CyberFundamentals Maturity Level description

The following describes the different CyberFundamentals Maturity levels on a holistic manner and is meant as a guidance during assessments. Although during assessments two approaches have to be considered, documentation and implementation, the following gives insight in how the maturity levels are understood as a whole.

The 5 CyberFundamentals Maturity Levels are:

- CyFun® Level 1 – Initial
- CyFun® Level 2 – Repeatable
- CyFun® Level 3 – Defined
- CyFun® Level 4 – Managed
- CyFun® Level 5 – Optimizing

What is important in the CyberFundamentals Framework is that each maturity level builds on the previous maturity level. Cybersecurity practices in a previous maturity level are therefore considered as established.

CyFun® Level 1 – Initial

Key elements: Process unpredictable, reactive, not documented & poorly controlled

Safeguards or countermeasures are not embedded in documented processes, which justifies the conclusion that cybersecurity controls (e.g. imposed via contract or sectoral requirements) are not implemented.

There is a lack or total absence of governance and cybersecurity-related interventions are mainly limited to "break/fix" work.

There is no evidence of due diligence to demonstrate compliance with applicable legal, regulatory and/or contractual obligations.

CyFun® Level 2 – Repeatable

Key elements: Ad Hoc Processes, mostly informal, project oriented & often reactive

Cybersecurity practices are "ad hoc" and when a control is met, it often lacks consistency and formality.

Cybersecurity practices tend to be project-oriented (driven by requirements set by a specific project) where the intent of the respective controls is met in most cases, but where the practice is not standardised across the organisation. Here, cybersecurity practices are mainly focused on specific systems, networks, applications or processes for which controls need to be implemented for a compliance need and often limited to a specific period in time. The latter could result in practices that are not reviewed and updated in the previous 2 years.

There is evidence of diligence to demonstrate compliance with specific legal, regulatory and/or contractual obligations, but limited to the projects where this is required.

Implementation is dependent on specific knowledge and effort of the person performing the task(s), where implementation of these practices may be a single point of failure and not proactively addressed.

It could be stated that due to their project orientation, CyFun® Level 2 cybersecurity practices focus on compliance rather than security and therefore have rarely been rolled out organisation-wide.

CyFun® Level 3 – Defined

Key elements: Formal processes, organisation oriented & proactive

Cybersecurity practices are standardised "organisation-wide" and implemented according to formally defined and approved processes. Controls are implemented according to documented and approved procedures.

Exceptions are documented, justified and approved. The number of exceptions from organisation-wide and standardised cybersecurity practices are limited to less than 5% of the total number of processes.

Assessment of the processes shows that less than 10% of the processes have a deviation from the anticipated outcome of those processes.

CyFun® Level 3 cybersecurity practices focus on security over compliance. Compliance can reasonably be seen as a "natural by-product" of cybersecurity practices.

There is adequate evidence of due diligence to demonstrate compliance with specific legal, regulatory and/or contractual obligations.

CyFun® Level 4 – Managed

Key elements: Formal processes, organisation oriented, controlled, proactive & measured

Cybersecurity practices build further on the CyFun® Level 3 maturity criteria and are "metrics-driven" to provide management insight into the cybersecurity status of the organisation.

Exceptions to organisation-wide implemented cybersecurity practices are limited to less than 3% of total processes, and are documented, justified and approved.

Detailed performance metrics are collected, analysed and reported. This leads to a quantitative understanding of process capabilities and an ability to predict performance.

Assessment of the processes shows that less than 5% of the processes have a deviation from the anticipated outcome of those processes.

Business stakeholders (top management, board of directors...) are aware of the cyber security status of the organisation (through e.g. regular management reviews), where situational awareness is supported by detailed metrics.

CyFun® Level 5 – Optimizing

Key elements: Formal processes, organisation oriented, controlled, proactive, measured & continual improvement focus

Cybersecurity practices build on established CyFun® Level 4 maturity criteria and are time-sensitive to support operational efficiency, which may include automated actions (e.g. through machine learning or artificial intelligence (AI)).

Exceptions to organisation-wide implemented cybersecurity practices are limited to less than 0.5% of total processes, and are documented, justified and approved.

Quantitative performance objectives (targets) for process effectiveness and efficiency are set, based on the organisation's business goals.

Assessment of the processes shows that less than 1% of the processes have a deviation from the anticipated outcome of those processes.

Process improvements are implemented according to "continuous improvement" practices to influence process change.

The above is based on interpretations contained in the Secure Controls Framework - Cybersecurity & Data Privacy Capability Maturity Model (C|P-CMM).

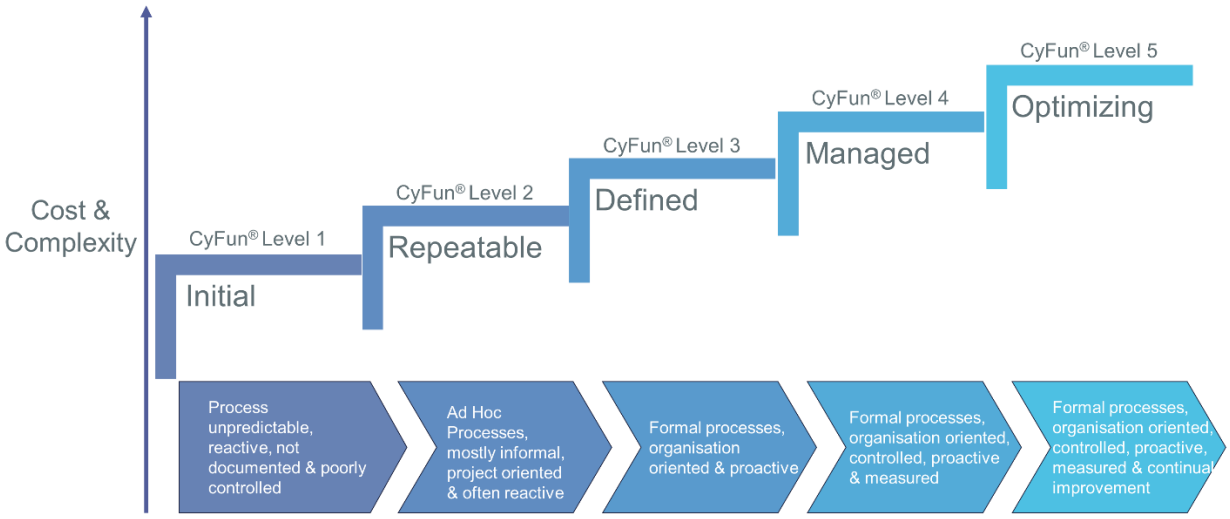

Figure: CyberFundamentals Maturity Level Overview