Cybermeter

National framework for the assessment of cybersecurity capabilities

User guide

Contents

1 Introduction

Threats to critical infrastructure have increased and become more diverse. Cyber threats, in particular, have increased and protection against them has become an integral part of securing the functioning of our information society and security of supply. Because functions are interdependent, it must be ensured that every organisation critical for the functioning of society is prepared for cyber threats. This calls for national cooperation to develop cybersecurity across different organisations, sectors, and society at large.

Currently, cybersecurity is measured using different frameworks that vary from one organisation and sector to the next. Results produced using these different frameworks are not often comparable, which makes it difficult to benchmark the results and set harmonised development goals. What is lacking is not only a shared set of indicators, but also ways to confidentially share information about the maturity levels of organisations and best practices to develop cybersecurity.

Cybermeter is a national cybersecurity assessment framework developed by the National Cyber Security Centre (NCSC-FI) of the Finnish Transport and Communications Agency (Traficom). The framework provides a harmonised approach to the assessment and development of cybersecurity capabilities. The framework has been designed based on national and international best practice, and it provides different organisations, sectors, and the society at large with the means to comprehensively assess the status of cybersecurity capabilities and to identify potential development areas. A national approach enables benchmarking between companies and sectors and sets a common language for the measuring and developing cybersecurity capabilities within and between organisations. The role of NCSC-FI is to secure continuity of the framework and to facilitate the sharing of confidential information in cooperation with critical organisations about best practices, recommendations, and reference results.

NCSC-FI offers Cybermeter free of charge for companies, associations, and public organisations to use. The framework can also be used and adapted by commercial parties orauthorities. The most up-to-date material package and terms of use for the framework are available to download for free at www.kybermittari.fi in Finnish, Swedish and English. The primary target group for the framework includes critical infrastructure companies, however, the framework is also suitable for use by organisations of all sizes, regardless of the sector.

The benefits of Cybermeter for companies, associations, and public organisations include:

- An open and free-to-useframework for assessment and long-term development of cybersecurity capabilities;
- Benchmarking capabilities towards other Finnish organisations and sharing of best practices; and
- A shared framework and language for communicating, assessing, and developing cybersecurity capabilities within organisations, with subcontractors or with the authorities.

On a national level, Cybermeter supports the national cybersecurity strategy, one strategic element of which is to develop the verification, testing and assessment of the provision of products and complete solution environments related to critical functions, as well as recommendations for their use. The large-scale use of the framework supports the creation of situational awareness, supports the activities and decision-making of competent authorities, and helps with the optimal allocation of national development resources.

1.1 Target audience

This user guide is intended to support the deployment and use of Cybermeter by providing instructions and advice on how to use the framework, conduct assessments, and use printouts. This user guide is specifically intended for managers of organisations, specialists in risk management and cybersecurity, and others involved in the assessment process. This guide has been divided into the following parts:

- **Section 2** describes how organisations can best use Cybermeter and what its deployment requires.
- **Section 3** presents the structure and operating principles of Cybermeter.
- **Sections 4 and 5** include detailed instructions and recommendations for facilitators and other participants in assessment processes.
- **Section 6** includes a glossary of terms related to Cybermeter and cybersecurity.

This user guide is intended to be used together with the self-assessment tool.

1.2 Background

Cybermeter was developed by NCSC-FI and the National Emergency Supply Agency during 2019 and 2020, and its first version was released in October 2020. NCSC-FI is responsible for the maintenance and further development of the framework.

The aim was to develop the framework using a widely known international frame of reference which is updated actively and is openly accessible. On the basis of these criteria and an extensive analysis process, two frames of reference were selected, which Cybermeter is primarily based on. These are the *National Institute of Standards and Technology Cybersecurity Framework* (NIST CSF) [1] and the *U.S. Department of Energy Cybersecurity Capability Maturity Model* (C2M2) [2] [3]. In addition, Finland’s national risk assessment (2015) [4] and the Security Strategy for Society [5] were used in the preparation of the guidelines.

Cybermeter is based on version 1.1 and draft version 2.0 of the C2M2 whose domains and practices have been translated into Finnish and Swedish from English. At the same time, the domains and practices have been adapted to better meet Finnish conditions and demands of Finnish organisations. These ten domains form the framework of Cybermeter. In addition to this framework, NCSC-FI has prepared separate domains regarding the protection of critical services and investments in cybersecurity. Cybermeter also includes NSCS-FI’s indicative cross-reference with NIST CSF which enables the results produced by Cybermeter to be reported on the basis of the divisions defined in NIST CSF.

Organisations can share the assessment results produced using Cybermeter confidentially with NCSC-FI. NCSC-FI can use the results to carry out its statutory tasks. It can also use the results to define anonymised reference and recommendation levels, which it can offer to organisations to support the use of Cybermeter and the development of cybersecurity. Any reference and recommendation levels will be defined so that no individual organisations or their assessment results can be identified from them. More detailed information about the sharing of assessment results and reference results is available at www.kybermittari.fi.

2 Using the Cybermeter Framework

This section describes an assessment process recommended by NCSC-FI which makes it easier for organisations to use Cybermeter. The process has been prepared on the basis of experiences obtained from pilot projects.

It is recommended that Cybermeter be used as part of a continuous operational assessment and development process. The five-step process consists of the launch of assessments, preparations, the assessment process, and the identification and implementation of development activities. When the development activities progress and the operating environment changes, the assessment must be updated, or a re-assessment must be conducted. The assessment process and its continuity are presented in Figure 1.

Cybermeter assessments can be conducted as a one-off process. However, the framework provides the best benefits when it is part of continuous operational development. It is also recommended that assessments be integrated into organisations' risk management processes, and the development of cybersecurity based on assessments become an integral part of other development activities in organisations.

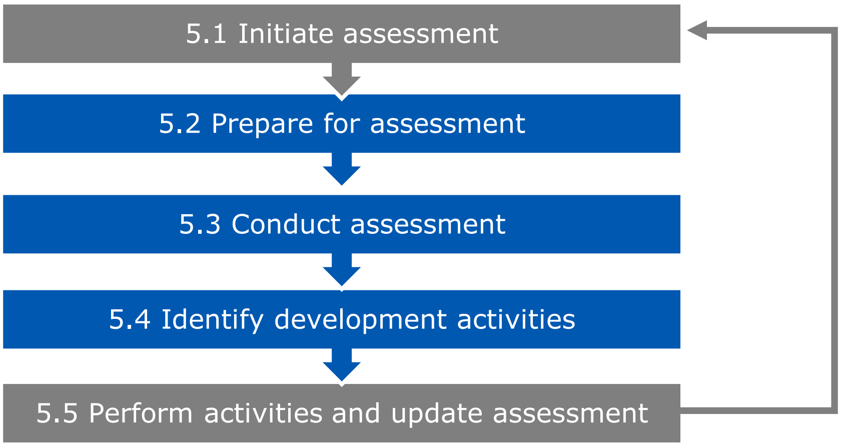

5.1 Initiate assessment
5.2 Prepare for assessment
5.3 Conduct assessment
5.4 Identify development activities
5.5 Perform activities and update assessment

Figure 1. A five-step cybersecurity assessment process, which makes it easier to use Cybermeter in organisations.

Each process step and their key participants and tasks are described briefly below. A summary of each step and key tasks is presented at the end of the section. More detailed instructions on how to use Cybermeter are presented in Section 4.

2.1 Initiate assessment

Participants: An organisation's management team or other decision-making body.

Tasks:

1. Deciding on the implementation and target for the assessment; and
2. Appointing a sponsor and facilitator for the assessment who are responsible for further measures.

An assessment starts by deciding to assess a pre-defined area to a pre-defined extent. It is recommended that this decision is made by an organisation's management team or other decision-making body in the area of cybersecurity and risk management. This provides sufficient support and preconditions for the assessment and the long-term development of cybersecurity.

Selecting *the operating area* to be assessed is the most important decision. The "operating area" means the services or functions which are critical for the organisation or society at large and whose cybersecurity is to be assessed. The assessment may cover the entire organisation, while it is recommended, especially in larger organisations, that it only focus on one critical service or function at a time. Assessing operations as a whole requires that processes and practices are sufficiently harmonised throughout the operating area being assessed. If the aim is to assess several operating areas, it is recommended that a separate assessment is launched for each area.

The assessment facilitator can be selected from inside the organisation or from an external service provider.

Key criteria include previous cybersecurity experience, time allocation and the organisation of the assessment process.

Another important decision is to appoint *an assessment sponsor* and *an assessment facilitator* who is responsible for the practical implementation of the assessment. These can be appointed from inside or outside the organisation. It is recommended, that these appointments are made by the management team or other decision-making body. The assessment sponsor should be a member of the management team or another person in a managerial position, while the assessment facilitator may also be a specialist of an external service provider. In addition, the assessment can be outsourced to a service provider in full or in part.

Once the decision on the assessment has been made and the sponsor and facilitator have been appointed, they will assume responsibility for the practical implementation.

2.2 Prepare for assessment

Participants: The assessment sponsor and facilitator together.

Tasks:

1. Defining the operating area being assessed more closely and identifying critical dependencies in that area;
2. Identifying the specialists required for the assessment; and
3. Agreeing upon the assessment method and schedule.

The assessment sponsor and facilitator define the operating area being assessed in more detail and identify any dependencies critical for the reliability of the operating area. Critical dependencies include the systems, processes and data assets required to provide the selected services or functions. If any challenges are identified at this stage regarding the scope of the assessment, the decision on the selected operating area can be re-assessed by the management team. Section 4.2 presents more detailed instructions for identifying the operating area and its dependencies.

***The operating area should be defined** in detail so that the assessment can be completed within the pre-defined time and the results can be later interpreted correctly.*

*An assessment **in the form of a workshop** has been found to be the most popular method.*

On the basis of the operating area to be assessed and its dependencies, the assessment sponsor and facilitator identify the specialists required from the organisation. The specialists add necessary skills to the assessment from their respective areas of responsibility, such as business operations, risk management, data management or other processes. The suitable number of participants varies from one organisation to the next.

On the basis of the scope of the assessment, the number of participants and the preferences of the organisation, the assessment sponsor and facilitator agree upon the assessment method. It is recommended that a workshop- or personnel driven assessment be used. In a workshop-driven assessment, participants are invited to one or more assessment workshops, during which they conduct the assessment from start to finish. In a personnel-driven assessment, different assessment areas are divided between the participants, and the assessment facilitator compiles the final assessment from the different responses. The advantages of different assessment methods are described in Section 4.3.

Once all the factors above have been defined, the assessment sponsor and facilitator will agree upon the assessment schedule. It is recommended that assessment meetings and participating specialists are booked beforehand.

2.3 Conduct assessment

Participants: Assessment facilitator, assessment sponsor and the organisation’s specialists.

Tasks: Conducting the assessment based on the selected assessment method using the Cybermeter framework.

Estimated duration: One to two working days.

The assessment facilitator is responsible for practical arrangements and training the organisation’s participating specialists regarding the use of Cybermeter. Practical arrangements include meeting invitations, the distribution of material and the compilation of responses, depending on the selected assessment method. Training can be provided using Cybermeter’s user guide and other supporting material.

The assessment is conducted using the Cybermeter self-assessment tool. The participants respond to questions related to cybersecurity practices and their implementation in the organisation’s operations. The tool steers the assessment process and defines the organisation’s maturity indicator level on the basis of responses as the assessment progresses.

2.4 Identify development activities

Participants: Assessment facilitator, assessment sponsor, the organisation’s specialists, and owners of development plans.

Tasks:

1. Analysing assessment results;
2. Defining any target level for activities; and
3. Identifying and prioritising key development activities.

The assessment facilitator is responsible for summarising and analysing the assessment results together with the assessment sponsor, the organisation's specialists, and owners of development plans. Reports produced automatically by the Cybermeter self-assessment tool help to analyse the results and to identify the strengths and weaknesses of the organisation's operations using several different indicators. If the organisation also uses reference or recommendation levels of reference groups, the reports can be enriched with information about the average maturity indicator level in the sector, for example.

***The target level** should be defined on the basis of reference/recommendation levels that are available from NCSC-FI.*

In general, it is recommended that all operations are first at level 1.

To identify suitable development activities, it is recommended that the organisation's target level of cybersecurity is always defined. It may not be cost effective to strive for the highest maturity indicator level in all areas being assessed. A sufficient level can be defined on the basis of achieved results, any reference and recommendation levels of reference groups, or the organisation's internal goals. These can be related to business operations or could be based on threats identified in a risk assessment. For organisations that conduct an assessment for the first time, the target level is usually defined on the basis of results and findings of the first assessment. In general, it is recommended that all organisations aim at least at maturity indicator level 1 in all sections.

On the basis of the assessment results and the target state, the development activities that the organisation should take to develop its operations and achieve the target state can be identified. The measures are defined in a development plan, which should include not only the prioritisation of the measures, but also at least a measure-specific schedule, responsibility plan, and a more detailed implementation plan. Cybersecurity cannot be developed separately from other operations, which is why the development plan must be prepared addressing the organisation's regular operational planning and budgeting processes. These affect decision-making and the schedule set for fulfilling the plan.

Once the development activities have been selected and schedules have been set for them, the responsibility for coordination will transfer to the appointed owners of the development plans.

2.5 Perform activities and update assessment

Participants: Owners of development plans, the organisation's specialists, and the organisation's management team or other decision-making body.

Tasks: Carrying out planned development activities, updating the assessment and launching a re-assessment process, if required.

The use of the Cybermeter framework must be seen as a process in which the assessment and development activities alternate regularly. The maturity indicator level of cybersecurity can be raised step by step towards the target level defined in accordance with the organisation's risk-carrying capacity.

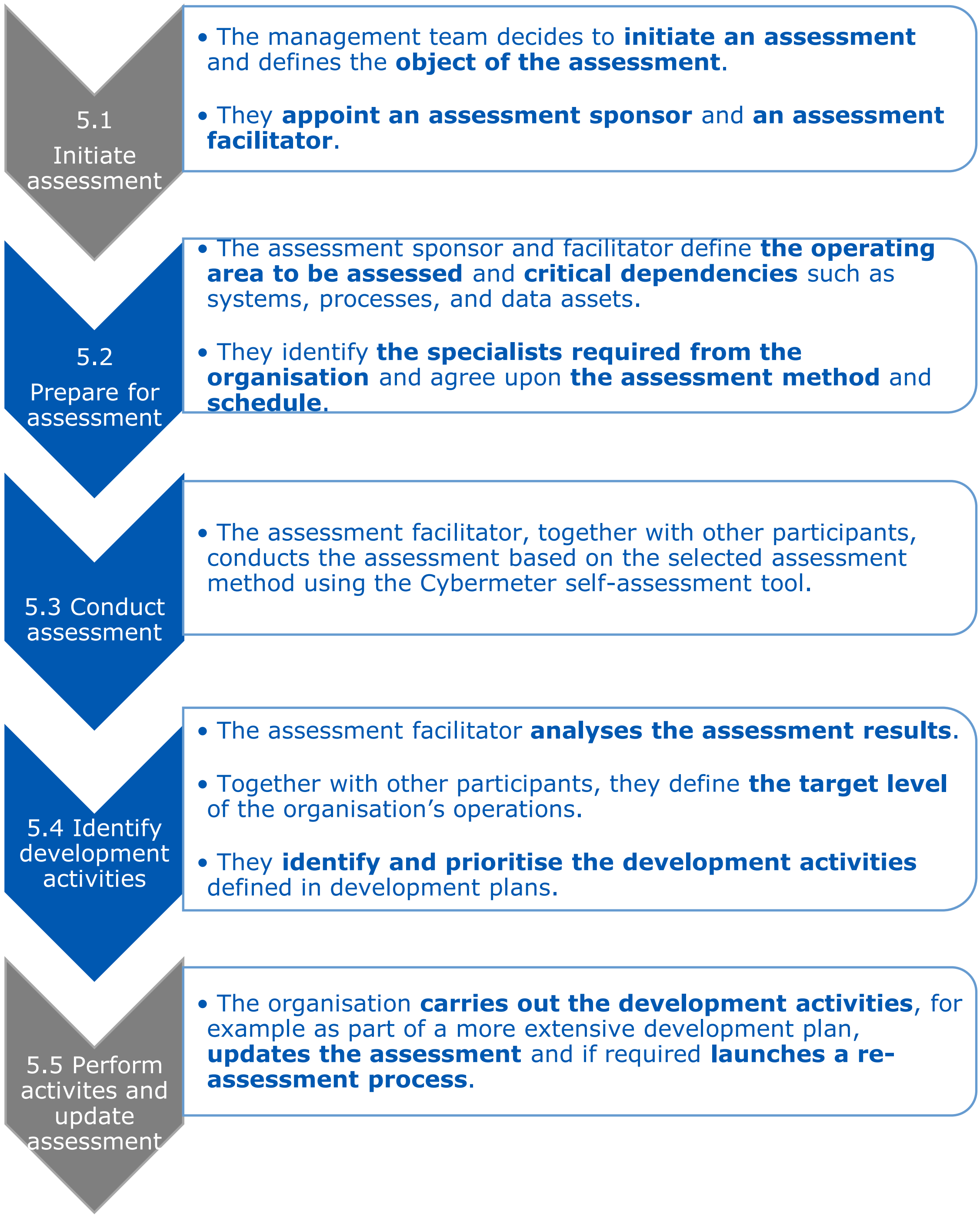
***A re-assessment** should be conducted every one to two years, depending on the organisation and the assessed area.*

The key task of development plan owners is to coordinate the implementation of the plans and maintain an overview of the progress of the measures taken. The goal is to ensure that the decided measures are taken and a correct time for updating the assessment is identified.

The assessment should be updated, or a re-assessment should be conducted when the development plans progress or the organisation’s operating environment changes. The advantages of the Cybermeter approach can best be utilised when operations are re-assessed regularly, and the impact of the development activities are also visible in reports. The Cybermeter self-assessment tool enables benchmarking with previous assessments, making it easier to monitor and report the impact of the development activities.

Summary and checklist of the assessment process

Key steps in the Cybermeter assessment process and key factors to be considered during each step are listed below.



5.1 Initiate assessment

- The management team decides to **initiate an assessment** and defines the **object of the assessment**.
- They **appoint an assessment sponsor** and **an assessment facilitator**.

5.2 Prepare for assessment

- The assessment sponsor and facilitator define **the operating area to be assessed** and **critical dependencies** such as systems, processes, and data assets.
- They identify **the specialists required from the organisation** and agree upon **the assessment method** and **schedule.**

5.3 Conduct assessment

- The assessment facilitator, together with other participants, conducts the assessment based on the selected assessment method using the Cybermeter self-assessment tool.

5.4 Identify development activities

- The assessment facilitator **analyses the assessment results**.
- Together with other participants, they define **the target level** of the organisation’s operations.
- They **identify and prioritise the development activities** defined in development plans.

5.5 Perform activites and update assessment

- The organisation **carries out the development activities**, for example as part of a more extensive development plan, **updates the assessment** and if required **launches a re-assessment process**.

3 Cybermeter maturity model

The Cybermeter maturity model and its key properties are described in this section, including especially the structure of the maturity model and the calculation model for the maturity indicator level.

Cybermeter represents a maturity model designed for the assessment and development of cybersecurity capabilities. The model serves to assess cybersecurity capabilities and guide development activities at four maturity indicator levels (0–3), representing systematic and advanced activities from weaker to stronger. The aim is that organisations define the current state of their activities and advance from one level to the next towards better and more effective activities.

Level 0 Activities do not meet basic requirements.

Level 1 Activities meet basic requirements, but mainly ad hoc, and the level of activities may vary from one situation to the next.

Level 2 Activities are more advanced and comprehensive than at lower levels. In addition, the following describe the management of cybersecurity:

- Documented processes and practices;
- Sufficient resources and skills; and
- Defined roles and responsibilities.

Level 3 Activities are advanced and comprehensive. In addition, the following describe the management of cybersecurity:

- Activities are steered by the organisation’s policies (or similar guidelines);
- Performance goals have been set for activities, and they are monitored; and
- Documented processes and practices are in line with the organisation’s standards, and their development is continuous.

3.1 Key concepts

Different concepts are used in conjunction with Cybermeter. Understanding them is important in order to apply the framework and interpret its results correctly. Four concepts are presented below, and a larger glossary of concepts related to Cybermeter and terms related to cybersecurity are presented in Section 6.

Capability means the ability to operate correctly in a specific area and use individual skills and resources to achieve objectives. To use the capabilities of organisations, combinations of three elements are often required, including operating models and processes, personnel and skills, as well as information and systems. Cybermeter helps to assess and develop organisations’ capabilities with regard to cybersecurity.

A maturity model examines activities at levels or steps, with the aim of climbing towards more systematic and advanced activities. Each level includes pre-defined objectives or requirements that the assessed activity should fulfil at the specific level. These objectives and levels typically represent best practices and may comply with an act or standard. In the maturity model, activities are typically divided into different domains, each of which is approached separately. Cybermeter assesss organisations' cybersecurity capabilities using four different maturity indicator levels and 11 assessed domains.

Used in conjunction with Cybermeter, an **operating area** is a concept meaning the services or functions which are critical for the organisation or society at large and whose cybersecurity is to be assessed. In addition to services, the operating area covers processes, systems, and data resources which are critical for the provision of services. Identifying and clearly defining operating areas play key parts in assessments and the use of results.

3.2 Domains, objectives, and practices

Cybermeter consists of 11 cybersecurity *domains*, *objectives* set for each domain and *practices* that measure the fulfilment of the objectives. The practices represent typical and proven cybersecurity procedures that companies from different sectors follow in their operations. Each practice represents a specific difficulty/maturity indicator level and is associated with a specific cybersecurity objective. The practices have been grouped according to objectives and difficulty levels.

Domains
The Cybermeter framework examines the following 11 domains:

1. Protection of critical services (CRITICAL);
2. Risk management (RISK);
3. Supply chain and external dependencies management (DEPENDENCIES);
4. Asset, change and configuration management (ASSET);
5. Identity and access management (ACCESS);
6. Threat and vulnerability management (THREAT);
7. Situational awareness (SITUATION);
8. Event and incident response (RESPONSE);
9. Workforce management (WORKFORCE);
10. Cybersecurity architecture (ARCHITECTURE); and
11. Cybersecurity program management (PROGRAM).

While this is the recommended assessment order, the domains can also be assessed in another order. It is recommended that the assessment covers all domains so that the end result is an overview of the organisation's cybersecurity activities and that any hidden vulnerabilities can be identified.

Objectives
Cybermeter consists of 52 objectives that have been divided so that each Cybermeter domain consists of three to five cybersecurity objectives. These represent typical and proven cybersecurity objectives.

The objectives and their inherent practices represent either:

- Cybersecurity objectives; or
- General management objectives.

Cybersecurity objectives represent objectives that each organisation should achieve in their activities to protect against cyber threats (see management measures that represent objectives related to the stabilisation of activities). Each domain has separate pre-defined cybersecurity objectives.

General management objectives measure how stabilised the organisation's activities are. The assessed practices are the same in each domain. It should be noted that no management objectives have been set for maturity indicator level 1. In other words, activities do not yet need to be stabilised and no formal processes need to be followed to reach level 1.

Practices
The cybersecurity maturity indicator level is defined by assessing practices that represent activities. Each Cybermeter domain and objective consists of a group of practices. The practices represent typical and proven cybersecurity procedures that organisations from different sectors follow in their operations. The practices have been divided according to objectives so that a specific group of practices represent activities at a specific maturity indicator level.

3.3 Maturity indicator level calculation model

The Cybermeter maturity indicator level calculation model defines organisations' maturity indicator level on a scale from 0 to 3. The maturity indicator level is defined in accordance with the practices implemented and their difficulty level. The more difficult the practices that are implemented are, the higher the maturity indicator level in the assessed area is.

The maturity indicator level is calculated at three stages:

1) Each practice is assessed either as implemented or not implemented.

2) The maturity indicator level of each objective is calculated on the basis of implemented practices (percentage); and

3) The maturity indicator level of each domain is defined according to the maturity indicator level of the lowest objective in the domain.

As a result, the cybersecurity maturity indicator level in all 11 domains is calculated.

Stage 1: The implementation of the practices is assessed using four response options.

1. **Not implemented** – the organisation does not implement the described practices;
2. **Partly implemented** – the organisation is starting to implement the described practices or activities are otherwise flawed in practice;
3. **Mostly implemented** – the organisation implements the described practices, at least mainly so, although development may still be in progress;
4. **Completely implemented** – the organisation implements the described practices, and no significant development is required.

Application instructions: If an organisation's practical implementation is flawed, response option 1 or 2 should be selected, even if development plans were prepared *to correct the flaws. The assessment should then be updated as development progresses and is completed.*

Stage 2: The maturity indicator level of the objectives is calculated as follows:

- At level 1, all (100%) practices at the specific level must be implemented.
- At level 2, more than half (>50%*) of the specific level's practices *and* all (100%) level 1 practices must be implemented; and
- At level 3, more than half (>50%*) of the specific level's practices *and* all (100%) level 1 and level 2 practices must be implemented.

For calculating the percentages, the four response options are summarised to be either implemented or not implemented so that options 4 (Completely implemented) and 3 (Mostly implemented) are regarded as implemented.

Stage 3: The maturity indicator level of the domains is defined according to the maturity indicator level of the lowest objective in the domain. If a domain consists of three objectives, whose maturity indicator levels are 1, 2 and 3, the domain's maturity indicator level will be the lowest of these, i.e. maturity indicator level 1.

The calculation model highlights comprehensive risk management, emphasising the significance of the weakest area. To attain a specific maturity indicator level, all or more than half of the specific maturity indicator level's practices must be implemented, depending on the level. It is not possible to progress to the next maturity indicator level until *all* the practices required for the lower maturity indicator levels have been implemented. In other words, organisations cannot attain higher maturity indicator levels until their activities fulfil the requirements set for a specific maturity indicator level regarding all assessed domains.

***Note:** This differs from the calculation model used in the C2M2 in which, to attain each level, all the practices of the specific level and lower levels must be implemented. The Cybermeter calculation model is a lighter version so that it better highlights development activities carried out at higher maturity indicator levels, even if a single practice at the specific maturity indicator level has not yet been implemented.

In addition, the following needs to be considered regarding the maturity indicator levels of the Cybermeter maturity model:

Maturity indicator levels are domain-specific. The maturity indicator level of each domain is defined on the basis of the objectives and practices set for the domain. Because the domains are not interdependent, companies may attain highly different maturity indicator levels in different domains.

Maturity indicator levels are cumulative. Attaining a maturity indicator level requires that the practices of the current level are implemented and that the practices for all the lower levels are implemented. A high level of maturity cannot be reached if the groundwork has not been done properly, despite advanced or expensive actions.

Setting target levels. A suitable target level depends on the organisation and sector. Objectives should be set for each domain, and they should be in proportion to the organisation's current state, business objectives and risk assessment, as well as any reference or recommendation levels in the sector.

4 Facilitator Guide - instructions for the facilitator

This section includes detailed instructions on how to use Cybermeter. This section is intended to support the assessment facilitator and other participants in preparing for the assessment, conducting the assessment, and using the results. The following subsections describe key individuals in the assessment process, the operating areas, assessment methods and the use of assessment results and reports in more detail.

4.1 Key individuals and roles

For the assessment, it is recommended that key individuals are identified and assigned for the following roles: assessment sponsor, assessment facilitator, the organisation’s specialists participating in the assessment, and owners of any development plans.

The assessment sponsor creates preconditions for conducting the assessment and is responsible for the success of the assessment together with the assessment facilitator. The sponsor’s task is to ensure sufficient resources for the assessment and to ensure the support of the organisation’s management. Another important role is to engage the management level in the long-term development of cybersecurity. The assessment sponsor must always be appointed from inside the organisation.

The assessment facilitator is responsible for conducting the assessment, supported by the assessment sponsor. The assessment facilitator is responsible for assessment preparations and practical arrangements, as well as the processing of results. In addition, the assessment facilitator is responsible for learning how to use Cybermeter and its self-assessment tool, and for teaching other participants to use them. The assessment facilitator must have not only cybersecurity skills, but also the ability to organise and schedule the assessment process.

The assessment facilitator can be appointed from inside the organisation or from an external service provider. The role can also be divided so that a person responsible for the assessment is appointed from inside the organisation, while a person responsible for practical arrangements and conducting the assessment is appointed from the outside.

- **Internal assessment facilitator.** This role can be assigned to the information security manager or a cybersecurity specialist or another person specialised in this area.

- **External assessment facilitator.** The expertise of an external service provider can be used in the assessment process as the assessment facilitator or an external specialist or in planning development activities.

An external service provider can be recommended equally for smaller and larger companies. The use of an external specialist is particularly recommended for organisations that are not familiar with maturity models or have limited resources for the development of cybersecurity. Small and medium-sized enterprises gain benefits especially through external experience. For larger companies, benefits may focus more on the organisation of the assessment process and schedules.

The organisation’s specialists. The assessment requires expertise in the organisation’s business operations, cybersecurity, and risk and HR management. The assessment facilitator, together with the sponsor, defines the participants required for the assessment, especially from the business point of view. The number of specialists varies, depending on the size of the organisation. In smaller companies, the assessment can be conducted by a few key individuals, while it may be necessary, in larger companies, to invite specialists from several different departments.

Table 1 lists key specialists for responding to different questions. The list highlights the roles of the chief information security officer (CISO) and information security manager. However, other individuals who have responsibilities related to cybersecurity and are relevant considering the area being assessed can be used in place of these roles.

Table 1. Key roles in different Cybermeter domains

Cybermeter domain	*Key roles*
CRITICAL *Protection of critical services*	Risk management manager, CISO and information security manager, and business representatives together
RISK *Risk management*	Risk management manager, CISO and information security manager
ASSET *Management of protected assets, changes, and configurations*	CISO and CIO together (*OT assets: responsible business representatives in addition to the aforementioned)
PROGRAM *Management of the cybersecurity management program*	CISO/information security manager or other person responsible for cybersecurity in the organisation
DEPENDENCIES *Supply chain and external dependencies management*	Procurement manager, risk management manager, CISO/information security manager and CIO together
ACCESS *Authorisation and access management*	CISO/information security manager and CIO together
RESPONSE *Event and incident response*	CISO/information security manager, CIO and risk management manager together, as well as relevant business representatives
ARCHITECTURE *Cybersecurity architecture*	CISO/information security manager together with relevant architects
SITUATION *Situational awareness*	CISO/information security manager and CIO together
THREAT *Threat and vulnerability management*	CISO and information security manager together, as well as relevant business representatives
WORKFORCE *Workforce management*	CISO together with the HR director

Owners of development plans are responsible for the development plans prepared on the basis of the results. Their task is to coordinate the preparation of the development plans, ensure that the resources required are assigned for the activities and monitor the fulfilment of the plans. A responsible person can be the same as the assessment sponsor or facilitator. Considering the development of cybersecurity, it is important that the role is visibly filled by a separately appointed individual and that the individual is obligated to report to the company's management. It is recommended that the role be appointed from inside the organisation.

4.2 Scoping the function

The assessment sponsor and facilitator define the operating area to be assessed in detail. **"Operating area" means the *functions* and the *systems*, *processes* and *data assets* which are critical for the provision of the functions that are examined in the assessment.** The definition of the functions and their dependencies is a critical stage considering the success of the assessment. A detailed definition and clear documentation enable the assessment to be conducted within the targeted time and ensure that the assessment results are comparable and later development activities can be allocated correctly.

Identifying critical functions

It is recommended that the assessment cover **the *functions* the organisation requires to provide services that are critical for its (business) operations or society at large.** The primary target group of Cybermeter consists of organisations that are critical for the functioning of society in terms of security of supply. However, the framework is equally suitable for organisations of all types. The assessment should then cover functions which are critical for the organisation's operations and key dependencies considering their reliability.

The assessment can be defined in many ways, for example:

- To cover **the whole organisation**, e.g. SMEs;
- In accordance with **the organisational structure**, e.g. a country or business unit;
- In accordance with **functions**, e.g. a service provided across organisational boundaries.

For example, organisations can assess a specific function or service, such as heat generation, water supply or payment services, as well as systems, processes, and data assets which are critical for these functions or services. Then again, the assessment can equally cover a specific part of an organisation, such as a business area, unit, or operating country. A geographic division is not recommended, except if it matches any of the descriptions above.

SMEs can direct the assessment at the organisation's operating area as a whole. Larger organisations can limit the assessment to cover a specific service, business unit or production facility. Even though Cybermeter is suitable for assessing and developing cybersecurity in entire organisations, it is recommended that the assessment focus on a single critical function or part of an organisation at a time, especially in larger organisations. Assessing operations as a whole requires that processes and practices are sufficiently harmonised throughout the operating area being assessed.

If the aim is to assess several operating areas at the same time, it is recommended that a separate assessment is launched for each area. It is therefore easier to allocate individual assessment results and development activities correctly, and the assessment process does not run out of control. Considering practices implemented throughout the organisation, the same responses can be used in different assessments.

Identifying critical dependencies

In addition to critical functions and services, key dependencies considering the reliability of these functions and services must be identified to define the area to be assessed. These primarily include all the following related to the provision of critical services:

- **Business processes and operational processes;**
- **Systems and subsystems;** and
- **Data resources.**

Identifiable dependencies include different systems and their subsystems and data resources. Dependencies also include processes related to these, as well as business processes and operational processes, including internal services and critical services provided by an external supply chain. The most significant dependencies should be prioritised and selected, and these selections should be documented as a distinctive part of the assessment.

Dependencies can be identified by proceeding from processes to related systems and data. Then again, it is possible to start from the data critical which for functions and services and proceed towards systems and processes. Figure 2 illustrates these dependencies.

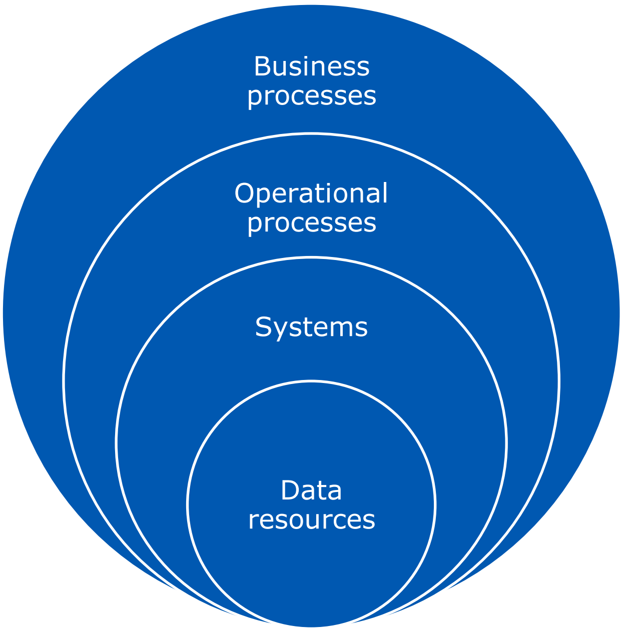


Figure 2. An example of an approach to identifying critical functions and their dependencies

An example of a process for identifying an operating area and its dependencies:

1. Identifying the organisation's critical functions or services;
2. If there are several functions or services, selecting the functions or services to be assessed;
3. Identifying and listing critical dependencies related to each critical function or service, including:
   a. Processes that guide critical functions and use systems to be protected. For example, it is possible to start by listing business-critical processes and defining their criticality.
   b. Systems that provide a function or service which is critical for society or the organisation. For example, it is possible to start by listing system assets and defining their criticality. Identifying internal and external dependencies related to systems.
   c. Data that is used in the provision of critical functions or services or in the operation of a critical system. For example, it is possible to start by listing the data assets to be protected.

A service which is critical for society at large. A service is critical for society at large if any disruption in the service would affect a significant number of customers or a large geographic area, or if it would have a severe consequential impact. The criticality can be defined on the basis of the National Emergency Supply Agency's sector-specific definitions.

A service which is critical for the (business) operations of an organisation. Identifying services which are critical for business operations should start from the organisation's goals or the focus areas of the organisation's business strategy.

4.3 Approaches to conducting an assessment

The assessment facilitator helps the organisation to select the most suitable assessment method. The assessment can be conducted as a guided workshop or a more independent personnel-driven assessment. The assessed domains can be divided between different evaluators. Depending on the assessment method, the facilitator takes care of practical workshop arrangements or otherwise coordinates the assessment with participating specialists.

In a guided workshop approach, the assessment facilitator organises the assessment by inviting specialists to one or more workshops.

Stages to be coordinated by the assessment facilitator (possibly together with the assessment sponsor and the organisation's specialists):

1. Appointing specialists and engaging them in the workshop
2. A kick-off meeting (one hour) or a message for participants in the assessment
3. One or more workshops (can also be conducted as a series of workshops in smaller groups, e.g. two to three hours per workshop)
4. Summarising and analysing results for the final workshop;
5. Reviewing the results, identifying any development areas and appointing individuals responsible for development during the final workshop (two hours).

The facilitator is responsible for the progress of the assessment, the coordination of tasks, sufficient documentation, and the organisation of workshops. One of the facilitator's key tasks is to ensure that the purpose and scope of the assessment are understood similarly in every discussion and assessed domain. During the process, the assessment facilitator obtains a comprehensive overview of the state of cybersecurity in the organisation.

In the groupwork-based approach, the purpose of the kick-off meeting is to communicate the purpose of the assessment and its implementation process to the participants. More information about the areas to be assessed can be provided at the beginning of a workshop or workshops. The kick-off meeting can also be replaced by a message sent to all members of the group.

In addition to holding a single longer workshop, the assessment can be conducted by holding a series of shorter thematic workshops for smaller groups consisting of the facilitator and two to four other individuals, including specialists in the specific area and the assessment sponsor. Discussions had during workshops help to build an understanding of cybersecurity and help to convey information to a larger group.

At the end of the process, the assessment facilitator will summarise the results and organise a final workshop for discussing the reports produced by the self-assessment tool. During the workshop, any flaws identified will be discussed and the responsibilities and schedules defined for development activities and plans will be agreed. The workshop agenda should include the analysis and reporting of the results and discussions of the target level.

An advantage of this approach is that the process results in a shared overview of the situation and an understanding of the current state and any target level. During the assessment, all Cybermeter domains must be discussed under proper guidance, while sharing ideas and knowledge. This prevents cybersecurity competence from being embodied in specific individuals only.

Challenges include the time required for workshops and especially finding a schedule that is suitable for everyone. However, an advantage of a series of workshops is that each workshop has a smaller number of participants and those who are genuinely connected to the domain being discussed. This working method may seem laborious for some roles if a specific individual is expected to participate in every workshop.

A personnel-driven assessment is an alternative Cybermeter assessment method. The assessment facilitator organises the assessment process together with the organisation’s individual specialists. A high-quality self-assessment requires that the individual appointed as the assessment facilitator has expertise in cybersecurity and the ability to study Cybermeter before the project starts.

Stages to be coordinated by the assessment facilitator:

1. Appointing specialists and engaging them in a workshop
2. A kick-off meeting (one to two hours) for participants in the assessment
3. The appointed specialists must independently complete their assigned Cybermeter domains following the agreed schedule
4. Summarising and analysing results for a workshop
5. Reviewing the results during a final workshop (two to four hours) to be participated in by all individuals who participated in the assessment

The purpose of the kick-off meeting is to familiarise the individuals responsible for different domains with Cybermeter, its use and the purpose of each domain. Next, the individuals will complete their respective domains independently or in small groups, depending on the domain. The assessment facilitator guides the independent process and provides assistance in interpretation, if required. Results are returned to the assessment facilitator who summarises them for the final workshop. The facilitator aims to identify the most significant conflicts and flaws in the responses and adds them to the workshop agenda.

During the final workshop, the results are discussed, and they may be modified to be more comparable with each other. Finally, the reports produced by Cybermeter are reviewed during the workshop. The target level can already be discussed when analysing the reports. During the workshop, it must be agreed how the results are reported forward and how the process will advance to the preparation of a development plan.

The advantages of this method include its effective and light structure, especially considering schedules, because only a brief kick-off meeting and a half-day final workshop must be arranged for the group. This method is particularly effective when the organisation can clearly identify responsible persons for different domains or their objectives.

The personification of responsibilities for cybersecurity and the production of a decentralised overview may be challenges in the independent assessment method. The final workshop will be laborious if different domains have been assessed on the basis of highly differing assumptions. The success of this method requires that the operating area being assessed has been defined and documented clearly and that it is communicated to all participants in the assessment.

4.4 Assessment results and reports

Cybermeter's automated reports support the analysis and use of the assessment results. The reports can be enriched with various reference and benchmarking data, and they can be used to define suitable target levels. The self-assessment tool produces three reports, each of which represents the organisation's level of maturity from slightly different perspectives or at different accuracy levels. These reports are:

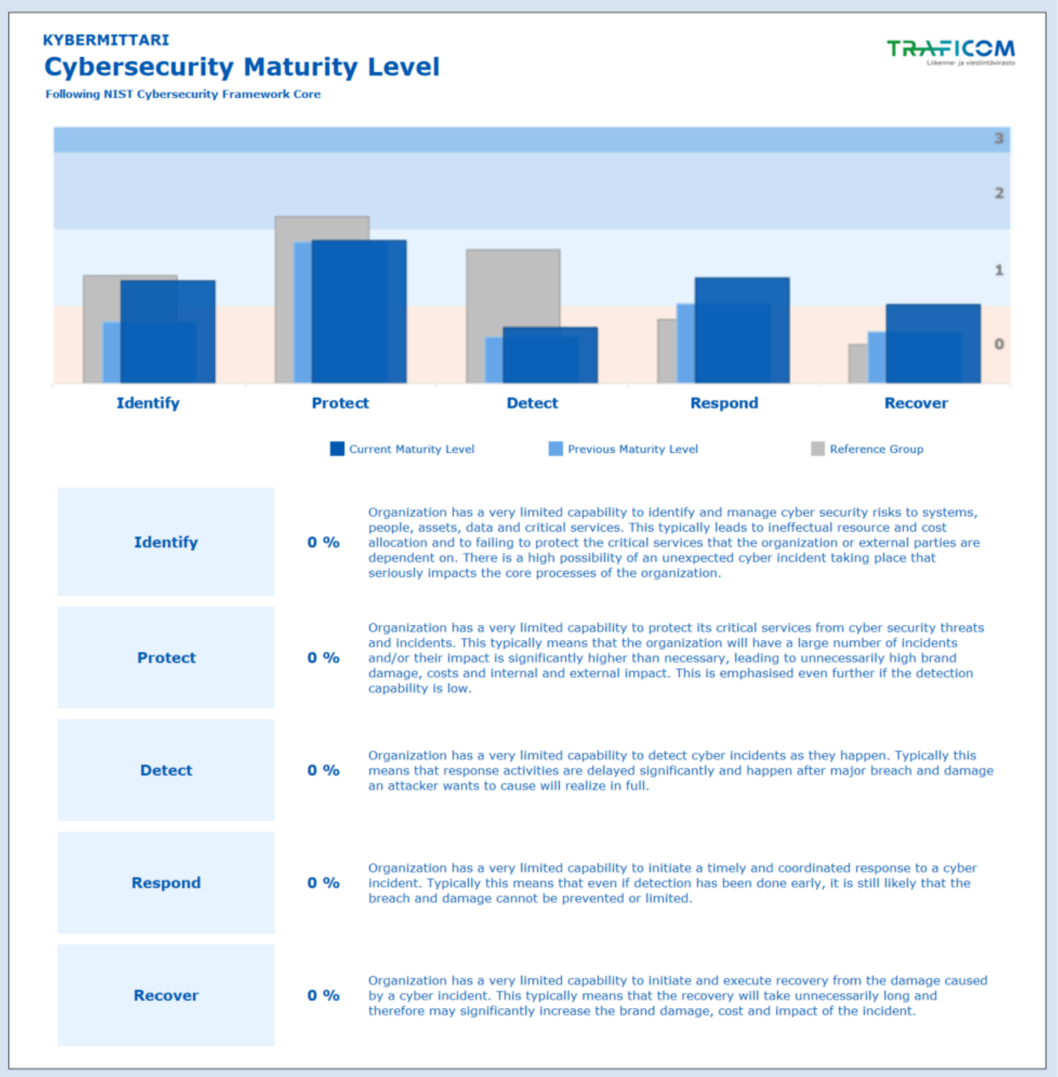
1. **The maturity report for the corporate management** is a general report intended for management reporting or use, for example in external communications;

2. **The Cybermeter maturity report** is a technical report intended for cybersecurity and risk management professionals and other technical responsible persons to identify the organisation's current state or define the target state and development activities;

3. **The detailed NIST Cybersecurity Framework Core report** is another technical report, which presents the Cybermeter assessment results in accordance with NIST CSF. The report is intended for organisations that have already used the NIST CSF framework or otherwise want to analyse or communicate their results using this framework.

Reports can be enriched with reference and benchmarking data, such as the organisation's previous assessment results or the sector's average maturity results. This feature can alternatively be used to visualise the organisation's target level, for example.

The maturity report for the corporate management is specifically intended for the reporting of assessment results to the organisation's management and for supporting internal and external communication.



KYBERMITTARI

Cybersecurity Maturity Level

Following NIST Cybersecurity Framework Core

Identify	0 %	Organization has a very limited capability to identify and manage cyber security risks to systems, people, assets, data and critical services. This typically leads to ineffectual resource and cost allocation and to failing to protect the critical services that the organization or external parties are dependent on. There is a high possibility of an unexpected cyber incident taking place that seriously impacts the core processes of the organization.
Protect	0 %	Organization has a very limited capability to protect its critical services from cyber security threats and incidents. This typically means that the organization will have a large number of incidents and/or their impact is significantly higher than necessary, leading to unnecessarily high brand damage, costs and internal and external impact. This is emphasised even further if the detection capability is low.
Detect	0 %	Organization has a very limited capability to detect cyber incidents as they happen. Typically this means that response activities are delayed significantly and happen after major breach and damage an attacker wants to cause will realize in full.
Respond	0 %	Organization has a very limited capability to initiate a timely and coordinated response to a cyber incident. Typically this means that even if detection has been done early, it is still likely that the breach and damage cannot be prevented or limited.
Recover	0 %	Organization has a very limited capability to initiate and execute recovery from the damage caused by a cyber incident. This typically means that the recovery will take unnecessarily long and therefore may significantly increase the brand damage, cost and impact of the incident.

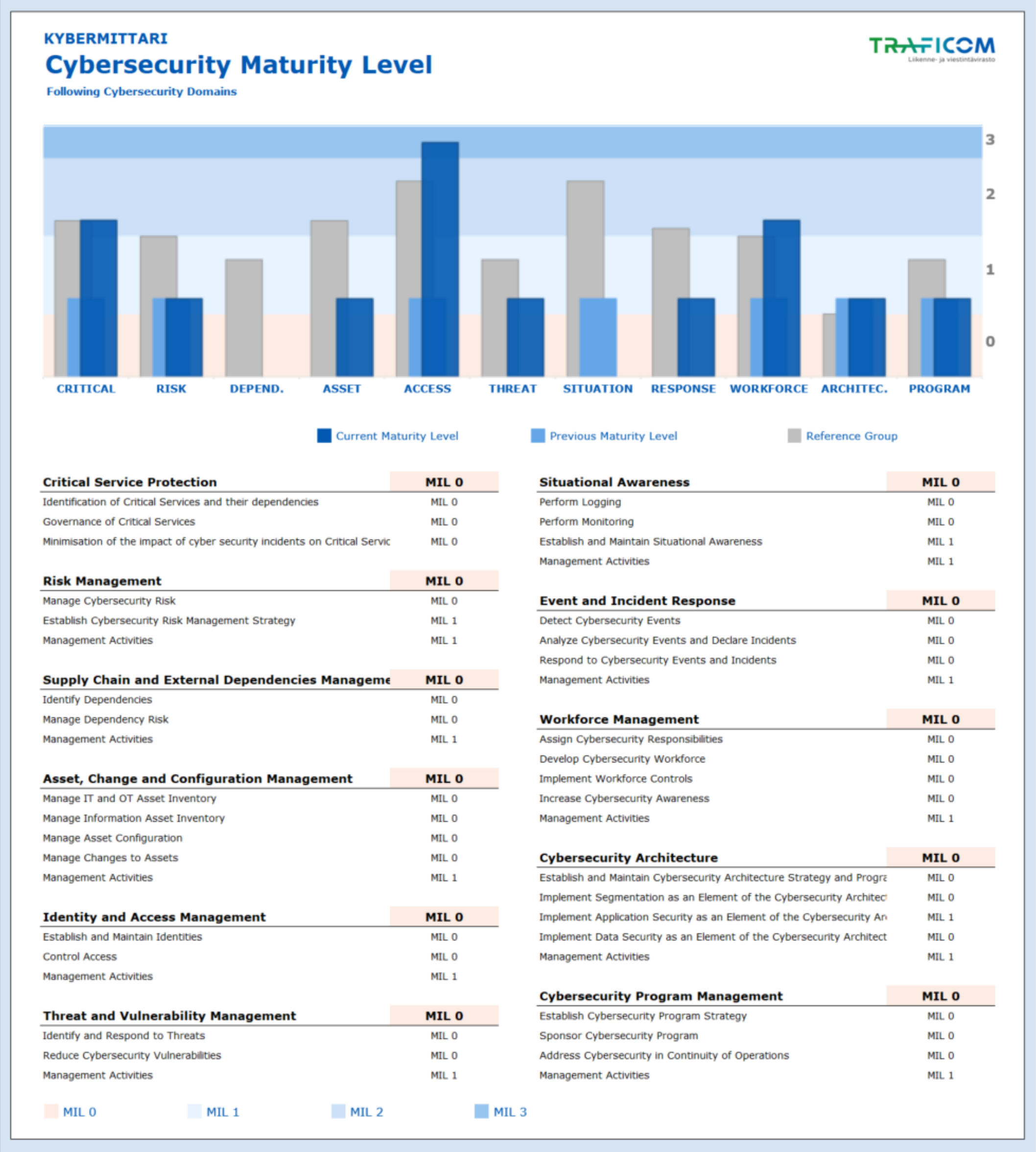
Figure 3. The Cybermeter maturity report is intended for the corporate management, based on five capabilities: identification, protection, detection, response, and recovery.

Results are presented in accordance with five capabilities of NIST CSF: identification, protection, detection, response, and recovery. The maturity indicator level of each capability is presented as a percentage, divided separately between L0-3. For each capability, the practical meaning of the results is described separately in writing.

Maturity model and cross-connections. The maturity indicator levels are defined on the basis of implemented Cybermeter practices. The practices have first been cross-connected to NIST CSF practices, where applicable. Next, the maturity indicator level of each of the five capabilities is calculated in accordance with implemented practices: level 0 means that less than 30% of the practices referring to the capability have been implemented (correspondingly level 1 -> less than 60%, level 2 -> less than 90%, and level 3 -> more than 90%).

It should be noted that NIST CSF is not a maturity model. As a result, cross-connections and maturity indicator levels are only indicative. Cross-connections between the practices of Cybermeter and NIST CSF are available in the Cybermeter self-assessment tool.

The Cybermeter maturity report is a more detailed report, which is intended for the analysis and reporting of the assessment results and for guiding internal development. The report is particularly intended for cybersecurity and risk management professionals and other technically responsible persons.



KYBERMITTARI

Cybersecurity Maturity Level

Following Cybersecurity Domains

Critical Service Protection	MIL 0
Identification of Critical Services and their dependencies	MIL 0
Governance of Critical Services	MIL 0
Minimisation of the impact of cyber security incidents on Critical Servic	MIL 0

Risk Management	MIL 0
Manage Cybersecurity Risk	MIL 0
Establish Cybersecurity Risk Management Strategy	MIL 1
Management Activities	MIL 1

Supply Chain and External Dependencies Manageme	MIL 0
Identify Dependencies	MIL 0
Manage Dependency Risk	MIL 0
Management Activities	MIL 1

Asset, Change and Configuration Management	MIL 0
Manage IT and OT Asset Inventory	MIL 0
Manage Information Asset Inventory	MIL 0
Manage Asset Configuration	MIL 0
Manage Changes to Assets	MIL 0
Management Activities	MIL 1

Identity and Access Management	MIL 0
Establish and Maintain Identities	MIL 0
Control Access	MIL 0
Management Activities	MIL 1

Threat and Vulnerability Management	MIL 0
Identify and Respond to Threats	MIL 0
Reduce Cybersecurity Vulnerabilities	MIL 0
Management Activities	MIL 1

Situational Awareness	MIL 0
Perform Logging	MIL 0
Perform Monitoring	MIL 0
Establish and Maintain Situational Awareness	MIL 1
Management Activities	MIL 1

Event and Incident Response	MIL 0
Detect Cybersecurity Events	MIL 0
Analyze Cybersecurity Events and Declare Incidents	MIL 0
Respond to Cybersecurity Events and Incidents	MIL 0
Management Activities	MIL 1

Workforce Management	MIL 0
Assign Cybersecurity Responsibilities	MIL 0
Develop Cybersecurity Workforce	MIL 0
Implement Workforce Controls	MIL 0
Increase Cybersecurity Awareness	MIL 0
Management Activities	MIL 1

Cybersecurity Architecture	MIL 0
Establish and Maintain Cybersecurity Architecture Strategy and Progra	MIL 0
Implement Segmentation as an Element of the Cybersecurity Architect	MIL 0
Implement Application Security as an Element of the Cybersecurity Ar	MIL 1
Implement Data Security as an Element of the Cybersecurity Architect	MIL 0
Management Activities	MIL 1

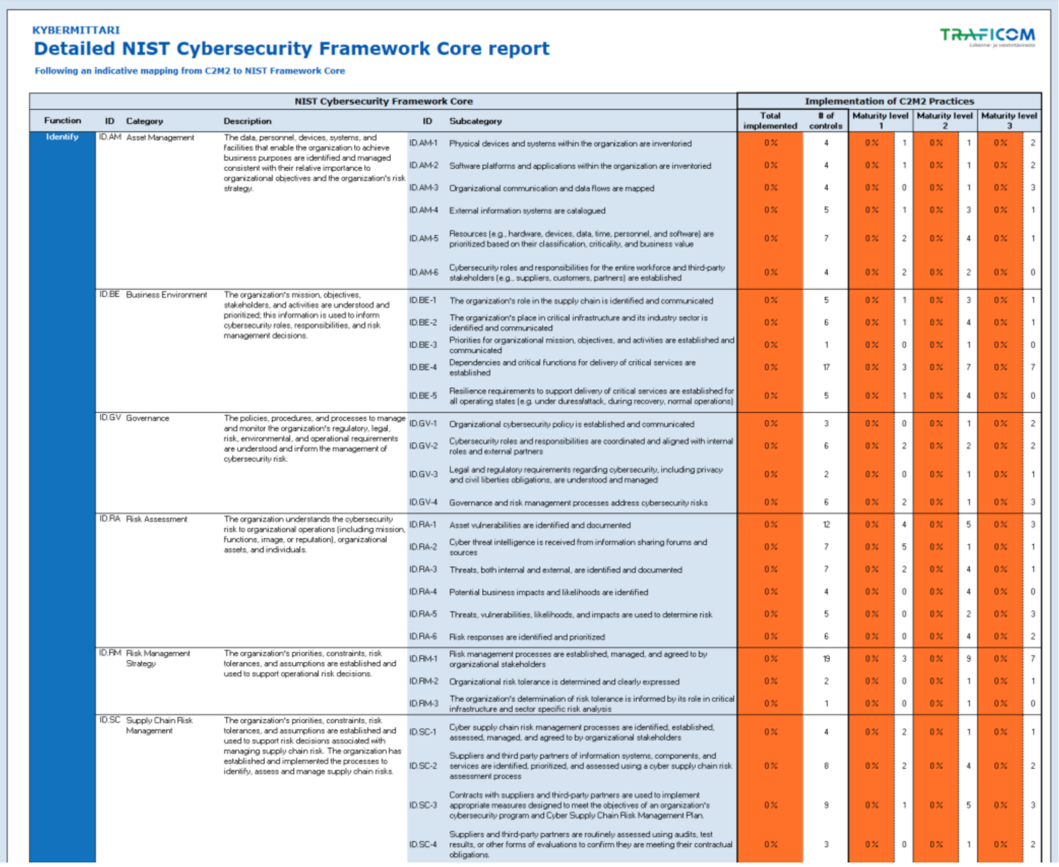
Cybersecurity Program Management	MIL 0
Establish Cybersecurity Program Strategy	MIL 0
Sponsor Cybersecurity Program	MIL 0
Address Cybersecurity in Continuity of Operations	MIL 0
Management Activities	MIL 1

Figure 4. The Cybermeter cybersecurity maturity report, based on 11 cybersecurity domains, presents concrete development areas.

The results are presented in accordance with Cybermeter's 11 cybersecurity capabilities. The maturity indicator level of each capability is presented at levels from 0 to 3. In addition to the domain-specific graph, the report presents the maturity indicator level of each objective.

Maturity model. The maturity indicator level calculation model complies with the Cybermeter calculation model presented in Section 3.3. Compared with C2M2 scoring, Cybermeter uses a lighter assessment process at maturity indicator levels 2 and 3. A level can be reached if at least 50% of the specific level's practices are implemented regarding each objective. This is also described in more detail in Section 3.3.

The detailed NIST Cybersecurity Framework Core report is a more detailed report, which is intended for the analysis and reporting of the assessment results and for guiding internal development. The report is particularly intended for cybersecurity and risk management professionals and other technically responsible persons, as well as organisations that have previous experience in NIST CSF.



KYBERMITTARI

Detailed NIST Cybersecurity Framework Core report

Following an indicative mapping from C2M2 to NIST Framework Core

NIST Cybersecurity Framework Core						Implementation of C2M2 Practices							
Function	ID	Category	Description	ID	Subcategory	Total implemented	# of controls	Maturity level 1		Maturity level 2		Maturity level 3	
Identify	ID.AM	Asset Management	The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	ID.AM-1	Physical devices and systems within the organization are inventoried	0 %	4	0 %	1	0 %	1	0 %	2
				ID.AM-2	Software platforms and applications within the organization are inventoried	0 %	4	0 %	1	0 %	1	0 %	2
				ID.AM-3	Organizational communication and data flows are mapped	0 %	4	0 %	0	0 %	1	0 %	3
				ID.AM-4	External information systems are catalogued	0 %	5	0 %	1	0 %	3	0 %	1
				ID.AM-5	Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	0 %	7	0 %	2	0 %	4	0 %	1
				ID.AM-6	Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	0 %	4	0 %	2	0 %	2	0 %	0
	ID.BE	Business Environment	The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	ID.BE-1	The organization's role in the supply chain is identified and communicated	0 %	5	0 %	1	0 %	3	0 %	1
				ID.BE-2	The organization's place in critical infrastructure and its industry sector is identified and communicated	0 %	6	0 %	1	0 %	4	0 %	1
				ID.BE-3	Priorities for organizational mission, objectives, and activities are established and communicated	0 %	1	0 %	0	0 %	1	0 %	0
				ID.BE-4	Dependencies and critical functions for delivery of critical services are established	0 %	17	0 %	3	0 %	7	0 %	7
				ID.BE-5	Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	0 %	5	0 %	1	0 %	4	0 %	0
	ID.GV	Governance	The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	ID.GV-1	Organizational cybersecurity policy is established and communicated	0 %	3	0 %	0	0 %	1	0 %	2
				ID.GV-2	Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners	0 %	6	0 %	2	0 %	2	0 %	2
				ID.GV-3	Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	0 %	2	0 %	0	0 %	1	0 %	1
				ID.GV-4	Governance and risk management processes address cybersecurity risks	0 %	6	0 %	2	0 %	1	0 %	3
	ID.RA	Risk Assessment	The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	ID.RA-1	Asset vulnerabilities are identified and documented	0 %	12	0 %	4	0 %	5	0 %	3
				ID.RA-2	Cyber threat intelligence is received from information sharing forums and sources	0 %	7	0 %	5	0 %	1	0 %	1
				ID.RA-3	Threats, both internal and external, are identified and documented	0 %	7	0 %	2	0 %	4	0 %	1
				ID.RA-4	Potential business impacts and likelihoods are identified	0 %	4	0 %	0	0 %	4	0 %	0
				ID.RA-5	Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	0 %	5	0 %	0	0 %	2	0 %	3
				ID.RA-6	Risk responses are identified and prioritized	0 %	6	0 %	0	0 %	4	0 %	2
	ID.RM	Risk Management Strategy	The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	ID.RM-1	Risk management processes are established, managed, and agreed to by organizational stakeholders	0 %	19	0 %	3	0 %	9	0 %	7
				ID.RM-2	Organizational risk tolerance is determined and clearly expressed	0 %	2	0 %	0	0 %	1	0 %	1
				ID.RM-3	The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	0 %	1	0 %	0	0 %	1	0 %	0
	ID.SC	Supply Chain Risk Management	The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.	ID.SC-1	Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders	0 %	4	0 %	2	0 %	1	0 %	1
				ID.SC-2	Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process	0 %	8	0 %	2	0 %	4	0 %	2
				ID.SC-3	Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.	0 %	9	0 %	1	0 %	5	0 %	3
				ID.SC-4	Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.	0 %	3	0 %	0	0 %	1	0 %	2

Figure 5. The detailed Cybermeter report presents results and development areas based on practices in accordance with NIST CSF.

Cross-connections. The percentages and figures presented in the report are based on implemented Cybermeter practices. The practices have first been cross-connected to NIST CSF practices, where applicable. The percentages are calculated by comparing the implemented practices of each domain with all practices applicable to the specific domain.

It should be noted that cross-connections are only indicative, as NIST CSF does not include a maturity model or cover all of the domains included in Cybermeter. Cross-connections between the practices of Cybermeter and NIST CSF are available in the Cybermeter self-assessment tool.

If a domain has zero practices or zero per cent, the domain cannot be found from Cybermeter.

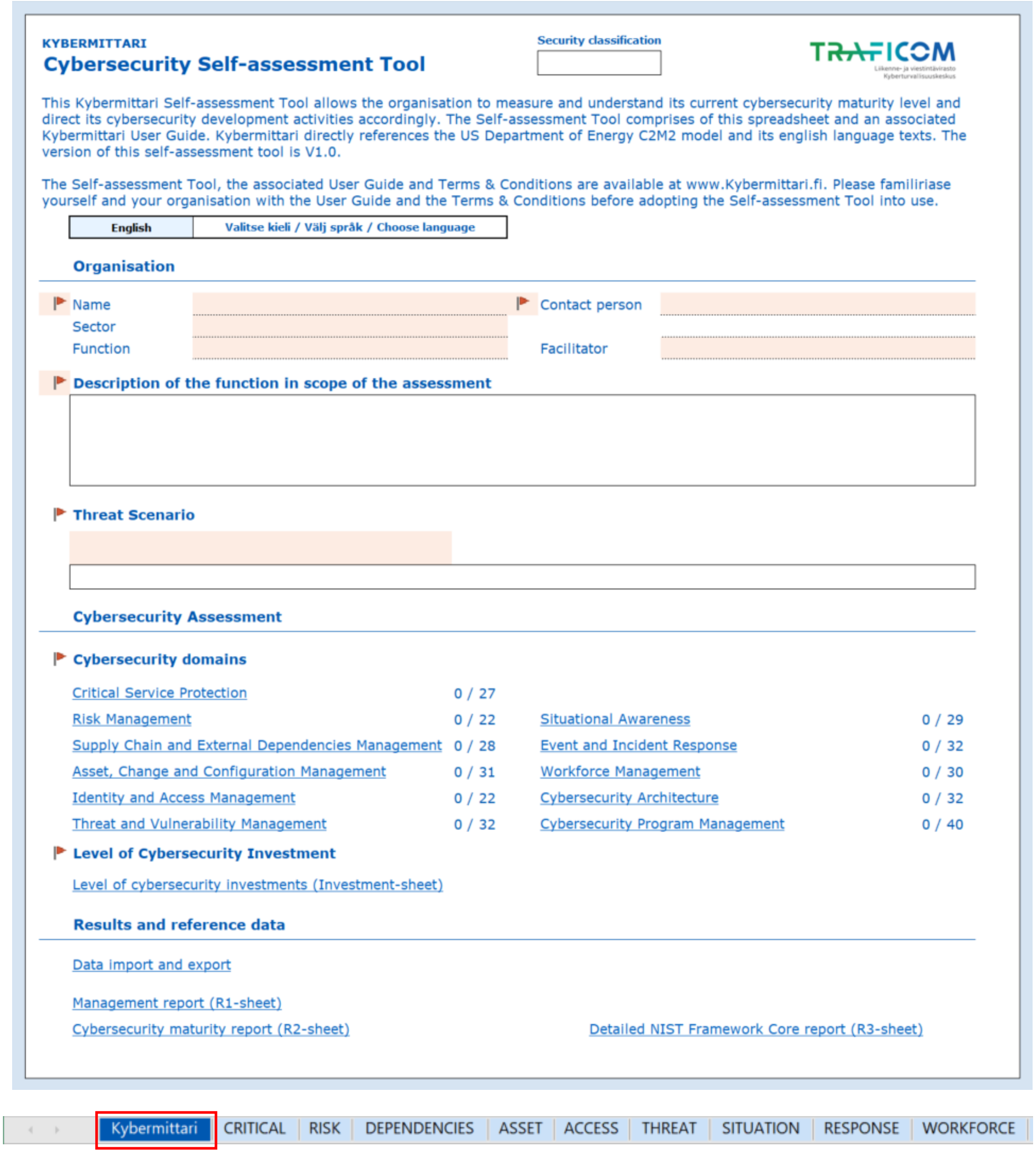
5 User Guide for the self-assessment tool

This section includes detailed instructions on how to use the Cybermeter self-assessment tool and input data. The tool supports and guides the assessment process. These instructions are particularly intended to support the assessment facilitator and other participants in using the tool effectively.

5.1 Cybermeter tab

The **Cybermeter** tab includes the following:

- Language selection in the tool (Finnish, Swedish or English);
- Classification of data as defined by the organisation;
- Organisation and operating area; and
- Cybersecurity assessment, results, and benchmarking data.



KYBERMITTARI
Cybersecurity Self-assessment Tool

Security classification

This Kybermittari Self-assessment Tool allows the organisation to measure and understand its current cybersecurity maturity level and direct its cybersecurity development activities accordingly. The Self-assessment Tool comprises of this spreadsheet and an associated Kybermittari User Guide. Kybermittari directly references the US Department of Energy C2M2 model and its english language texts. The version of this self-assessment tool is V1.0.

The Self-assessment Tool, the associated User Guide and Terms & Conditions are available at www.Kybermittari.fi. Please familiriase yourself and your organisation with the User Guide and the Terms & Conditions before adopting the Self-assessment Tool into use.

English | Valitse kieli / Välj språk / Choose language

Organisation

Name
Sector
Function
Contact person
Facilitator

Description of the function in scope of the assessment

Threat Scenario

Cybersecurity Assessment

Cybersecurity domains

Critical Service Protection	0 / 27		
Risk Management	0 / 22	Situational Awareness	0 / 29
Supply Chain and External Dependencies Management	0 / 28	Event and Incident Response	0 / 32
Asset, Change and Configuration Management	0 / 31	Workforce Management	0 / 30
Identity and Access Management	0 / 22	Cybersecurity Architecture	0 / 32
Threat and Vulnerability Management	0 / 32	Cybersecurity Program Management	0 / 40

Level of Cybersecurity Investment

Level of cybersecurity investments (Investment-sheet)

Results and reference data

Data import and export

Management report (R1-sheet)
Cybersecurity maturity report (R2-sheet)
Detailed NIST Framework Core report (R3-sheet)

Figure 6. The first tab in the Cybermeter self-assessment tool, including an overview of the assessed area and situation.

Finnish, Swedish or English can be selected as **the language used in the tool**. The tool's texts will change dynamically according to the selected language, apart from options in drop-down menus (e.g. translations of response options in the assessed domains).

The classification of data can be documented under **data classification**. Typically, data is classified by the organisation being assessed during or after the assessment. The data classification section can also be used by the authorities to classify documents transferred to them.

The organisation and operating area being assessed are documented under **organisation and operating area**. Here, the following information must be documented:

- The organisation's name, sector, and function;
- Contact person and assessment facilitator;
- A description of the operating area being assessed; and
- The social impact of the operating area.

The **cybersecurity assessment** and **results and benchmarking data** sections present a view of the assessment status and offer direct links to assessment domains and final reports.

Completion instructions: Enter the organisation's name, sector (e.g. logistics) and function (e.g. road transport) in this tab. The classification of sectors and functions is based on the sectors which are critical in terms of the security of supply and their sector pools defined by the National Emergency Supply Agency. The options are presented in Table 2.

If an organisation cannot find their sector from the list, the "ei-hvk toimiala" (not a critical sector) option must be selected in both menus. The classification supports the later compilation of statistics and benchmarking data, and it does not affect the assessment or its results.

Enter the organisation's contact person and the person and organisation acting as the assessment facilitator. This information will be needed later if any specifying questions or clarifications are required.

Enter a description of the operating area being assessed, including any critical dependencies, such as processes, systems, and data resources. Section 4.2 presents more detailed instructions for defining the operating area and critical dependencies. The description of the operating area will be documented for the analysis and benchmarking of results. This is particularly important so that it can later be identified which functions, systems, processes, and data assets the assessment covered.

Table 2. Definitions of sectors and operating areas which are critical in terms of the security of supply used in Cybermeter statistics

Critical sector	Critical operating area
Food supply	*Primary production* *Food industry* *Trade and distribution*
Energy	*Energy supply* *Oil*
Finances	*Financial management* *Insurance*
Critical industrial production	*Chemistry* *Forestry* *Military and defence* *Plastic and rubber* *Construction* *Technology*
Logistics	*Air transport* *Road transport* *Water transport*
Healthcare	*Healthcare* *Water supply*
Information society	*Digital services* *Media services*
Non-critical sector	*Activities other than those critical in terms of the security of supply*

Finally, estimate the social impact of the operating area in a situation where the function or service is unavailable. This applies to organisations that provide *services critical for society at large*. The social impact is described using three options and an open-ended description. The options are:

1. **Minor systemic impact:** The impact is only directed at the organisation itself or a small number of partners and/or customer organisations, or the impact is limited to fewer than 50,000 citizens.

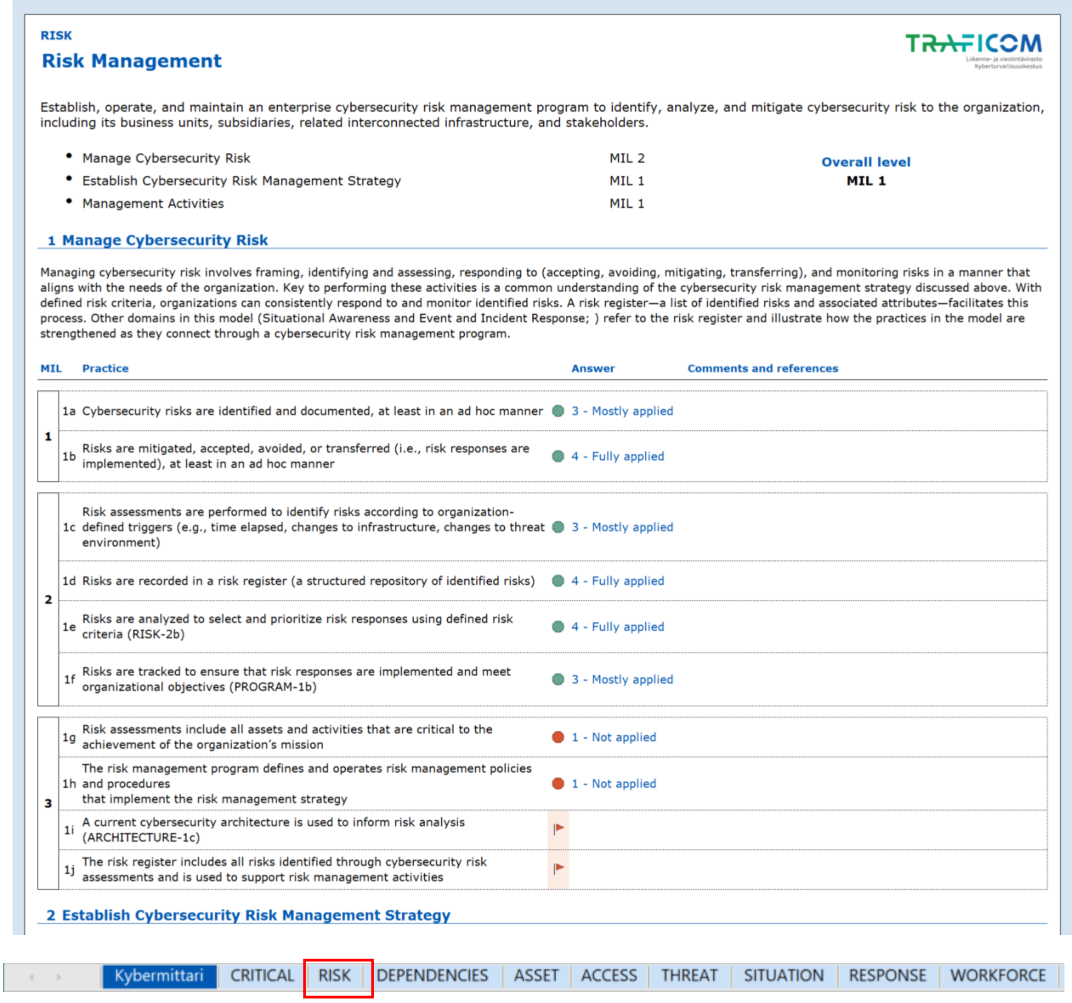
2. **Significant systemic impact:** An adverse impact on the activities of a significant number of partners and/or customer organisations, or harm or losses for more than 50,000 citizens.

3. **Crippling systemic impact:** Crippling basic functions of society, or losses for more than 100,000 citizens.

Once the organisation and operating area being assessed have been documented, the domain-specific tabs can be completed.

5.2 Domain-specific tabs

The 11 cybersecurity domains are each presented in a separate tab. The Cybermeter tab includes direct links to and an overview of each domain.



RISK

Risk Management

Establish, operate, and maintain an enterprise cybersecurity risk management program to identify, analyze, and mitigate cybersecurity risk to the organization, including its business units, subsidiaries, related interconnected infrastructure, and stakeholders.

		Overall level
• Manage Cybersecurity Risk	MIL 2	**MIL 1**
• Establish Cybersecurity Risk Management Strategy	MIL 1	
• Management Activities	MIL 1	

1 Manage Cybersecurity Risk

Managing cybersecurity risk involves framing, identifying and assessing, responding to (accepting, avoiding, mitigating, transferring), and monitoring risks in a manner that aligns with the needs of the organization. Key to performing these activities is a common understanding of the cybersecurity risk management strategy discussed above. With defined risk criteria, organizations can consistently respond to and monitor identified risks. A risk register—a list of identified risks and associated attributes—facilitates this process. Other domains in this model (Situational Awareness and Event and Incident Response;) refer to the risk register and illustrate how the practices in the model are strengthened as they connect through a cybersecurity risk management program.

MIL		Practice	Answer	Comments and references
1	1a	Cybersecurity risks are identified and documented, at least in an ad hoc manner	● 3 - Mostly applied	
	1b	Risks are mitigated, accepted, avoided, or transferred (i.e., risk responses are implemented), at least in an ad hoc manner	● 4 - Fully applied	
2	1c	Risk assessments are performed to identify risks according to organization-defined triggers (e.g., time elapsed, changes to infrastructure, changes to threat environment)	● 3 - Mostly applied	
	1d	Risks are recorded in a risk register (a structured repository of identified risks)	● 4 - Fully applied	
	1e	Risks are analyzed to select and prioritize risk responses using defined risk criteria (RISK-2b)	● 4 - Fully applied	
	1f	Risks are tracked to ensure that risk responses are implemented and meet organizational objectives (PROGRAM-1b)	● 3 - Mostly applied	
3	1g	Risk assessments include all assets and activities that are critical to the achievement of the organization's mission	● 1 - Not applied	
	1h	The risk management program defines and operates risk management policies and procedures that implement the risk management strategy	● 1 - Not applied	
	1i	A current cybersecurity architecture is used to inform risk analysis (ARCHITECTURE-1c)	⚑	
	1j	The risk register includes all risks identified through cybersecurity risk assessments and is used to support risk management activities	⚑	

2 Establish Cybersecurity Risk Management Strategy

Figure 7. An example of one of the Cybermeter self-assessment tool's 11 domain-specific tabs.

Each tab consists of the following sections:

- The name and presentation of the domain and a summary of the objectives set for the domain;
- The name and presentation of each objective and a description of the practices set for each objective; and
- The following information about each practice (from left to right):
  - Maturity indicator level, and the identifier and a description of each practice;
  - Response options 1–4 (multiple choice); and
  - Space for comments and references (free text field).

Completion instructions: assess by selecting the suitable response option for the practices presented. More information about the response options and their application is presented in Section 3.3. Comments are optional.

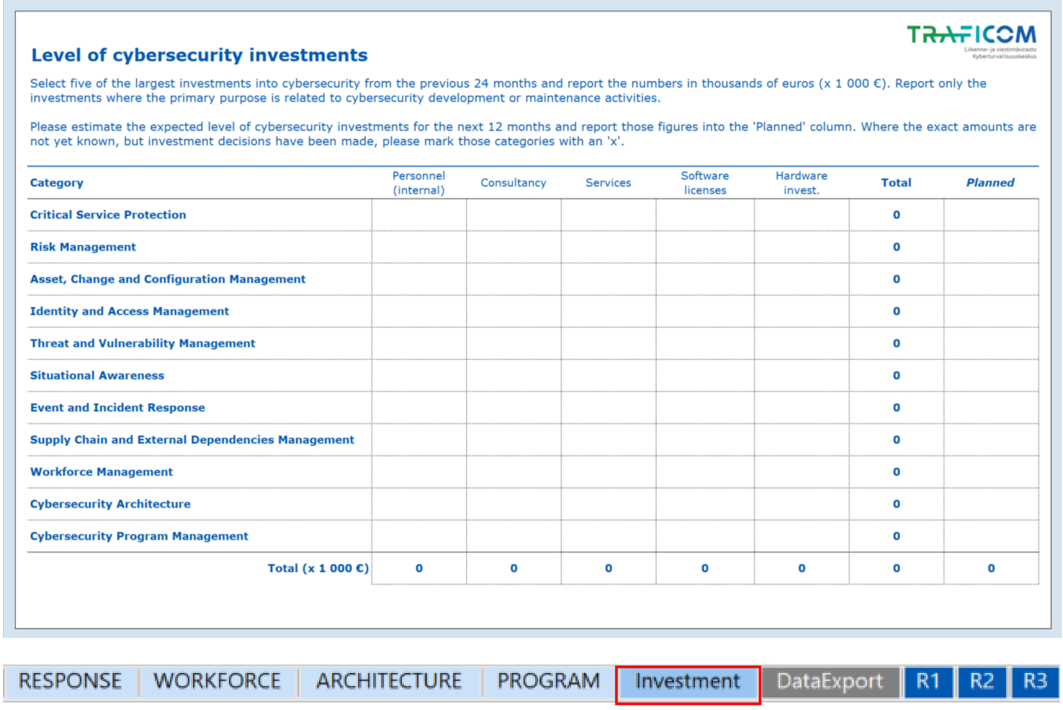
On the basis of the responses given, the tool automatically calculates the maturity indicator level for the objective, domain, and organisation along with the use of the tool.

While the domains can be assessed in any order, it is recommended that the assessment starts from the “Protection of critical services” domain. On this basis, later domains can be interpreted more easily.

Once all assessment domains have been completed, the level of investments can be assessed next and the assessment results produced by the self-assessment tool can be reviewed.

5.3 Investments tab

The level of cybersecurity investments is shown in a separate tab. The purpose of this tab is to assess the level of investments and costs associated with cybersecurity and categorise them in accordance with the assessed domains using Cybermeter. This enables the impact of investments to be analysed when the maturity indicator level of each domain is finally benchmarked with the investments made.



Level of cybersecurity investments

Select five of the largest investments into cybersecurity from the previous 24 months and report the numbers in thousands of euros (x 1 000 €). Report only the investments where the primary purpose is related to cybersecurity development or maintenance activities.

Please estimate the expected level of cybersecurity investments for the next 12 months and report those figures into the 'Planned' column. Where the exact amounts are not yet known, but investment decisions have been made, please mark those categories with an 'x'.

Category	Personnel (internal)	Consultancy	Services	Software licenses	Hardware invest.	**Total**	***Planned***
Critical Service Protection						**0**	
Risk Management						**0**	
Asset, Change and Configuration Management						**0**	
Identity and Access Management						**0**	
Threat and Vulnerability Management						**0**	
Situational Awareness						**0**	
Event and Incident Response						**0**	
Supply Chain and External Dependencies Management						**0**	
Workforce Management						**0**	
Cybersecurity Architecture						**0**	
Cybersecurity Program Management						**0**	
Total (x 1 000 €)	**0**	**0**	**0**	**0**	**0**	**0**	**0**

Figure 8. The cybersecurity investments tab in the Cybermeter self-assessment tool is used to collect information about the investments in each domain and their quality.

Completion instructions: Consider the following when completing the table.

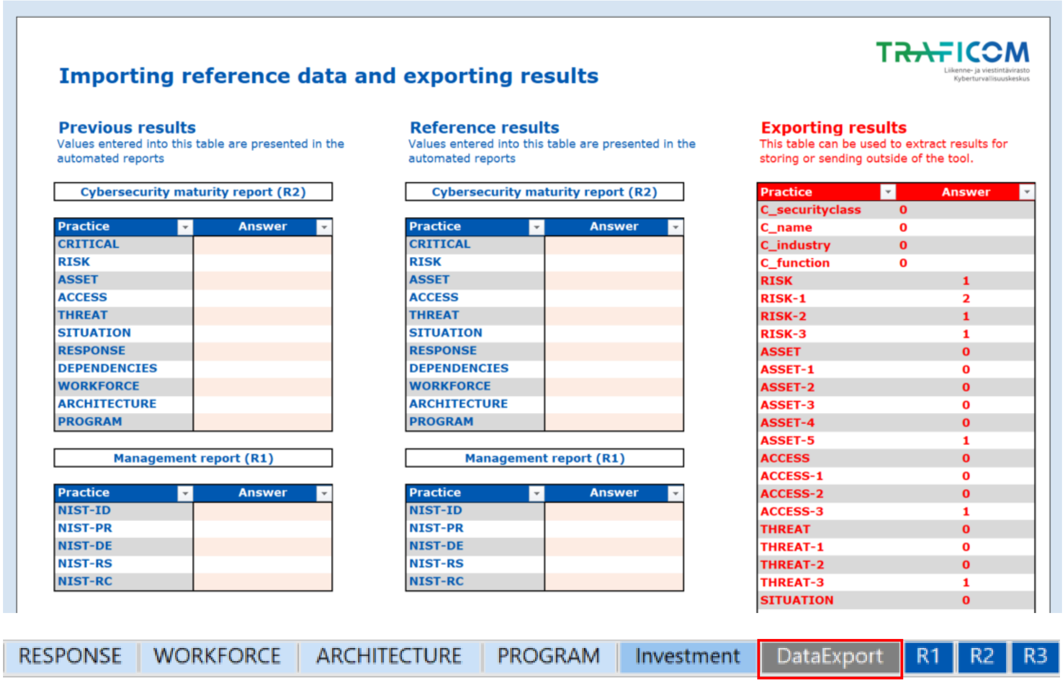
- The investment review period consists of the past 24 months;
- Sums must be entered in EUR thousand (× EUR 1,000);
- Only the investments and costs that are primarily connected to the development or maintenance of cybersecurity must be entered. Cybersecurity capabilities or functions associated with investments or costs based on other grounds must not be entered; and
- It is recommended that the assessment should focus on the five to ten largest cost items, for example.

The purpose of the "Planned" column in the table is to collect information about costs planned for the next 12 months. Only enter the costs that have already been approved or are so far in the process that their approval seems probable. However, if exact sums are not yet known, tick the category to which the costs belong. It is easier to complete the table if each domain has first been assessed to help understand the context for each row of the table.

5.4 Reports and benchmarking data

On the basis of the assessment, the Cybermeter self-assessment tool automatically produces three reports. The tool also supports the enrichment of reports with external benchmarking data and can export the assessment results in XML format.

Benchmarking data. The reports produced by the self-assessment tool can be enriched by adding benchmarking data to the tool in the DataExport tab. The data is imported automatically into the reports produced by the tool.



Importing reference data and exporting results

Previous results
Values entered into this table are presented in the automated reports

Cybersecurity maturity report (R2)

Practice	Answer
CRITICAL	
RISK	
ASSET	
ACCESS	
THREAT	
SITUATION	
RESPONSE	
DEPENDENCIES	
WORKFORCE	
ARCHITECTURE	
PROGRAM	

Management report (R1)

Practice	Answer
NIST-ID	
NIST-PR	
NIST-DE	
NIST-RS	
NIST-RC	

Reference results
Values entered into this table are presented in the automated reports

Cybersecurity maturity report (R2)

Practice	Answer
CRITICAL	
RISK	
ASSET	
ACCESS	
THREAT	
SITUATION	
RESPONSE	
DEPENDENCIES	
WORKFORCE	
ARCHITECTURE	
PROGRAM	

Management report (R1)

Practice	Answer
NIST-ID	
NIST-PR	
NIST-DE	
NIST-RS	
NIST-RC	

Exporting results
This table can be used to extract results for storing or sending outside of the tool.

Practice	Answer
C_securityclass	0
C_name	0
C_industry	0
C_function	0
RISK	1
RISK-1	2
RISK-2	1
RISK-3	1
ASSET	0
ASSET-1	0
ASSET-2	0
ASSET-3	0
ASSET-4	0
ASSET-5	1
ACCESS	0
ACCESS-1	0
ACCESS-2	0
ACCESS-3	1
THREAT	0
THREAT-1	0
THREAT-2	0
THREAT-3	1
SITUATION	0

Figure 9. Using the tables in the DataExport tab of the Cybermeter self-assessment tool, Cybermeter results can be exported/saved or automated reports can be enriched.

Completion instructions: Selected benchmarking values can be copied or entered in the marked fields. The values entered in the fields are displayed in automatically produced reports.

The DataExport tab includes two sections for reference results. These are titled “Previous results” and “Reference results”. However, organisations can use these sections as desired.

Exporting assessment results. The assessment results produced by the self-assessment tool can be converted into a different format for storage or sending, for example. Exported assessment results include:

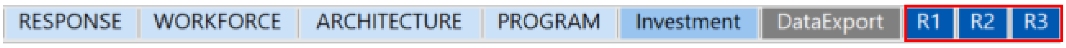
- The organisation’s basic information so that the results can later be allocated and interpreted correctly;
- Numerical results for each domain, objective, and practice, but <u>no comments or internal references</u>; and
- Numerical values regarding the levels of cybersecurity investments.

The organisation’s comments, references or personal data are not included in exported assessment results.

The DataExport tab includes a table of assessment results. The table is updated automatically on the basis of the responses given during the assessment.

<u>Instructions for use:</u> assessment results can be exported from the table by exporting them from the tool in XML format or by copying them and pasting them into another tool via the clipboard.

Note: If the values in the table are edited or overwritten, the assessment results may no longer be updated as intended.



Automated reports. On the basis of the responses given and any benchmarking data, the self-assessment tool generates three automatically updated reports:

- Cybermeter maturity report (R1 tab);
- Maturity report for the corporate management (R2 tab); and
- Detailed NIST CSF maturity report (R3 tab).

<u>Instructions for use:</u> Reported data is read from a hidden *Data* tab (regarding assessment results) and from the aforementioned sections in the *DataExport* tab (regarding benchmarking data). The reports are updated automatically on the basis of the responses and benchmarking data entered in domain-specific tabs.

6 Glossary

Key terms related to Cybermeter are presented in a separate glossary. As the purpose of this section is not to offer an exhaustive cybersecurity glossary, it may not necessarily include all terms that need to be understood to conduct Cybermeter assessments. This is why organisations are recommended to use official documents published by the Finnish Terminology Centre TSK: Vocabulary of Cyber Security (TSK 52) and Vocabulary of Comprehensive Security (TSK 50). These vocabularies are available in Finnish, Swedish and English on the TSK website under Publications.

Term	***Description***
C2M2 (Cybersecurity Capability Maturity Model)	A maturity model for cybersecurity capabilities maintained by the U.S. Department of Energy. The C2M2 helps organisations to observe, allocate, manage, and implement challenge related to cybersecurity practices. The C2M2 is one of the frames of reference behind Cybermeter.
Organisation critical in terms of the security of supply	An organisation which is particularly significant for securing functions that are vital for society. A critical organisation can be a company or other organisation. The primary goal of Cybermeter is to develop the contingencies for these critical organisations. Therefore, Cybermeter refers to these organisations and the critical functions and services they provide. It is important to note that Cybermeter is equally suitable for non-critical organisations. In this case, the references to critical functions or services used in Cybermeter must be interpreted to cover functions or services that are critical for the organisation's business operations.
IT system	An information technology system
Cybermeter	Cybermeter is a framework produced by the National Cyber Security Centre (NCSC-FI) of the Finnish Transport and Communications Agency (Traficom) and the National Emergency Supply Agency, which organisations can use to assess their maturity indicator levels of cybersecurity.
Cyber risk, cybersecurity risk	An area combining any negative impact of the cyber environment, cyber threats, and cybersecurity on an organisation's ability to operate. An example of a cyber risk is a chain of events in which a motivated perpetrator exploits a vulnerability in an organisation's operations to cause damage, resulting in losses and endangering the organisation's critical assets, such as data or a production process.
Cyber risk management, cybersecurity risk management	A proactive process to prepare for cybersecurity threats directed at an organisation's operations. In cybersecurity risk management, risks are identified, assessed, and processed, and they are reported and monitored regularly.

Cyber environment	An environment consisting of one or more digital data systems in which an organisation processes its data. An organisation's cyber environment consists of technical and technological selections, its sector's special features, and links to external stakeholders such as the authorities, contractual partners and customers.
Cybersecurity	A target state, in which the cyber environment can be trusted, and its operations can be secured. Cybersecurity differs from information security in that it is a broader concept, and its goal is also to control threats directed at physical security.
Cybersecurity architecture strategy	Goals, priorities, responsibilities, and monitoring processes defined for the cybersecurity architecture. This must be in line with the general cybersecurity strategy and corporate architecture.
Cybersecurity strategy	A cybersecurity strategy defines an organisation's cybersecurity goals and their priority, responsibilities, and monitoring. This can be a separate document, while it is often defined in the cybersecurity policy (information security policy) set by the organisation's management.
Cyber threat, cybersecurity threat	A possible harmful event or chain of events directed at the cyber environment and, if realised, endangers a dependent function. A cyber threat may present a cybersecurity risk to an organisation. An example of a cyber threat includes a remote connection, which an external attacker can use to access an organisation's data systems. Whether the remote connection presents a risk to the organisation depends on available information security controls and whether the connection can be used to endanger a function or data which is critical for the organisation's operations.
Practice (in Cybermeter)	In the context of Cybermeter, a practice means a set of claims grouped under the objectives of cybersecurity domains. In Cybermeter, organisations assess the implementation of practices in their operations using four levels, and the maturity of each domain and objective is determined on the basis of the results.
National Institute of Standards and Technology (NIST)	The NIST is an agency operating under the U.S. Department of Commerce, whose purpose is to develop and promote measuring methods, standards, and technologies. The NIST produces standards and best practices related to cybersecurity and privacy protection to support organisations' cybersecurity capabilities.
Inventory of assets	A list of a company's assets to be protected. The inventory of assets includes data about a company's protected data assets, hardware, and its configuration, such as the company's workstations,

	including programs, data, and data network structure, as well as IPR, licences, personal data, surveillance systems in facilities and floor plans of facilities.
Domain (in Cybermeter)	In the context of Cybermeter, cybersecurity domains are 11 areas, for which cybersecurity capabilities are assessed.
OT system	Operational technology (OT) generally means information and communication systems that are used to monitor and control industrial or physical devices, processes, or events. Traditionally, OT refers to industrial control systems, and its purpose is to separate the terms of OT and IT (information technology), which refers to conventional information and communication systems. In the context of Cybermeter, OT covers not only regular industrial control devices, but also other comparable devices that are either connected to the physical world or otherwise fulfil cybersecurity challenges that are typical to OT devices. Such devices include medical devices, financial payment systems and automated teller machines, lifting, transport and other automated devices in construction or logistics, or control devices for heating, ventilation or cost management in building automation systems. Considering cybersecurity, OT systems and devices often include various characteristic challenges. OT systems are increasingly connected to the Internet, while they are often excluded from the scope of IT controls, they cannot be updated, or they remain completely unidentified.
Resilience	An organisation’s ability to resist or tolerate crises, meaning the ability to maintain the ability to operate in changing conditions and the readiness to face disruptions and crises and recover from them.
Protected asset	An organisation’s physical or data asset that produces value for business operations. Examples include customer data, settings of production systems and production systems.
Objective (in Cybermeter)	In the context of Cybermeter, an objective is associated with a domain, in relation to which its capabilities are assessed.
Situational awareness	An organisation’s awareness of its state of cybersecurity maturity. Good situational awareness consists of the ability to collect, understand, and analyse data, and to react to threats in real time. An organisation’s understanding of which parts of cybersecurity are under control and where it has challenges and room for improvement is part of situational awareness.
Configuration baseline	A configuration baseline means settings that have been defined and documented so that the process can safely be recovered after disruptions.

Service critical for society at large	A service is critical for society at large if any disruption in the service affects a significant number of customers or a large geographic area, or it has a severe consequential impact.

7 Sources

[1] NIST Cybersecurity Framework Version 1.1, NIST, 04 2018 [Available at: https://doi.org/10.6028/NIST.CSWP.04162018]

[2] Cybersecurity Capability Maturity Model (C2M2) version 1.1, U.S. Department of Energy, 02 2014 [Available at: https://www.energy.gov/sites/prod/files/2014/03/f13/C2M2-v1-1_cor.pdf]

[3] Cybersecurity Capability Maturity Model (C2M2) version 2.0 (draft), U.S. Department of Energy, 06 2019 [Available at: https://www.energy.gov/sites/prod/files/2019/08/f65/ C2M2 v2.0 06202019 DOE for Comment.pdf] Link broken (13.4.2021). Ask document from Cybermeter team.

[4] National risk assessment 2018, Ministry of the Interior, 01 2019 [Available at: https://julkaisut.valtioneuvosto.fi/handle/10024/161351]

[5] Security Strategy for Society 2017, Security Committee, 11 2017 [Available at: https://turvallisuuskomitea.fi/wp-content/uploads/2018/02/YTS_2017_suomi.pdf]