NIS2-Preliminary Assessment high

Purpose
The purpose of the assessment is to provide the organization with a preliminary assessment of whether the organization will be affected by the requirements of the NIS2 directive, as well as to what extent and for which services. In addition, the assessment comes with some high-level recommendations for the organization.

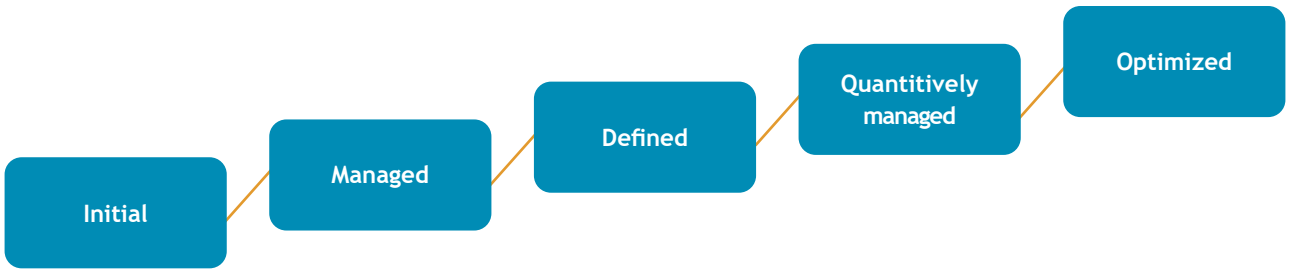
Assessment
The assessment consists of 1-3 interviews with the organization's management/IT management. This gives us an insight into your services and the systems that support any covered services. Based on the interviews held, we will, make a preliminary assessment of whether the organization is expected to be covered by the requirements of the directive.

Maturity
An assessment of the organizations cyber-maturity based on questions from the CSF-standard will be performed. This will be based on answers from the interviews as well as relevant documentation and can be used as a baseline for the organizations management to define targets for which level of maturity the organization must strive to achieve in the long term. The CSF-standard works with five areas, which can be seen in the figure and described below.

Identify:
The ability to identify risks related to people, systems, assets, and data.
Protect:
The ability to protect critical processes through safeguards.
Detect:
The ability to detect security incidents through targeted activities.
Respond:
The ability to effectively handle identified security incidents.
Recover:
The ability to restore operations in the event an incident and to continuously mitigate vulnerabilities.

Maturity levels
Based on the five areas a maturity level will be scored, based on the CMMI model as described below.

Level 1: Initial
The organization has no or few risk management processes and works very little with cyber and information security.
Level 2: Managed
The organization's risk management processes within information security are not all formalized, and risk is to some degree handled ad hoc.
Level 3: Defined
A method for risk management has been established, which is widespread in the organization and approved by management but is not fully anchored through comprehensive policies.
Level 4: Quantitively managed
The organization's risk management is approved by management and anchored through comprehensive policies. Practices are regularly updated based on changes in business requirements and environment.
Level 5: Optimized
The organization continuously optimizes implemented processes or approved policies on the basis of activities and experiences.



Report
We will prepare a short report (4-5 pages) that briefly describes the reasoning to the assessment, as well as which services are likely to be covered by the directive. The report will also describe what it means for the organization and come up with high-level recommendations on which areas should be prioritized.

Presentation
The report is presented to the organization at a one-hour physical meeting with slides highlighting the relevant points. There will be an opportunity to ask clarifying questions.

Output
The preliminary analysis will provide the organization with the following:

- A preliminary assessment of whether the organization will be directly or indirectly covered by the NIS2 directive
- An overview of which systems will be covered
- A maturity assessment in relations to the NIS2 requirements
- A high-level description of what is important if the organization is covered by the NIS2 directive
- Recommendations for which areas should be prioritized if the organization is covered by the NIS2 directive
- Suggestions for concrete actions that should be prioritized by the organization

GLOBETEAM

Address

Globeteam A/S
Virumgårdsvej 17A
DK-2830 Virum

Contact

Market Manager Kim Lindberg
Tel.: +45 5361 5020
Mail: kil@globeteam.com