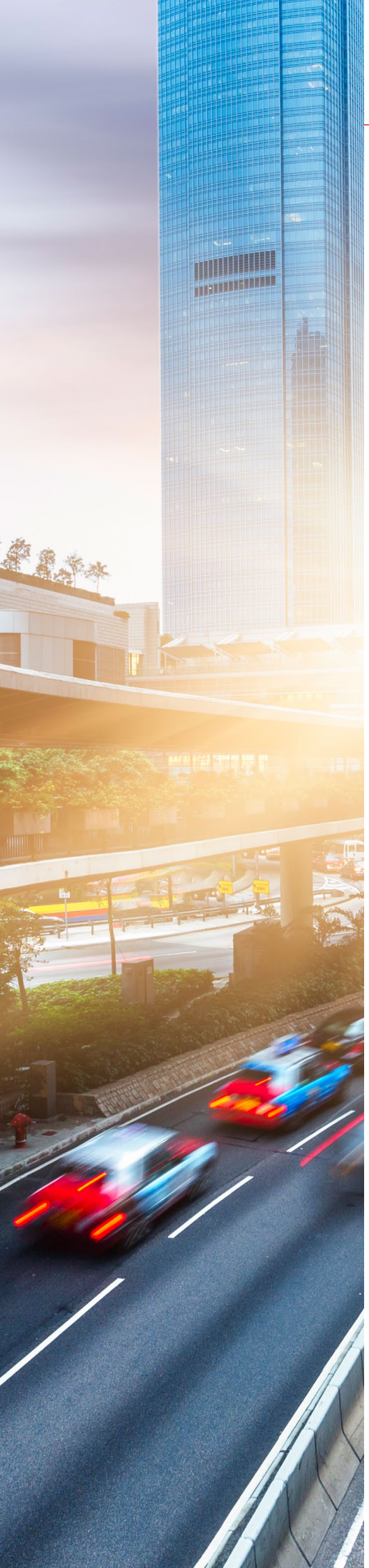
An in-depth risk assessment and analysis are one of the first steps in achieving effective security management.
In the approach of Secura the risk analysis is very key for determining the (inherent) Risk Profile of the organization in order to define the focus areas.

- For the Security Maturity Review a basic risk assessment is done
- For the Security Maturity Audit an organizational Risk Profile is determined.

2. Assessment

For the Assessment we chose relevant controls from the ISO 27001 (Governance & Risk Management) and the NIST Cyber Security Framework (Identify, Protect, Detect, Respond, Recover)'. This leads to the following scope of the assessment:

Domain	Scope
Identify	**Develop the organizational understanding of the business context, the resources that support critical functions to focus and prioritize its efforts,** consistent with its risk management strategy and business needs as defined and managed in the risk management domain. Relevant controls are covering asset management and determining the impact of the assets for your organization and the partners in the supply and delivery chain.
Protect	Protect covers **the measures that are preventive, and to a large extent are also derived from the ISO 27k standards with which the NIST CSF also has a mapping. Protect addresses the controls that aim to outline appropriate safeguards to ensure delivery of critical infrastructure services.** The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event. Relevant controls are user management, authorization management, network integrity, encryption measures, disposal measures regarding stored data, protection against data leaks.
Detect	The Detect domain is an important part of the criteria set as it includes **controls that define the appropriate activities to identify the occurrence of a cybersecurity event.** The Detect Function enables **timely discovery of cybersecurity events.** Relevant controls are focusing on ensuring that anomalies and events are detected, and their potential impact is understood, have implemented security continuous monitoring capabilities to monitor cybersecurity events and verify the effectiveness of protective measures including network and physical activities.
Respond	After defining detection controls, the Respond domain concludes with **appropriate actionable activities regarding a detected cybersecurity incident.** The Respond Function supports the ability to **contain the impact of a potential cybersecurity incident.**
Recover	After the respond to cybersecurity events, it might occur that systems and/or data should be recovered in a secure way. **The recover controls support timely recovery to normal operations to reduce the impact from a cybersecurity incident.** Relevant controls are covering the recovery planning processes and procedures to restore systems and/or assets affected by cybersecurity incidents, implementing improvements based on lessons learned and reviews of existing strategies Internal and external and last but not at least the communications during and following the recovery from a cybersecurity incident with stakeholders and management.



Coverage of the Security Maturity Review

The review and activities will cover all detailed controls/ requirements of the domains in this model and consist of the following elements:

- Interviews with subject matter experts, who are able to explain the implementation of various security controls. Examples are incident management or asset management;
- Documentation supporting the various processes, controls and reviews performed, e.g., procedure descriptions, flow charts and reports;
- Evidence, showing that people actually work according to the defined processes. Examples such as reviewing incidents or changes will be requested during interviews.

This approach provides a fair insight in the actual status, allowing us to report on findings, possible risks and recommendations for improvement (measures to implement). For the Security Maturity Audit also the operating effectiveness will be assessed. This is done based on review of evidence and spot checks on the effectiveness within the organization (observing and assessing controls "in working"). Operating Effectiveness is done with focus on the High-Risk Areas.

High-Risk Areas (in-depth analysis)

Every organization will have identified higher-risk areas or domains/processes to focus on, usually derived from risk assessments or management goals/ decisions. The results of the risk assessment will be used to determine these higher-risk areas for the assessment. In combination with Secura's experience in other large multinational organizations, we are able to assess these high-risks and other well-known areas of attention in-depth with a limited time-frame for the total Security Maturity Audit.

- The assessment activities for these areas will cover similar steps as described above, except for the evidence collection for the higher-priority areas where we follow a more strict approach to validate the evidence. For such areas, evidence will be based on the following possible steps (and combinations):
- Samples are selected randomly, and reviewed in detail. This applies to e.g., incidents or changes;
- Completeness checks on items such as changes implemented in production environments, verification that all security relevant log events are processed;
- Independent verification, e.g., establishing the actual system and application configurations match up with baselines.
- Depending on the result of the risk assessment or management goals/ decisions this can be extended with additional technical checks, such as inventory scans to verify the asset registration matches the actual assets.

This provides more detailed insight in the actual status, allowing us to report in more detail on findings, possible risks and recommendations for improvement.

3. Maturity Scoring

Per category of controls, we score the current level of maturity based on COBIT Maturity levels (see the table below). The actual score is determined by Secura based on the findings of the Security Maturity Assessment. Apart from our score, you have the possibility to provide your own scoring as well.

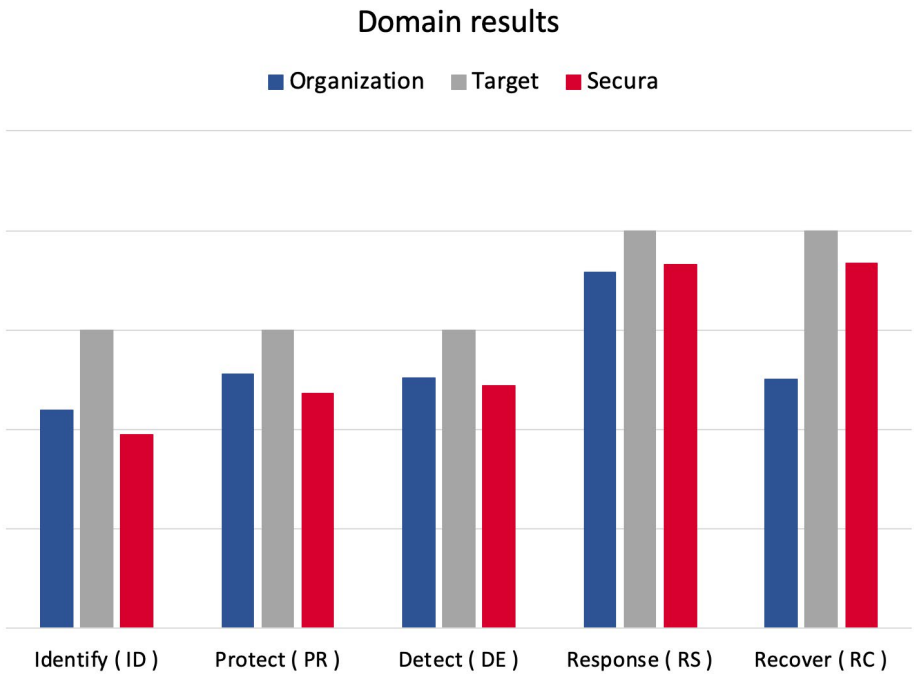
Based on these scores we can help you to define the aspired security levels. For the high-risk areas, it is our recommendation to have an ambition to go for maturity level 3 as least. To reach higher levels you may need to solve certain findings (also linked to the related risk). Secura can help you to select and prioritize those.

Maturity Level	Description
Level 0 Non-existent	**Complete lack of any recognisable processes.** The enterprise has not even recognised that there is an issue to be addressed.
Level 1 Initial/Ad Hoc	**There is evidence that the enterprise has recognised that the issues exist and need to be addressed.** However, there are no standardised processes. Instead, there are ad hoc approaches that tend to be applied on an individual or case-by-case basis. The overall approach to management is disorganized.
Level 2 Repeatable, but Intuitive	**Processes have developed to the stage where similar procedures are followed by different people undertaking the same task.** There is no formal training or communication of standard procedures, and responsibility is left to the individual. There is a high degree of reliance on the knowledge of individuals and, therefore, errors are likely.
Level 3 Defined Process	**Procedures have been standardised and documented, and communicated through training.** It is mandated that these processes should be followed, but it is unlikely that deviations will be detected. The procedures themselves are not sophisticated but are the formalisation of existing practices.
Level 4 Managed and Measurable	**Management monitors and measures compliance with procedures and takes action where processes appear not to be working effectively.** Processes are under constant improvement and provide good practice. Automation and tools are used in a limited or fragmented way.
Level 5 Optimized	**Processes have been refined to a level of good practice, based on the results of continuous improvement and maturity modelling with other enterprises.** IT is used in an integrated way to automate the workflow, providing tools to improve quality and effectiveness, making the enterprise quick to adapt.

4. Advice

Based on the maturity scoring, Secura indicates which control improvements help most raising the maturity level to the desired level. These measures are formulated high level, with aim to report the most important to involved Senior Management. Recommendations are prioritized based on the risk analysis and the maturity scoring.

In summary: Secura provides clear insight into the maturity of your security. We do this qualitative and quantitative; according to international standards (ISO 27001, ISO 27005, NIST Cyber Security Framework). As a next step Secura can help you to define an action plan to bridge the gaps identified. This helps you to get in control and get your cyber security at an acceptable level.



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