Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Protecting Small and Medium-sized Enterprises digital technology through an innovative cyber-SECurity framework

D2.3 Security Awareness Plan Report

Document Identification			
Status	Final	**Due Date**	30/11/2017
Version	1.0	**Submission Date**	15/12/2017

Related WP	WP2	**Document Reference**	D2.3
Related Deliverable(s)	-----	**Dissemination Level (*)**	PU
Lead Organisation	FHNW	**Lead Author**	Samuel Fricker
Contributors	FHNW, FORTH	**Reviewers**	George Oikonomou, CITRIX
			Francisco Hernandez, WOS

Keywords:
Awareness Goals, SME Challenges, Good Cybersecurity Practice, Awareness Roadmap, Validation Plan

This document is issued within the frame and for the purpose of the SMESEC project. This project has received funding from the European Union's Horizon2020 Framework Programme H2020-DS-SC7-2016 under Grant Agreement No. 740787 and supported by Swiss State Secretariat for Education, Research and Innovation (SERI) under contract number 17.00067. The opinions expressed and arguments employed herein do not necessarily reflect the official views of the European Commission.

Document Information

List of Contributors	
Name	Partner
Samuel Fricker, Alireza Shojaifar, Martin Gwerder	FHNW
Sotiris Ioannidis	FORTH

Document History			
Version	Date	Change editors	Changes
0.1	23/10/2017	Samuel Fricker FHNW	Initial draft
0.2	05/11/2017	Samuel Fricker FHNW	Complete draft
0.3	08/11/2017	Samuel Fricker FHNW	Finalised section 3
0.4	10/11/2017	Samuel Fricker FHNW	Finalised section 4
0.9	23/11/2017	Samuel Fricker FHNW	Accounted for review comments
0.99	28/11/2017	Samuel Fricker FHNW	Accounted for second review comments
1.0	15/12/2017	ATOS	Quality review and final version to be submitted.

Table of Contents

List of Tables

List of Figures

List of Acronyms

Abbreviation / acronym	Description
ACL	Network Access Control List
APT	Advanced Package Tool (Linux)
BSI	British Standards Institution
BYOD	Bring Your Own Device
CIRT	Cyber Incident Response Team
CSRF	Cross-site Request Forgery
CYSFAM	Cyber Security Focus Area Maturity Model
Dx.y	Deliverable number y belonging to WP x
EC	European Commission
FAQ	Frequently Asked Question(s)
HIPAA	American Health Insurance Portability and Accountability Act
ISFAM	Information Security Focus Area Maturity Model
ISMS	Information Security Management System
ISO	International Organisation for Standardisation
Mx	Month x
NERC CIP	North American Electric Reliability Corporation: Critical Infrastructure Protection
OSSEC	Open Source Host-based Intrusion Detection System
OWASP	Open Web Application Security Project
PCI DSS	American Payment Card Industry: Data Security Standard
PDCA	Plan-Do-Check-Act
SIEM	Security Information and Event Management
SME	Small and Medium Enterprises
WP	Work Package
XSS	Cross-site Scripting
YUM	Yellowdog Updater Modified (Linux flavor)

Executive Summary

Cybersecurity has become a problem for many small and medium-sized companies (SMEs). Awareness of the cybersecurity problem, knowledge of good practices, and the institutionalisation of tailored, effective capabilities in the SME are aims of SMESEC cybersecurity awareness plan.

In the context of cybersecurity for SME, a "security awareness plan" can have multiple interpretations, both for the entity developing the awareness and the scope of the plan. This document discusses primarily the process of an SME to develop awareness about cyber threats and building cybersecurity capabilities to address these threats. The document also addresses the second interpretation, the plan of the SMESEC project to raise awareness about cyber threats in the industry and in releasing, validating, evolving, and exploiting the SMESEC framework for increasing cybersecurity of European SME.

This document provides background about cybersecurity for SME, describes frameworks for improving cybersecurity capability, and standards that companies should adhere to. The document also describes experiences in assessing themselves and improving cybersecurity capability. These experiences were then used to propose the SMESEC approach for offering awareness and capabilities to the SME incrementally and adaptively. The document concludes with an overview of the SMESEC open call for implementing and evaluating the approach in an expanded set of SMEs.

Key takeaway messages:

- OWASP, ISO 27K, and CYSAM/ISFAM give a good overview of general awareness goals.
- Awareness and capability improvement in SMEs must address several hurdles.
- SMESEC proposes an incremental, adaptive approach to cybersecurity awareness and capability-improvement in an SME.
- The validation will be based on the four SMESEC use case SMEs and the Open Call.

The results of this document will be used as an input for WP3 in support of the SMESEC security framework development. In particular, D2.3 is input to the SMESEC security awareness and training reports D3.5 and D3.6. The CYSEC approach will be developed by FHNW and integrate UOP and ATOS training modules. The document will also be used as a basis for piloting, for evaluating the adoption of tailored versions of the SMESEC cybersecurity framework with SMEs as outlined in WP4. The document will also be used as a basis for the open call, which is used to assess the SMESEC cybersecurity framework with the open call.

1 Introduction

Cybersecurity has become a problem for many small and medium-sized companies (SMEs). Despite a continued rise in cyber threats and digital connectivity that allows threats to propagate, SMEs continue to protect themselves insufficiently. For that reason, SMESEC aims at improving the awareness of the cybersecurity problem, knowledge of good practices, and the institutionalisation of tailored, effective capabilities in SMEs. This aim applies to the whole company as well as to the individual employees who are the users of cybersecurity.

In the context of cybersecurity for SME, a "security awareness plan" can have multiple interpretations, both for the entity developing the awareness and the scope of the plan. Security awareness may be the awareness of the SME about cyber threats matched with capabilities for addressing these threats. Security awareness may also be the awareness of the SME's employees about cybersecurity threats and have the employees should behave to avoid or mitigate problems. The plan may be enacted from the perspective of the entity benefitting from cybersecurity. For example, the plan may be a step-wise process of discovering cyber threats and building the capabilities of addressing the threats. The plan may also be enacted from the perspective of SMESEC project. The plan may involve dissemination actions raising awareness in the targeted industries and the release, validation, evolution, and exploitation of the SMESEC framework that helps European SME to build cybersecurity capabilities.

1.1 Purpose of the document

This document provides background about the goals of cybersecurity for SME, describes frameworks that have been proposed for assessing and improving cybersecurity capability, and standards that companies should adhere to. The document also describes the SMESEC use case partners' experiences in assessing themselves and improving cybersecurity capability according to the best-fitting capability improvement framework. These experiences were then used to design the SMESEC approach for offering awareness and capabilities to the SME incrementally and adaptively. The document concludes with an overview of the SMESEC open call for implementing and evaluating the approach in an expanded set of SMEs.

The document starts by describing the awareness goals that are of relevance for the SMESEC use case SMEs. It describes the cybersecurity awareness goals by giving a summary of the OWASP Top-10 risk for web applications, mobile applications, and the internet of things, and the ISO 27K and BSI 100-X standards. It describes the existing capability improvement frameworks CYSFAM and ISFAM, which represent the starting point for describing the SMESEC awareness roadmap.

To understand the hurdles for adopting good cybersecurity practice, the document reviews relevant literature and let the four SMESEC use case SMEs experience the cybersecurity capability improvement framework CYSFAM, which fits well the themes the use case SMEs are concerned of. The results show the explanations and factors that need to be considered when planning for awareness campaigns and sustainable capability improvements.

Based on the learned, this document proposes the SMESEC awareness and capability improvement approach. It describes the architecture of the awareness and capability improvement roadmap, the

SMESEC offering of training, templates, and tools, the SMESEC approach to monitoring of adherence to recommendations, and the collection and delivery of cybersecurity user feedback. The validation of the approach will be performed according to the outlined SMESEC open call.

1.2 Relation to other project work

The results of this document will be used as follows:

- The document is an input for WP3 in support of the SMESEC security framework development. In particular, D2.3 is input to the SMESEC security awareness and training reports D3.5 and D3.6.
- The CYSEC approach will be developed by FHNW and integrate UOP and ATOS training modules.
- The document will also be used as a basis for piloting, for evaluating the adoption of tailored versions of the SMESEC cybersecurity framework with SMEs as outlined in WP4.
- The document will also be used as a basis for the open call, which is used to assess the SMESEC cybersecurity framework with the open call.

1.3 Structure of the document

The remainder document is structured as follows.

Section 2 describes the background, including cybersecurity goals, cybersecurity standards, and capability improvement frameworks.

Section 3 describes the SME's challenges in adopting and implementing good cybersecurity practices.

Section 4 describes the SMESEC approach.

Section 5 describes the planned validation of the SMESEC approach with the open call.

Section 6 summarises and concludes.

2 Awareness Goals and Existing Approaches

2.1 Cybersecurity Needs of SME Offering Digital Products

Any investment of an SME in cybersecurity capabilities needs to have a clear return on investment. For that reason, T2.4 orients knowledge and capability improvements toward the industry's top security risks and the SME needs as perceived by the SMESEC use cases. This section gives an overview.

2.1.1 Top-10 Challenges

The OWASP project[1] investigates and publishes a set of the most important cybersecurity risks every few years. The OWASP publications are significant because they result from cooperative efforts across the industry. The most recent relevant reports are the 2013 Top-10 report on web application security risks [OWASP 2013], the 2014 Top-10 report on the Internet of Things [OWASP 2014], and the 2016 Top-10 report on Mobile technology [OWASP 2016].

The following table gives an overview of the various security risks proposed by OWASP.

Table 1: OWASP Risks

Risk	Description: an attacker…
Domain: Web Applications	
1. Injection	Uses untrusted data to trick an interpreter into executing unintended commands or accessing data without proper authorisation.
2. Broken Authentication and Session Management	Uses incorrectly implemented authentication or session management functions to compromise passwords, keys, or tokens or exploits other implementation flaws to assume users' identities.
3. Cross-Site Scripting (XSS)	Uses untrusted data in a web browser without proper validation or escaping to execute scripts in a victim's browser and hijack user sessions, deface websites, or redirect the user to malicious sites.
4. Insecure Direct Object References	Manipulates an exposed reference to an internal implementation object, file, directory, or database to access unauthorised data without access control.
5. Security Misconfiguration	Uses misconfigured or default security configurations or depreciated software to abuse application frameworks, applications servers, web servers, database servers, or platforms.
6. Sensitive Data Exposure	Uses weakly protected data to conduct credit card fraud, identity theft, or other crimes.
7. Missing Function Level Access Control	Accesses functions on the server without access control to access functionality without proper authorisation.
8. Cross-Site Request Forgery (CSRF)	Forces a logged-on victim's browser to send an apparently legitimate but forged HTTP request, including the victim's session cookie and any other automatically included authentication information, to a vulnerable web application.
9. Using Known Vulnerable Components	Uses application components with known vulnerabilities and full privileges to undermine application defences to facilitate data theft or server takeover.

[1] www.owasp.org

10. Unvalidated Redirects and Forwards	Uses redirects with untrusted data to determine the destination pages to redirect victims to phishing or malware sites or to access unauthorised pages.
Domain: Mobile Applications	
1. Improper Platform Usage	Misuses a platform feature or failure to use platform security controls of the mobile operating system like Android intents, permissions, TouchID, or the Keychain.
2. Insecure Data Storage	Misuses insecure data storage and unintended data leakage.
3. Insecure Communication	Misuses poor handshaking, incorrect SSL versions, weak negotiation, and cleartext communication of sensitive assets.
4. Insecure Authentication	Misuses bad end user authentication or session management, including failing to identify the user at all and maintain the user's identity.
5. Insufficient Cryptography	Misuses incorrectly applied cryptography to access a sensitive information asset.
6. Insecure Authorisation	Misuses failures in authorisation such as wrong authorisation decisions on the client side or forced browsing.
7. Client Code Quality	Misuses code-level implementation problems in the mobile client such as buffer overflows, format string vulnerabilities, and other mistakes where the solution is to rewrite code running on the mobile device.
8. Code Tampering	Does binary patching, local resource modification, method hooking, method swizzling, and dynamic memory modification to replace the APIs the application uses or modify the application's data and resources.
9. Reverse Engineering	Analyses the final core binary to determine its source code, libraries, algorithms, and other assets to obtain insight into the inner workings of the application to exploit nascent vulnerabilities, obtain information about back-end servers, cryptographic constants and ciphers, and intellectual property.
10. Extraneous Functionality	Misuse hidden backdoors or unintended development security features included by developers to disable security controls.
Domain: Internet of Things	
1. Insecure Web Interface	Uses weak or captured plain-text credentials to access the web interface to retrieve or corrupt data, execute functions without accountability, or take over a complete device.
2. Insufficient Authentication or Authorisation	Uses weak passwords or insecure password recovery mechanisms to retrieve or corrupt data, execute functions without accountability, or take over a complete device.
3. Insecure Network Services	Uses vulnerable network services to attack the device or bound attacks off the device to access or corrupt data or execute denial of service attacks.
4. Lack of Transport Encryption	Uses the lack of transport encryption to views data being passed over the network to access or steal data and possibly compromise devices or user accounts completely.
5. Privacy Concerns	Uses insufficient authentication, lack of transport encryption, or insecure network services to view insufficiently protected or unnecessarily collected personal data to compromise a user.
6. Insecure Cloud Interface	Uses insufficient authentication, lack of transport encryption, and account enumeration to access data or controls via the cloud website to compromise user data and control devices.
7. Insecure Mobile Interface	Uses insufficient authentication, lack of transport encryption, and account enumeration to access data or controls to compromise user data and control devices.
8. Insufficient Security Configurability	Uses the lack of granular permissions, encryption, or passwords to access data or control devices.
9. Insecure Software Firmware	Captures update files or hijacks the DNS to replace software or firmware to compromise user data, control devices, and attack other devices.

10. Poor Physical Security	Uses USB ports, SD cards, or other storage means to access the operating system and potentially any data stored on the device to compromise the device and data stored on that device.

The Top-10 reports enable research and industry to set priorities in addressing the cybersecurity problem. Many standards, books, tools, and other EU projects refer to the OWASP report. For example, the H2020 Armour project proposes countermeasures to counter the OWASP Top-10 Internet of Things threats [ARMOUR 2016].

For establishing a cybersecurity framework like the SMESEC framework, the challenge is that the prioritised cybersecurity risks change over time. For example, a revision of the OWASP 2013 report is under industry consultancy. An updated version is expected to be released in 2018.

Also, the cybersecurity risk listings have been developed from a technology angle, while ignoring the social and commercial aspects of humans interacting with systems that need protection. Thus, for SMESEC, there remains a so far unfulfilled need of understanding the prioritised cybersecurity needs from the perspective of the small and medium enterprise. This document addresses this need by reporting them from the perspective of the four SMESEC use cases.

2.2 Cybersecurity Standards

By the SMESEC use case partners, ISO 27'00x has been indicated to be relevant. Compliance to ISO 27'00x is a requirement for customers of one of the SMESEC use case SMEs. The following sub-sections give an overview on ISO 27'00x and the BSI-Standards BSI100-x that offer an accessible approach to understanding ISO 27'001.

2.2.1 ISO 27'00x

The IEC/ISO 27K series is one of the most common standards worldwide regarding management of IT security. It is divided into several subdocuments whereas the document ISO/IEC 27001 is regarded as the main document and is normative.

It is complemented by the following generally applicable documents (among others):

- ISO/IEC 27002: Code of practice for cybersecurity management
- ISO/IEC 27003: ISMS implementation guidance
- ISO/IEC 27004: Cybersecurity management – Measurement
- ISO/IEC 27005: Cybersecurity risk management

And some specialised guidelines such as

- ISO/IEC 27011: Information technology – Security techniques – Cybersecurity management guidelines for telecommunications organisations based on ISO/IEC27002
- ISO 27799: Health informatics – Cybersecurity management in health using ISO/IEC27002

2.2.2 BSI 100-X

The BSI standards namely the standards [bsi100-1], [bsi100-2], and [bsi100-3] cover a subset of ISO/IEC27001 standard and tries to be more readable and easier for their respective reader. The BSI standard 100-1 defines the general requirements for an information security management system for

implementing the ISO 27001 standard. The BSI standard 100-2 describes how information security management may be set up and operated in practice. The step-by-step guidance helps to interpret the general requirements of ISO 2700x. The BSI standard 100-3 contains standard security safeguards required to protect a company's information domains. Regarding suitability and applicability, these documents are easier to handle for an SME that the original ISO 2700x standard.

2.3 Cybersecurity Capability Improvement Frameworks

The University of Utrecht has developed a portfolio of maturity models that allow companies to incrementally improve their awareness, understanding, and ability of cybersecurity. The CYSFAM maturity model addresses the cybersecurity needs of companies offering digital products and services. The ISFAM maturity model addresses the cybersecurity needs of small and medium enterprises that utilise ICT for their operations.

The models aid the improvement of an organisation's cybersecurity practices by letting managers and employees determine the organisation's maturity level and identify the areas that need improvement to reach a higher maturity level. The model allows the setting of priorities for assessment and improvement, thus allowing the user organisations to tailor their efforts to business needs and circumstances.

Maturity models define the objectives of cybersecurity capabilities. The maturity models state what a company might want to do but not how a company does it. A company can use a maturity model for obtaining awareness of what should be done, assessment of its capability profile, planning capability improvements, and tracking capability improvement progress. Training and tool providers can use a maturity model to position the training or tool, hence enabling a company to learn and build cybersecurity capabilities.

In the context of cybersecurity, two maturity models have been proposed: the CYSFAM and ISFAM models. The following sub-sections give an overview.

2.3.1 CYSFAM Maturity Model

The CYSFAM maturity model "Cybersecurity Focus Area Maturity Model" is intended to be applied by organisations that offer digital products and services. The model has been developed in collaboration with banks but could be applied by any other type of organisation that is responsible for digital products and services that could be attacked[2].

In the centre of CYSFAM is a maturity matrix that describes capabilities for a set of focus areas. The focus areas reflect the organisational and technical concerns of the organisation. The capabilities describe practices that the organisation employs to protect its digital products and services. The capabilities are ordered according to the maturity they represent for the organisation. Figure 1 gives an overview of the structure of the CYSFAM model.

[2] CYSFAM has been developed in a MSc thesis at the University of Utrecht. No publication is available at this moment for citation. Publication work is ongoing.

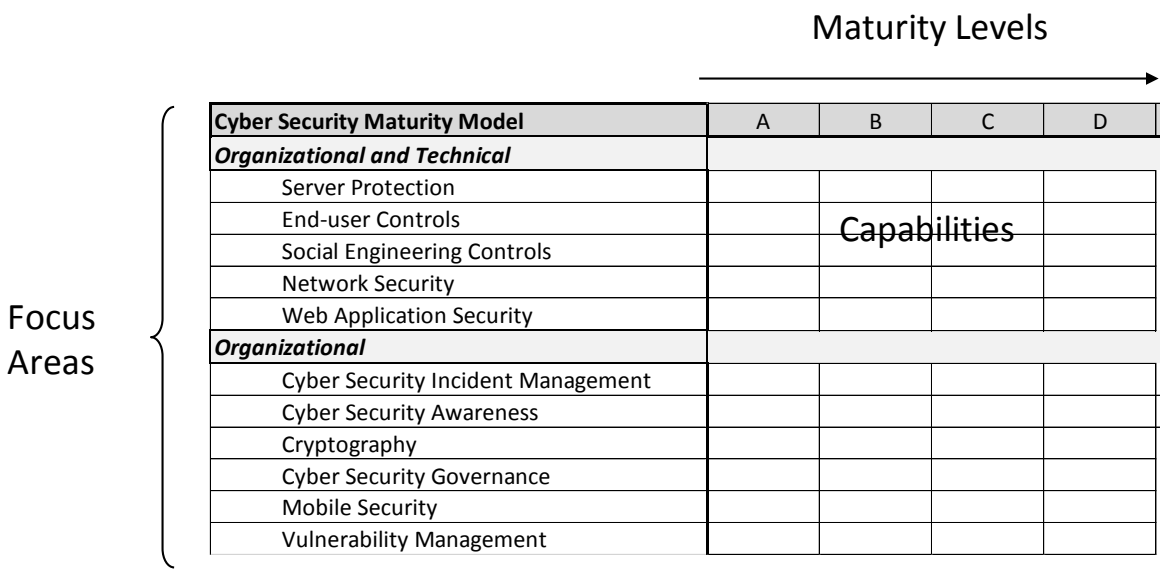

Figure 1: CYSFAM Maturity Model

CYSFAM is applied for assessing an organisation, for planning capability improvements, and for tracking improvement progress. To assess the organisation the focus areas relevant for the organisation are chosen and YES/NO statements about the capability suggested for these focus areas evaluated. To plan improvements, the company selects capabilities that it aims to have institutionalised within the improvement timeframe. The selected capabilities are then assessed at the end of the timeframe, and the updated YES/NO statements reflect the maturity improvement of the company.

Table 2 shows an extract of the CYSFAM model: the statements for the focus area *Server Protection*. The set of questions answered with YES reflects the company's maturity profile.

Table 2: CYSFAM statements for the focus area "Server Protection."

Maturity Levels	**A**	**B**	**C**	**D**
Baseline Security Configuration	The organisation's baseline security configuration is described.	The baseline security configuration is based on an open standard.	The baseline security configuration is reviewed at least once a year.	The baseline security configuration is updated after every significant configuration change or demonstrated vulnerability.
Patch Management	Patch management is tool-supported (patch-management suites).	The deployment of patches is tested and approved at least once before deployment in the production environment.	A process is in place that assures the organisation learns about patch releases as soon as possible.	The prioritisation of patches is risk-based; the business-cruciality is taken into account.
Security Incident and Event Management	A SIEM solution is in place.	The SIEM implementation is based on a baseline set of events.	The SIEM implementation includes events that were identified during a risk assessment.	The SIEM solution is connected to a managed SOC for a correlation of events, and is connected to the organisations' incident management system.

Maturity Levels	A	B	C	D
Technical Compliance Checking	A technical compliance checking solution is in place.	Technical compliance checking is performed manually (supported by appropriate tools).	Technical compliance checking is performed with the assistance of automated tools (with a reporting functionality).	The technical compliance checking solution is connected to the organisations' incident management system.

A CYSFAM-based assessment lets a company evaluate itself against the statements of each focus area in the order of increasing maturity levels. For example, to assess the capabilities related to the baseline configuration, the company first evaluates whether it has described a baseline security configuration (row "Baseline Security Configuration," column A in Table 2). If the configuration is described, the evaluation progresses to the question whether the configuration is based on an open standard (column B). Again, if the company confirms the statement, the evaluation proceeds to the next-higher maturity level. The evaluation of the focus area ends if a statement is rejected or the highest maturity level has been reached. In the former case, the rejected statement becomes an improvement target. In the latter case, the focus area is considered to be fully developed.

An organisation that implements the CYSFAM focus areas consistently at the highest maturity levels exhibits the following features. It has set up a comprehensive and well-managed documentation of policies and systems that define what is being regulated and what the regulation policies are. It has set up a sufficiently funded, accountable, and tool-supported organisation with well-defined roles for multiple lines of defences that are systematically audited and measured. The organisation's ICT architecture is decoupled and human errors minimised to avoid the emergence and propagation of security incidents. For its digital products and services, the organisation employs a secure development lifecycle that includes automated testing, version control, vulnerability scanning, and systematic management of incidents, defect, and patches. The organisation's operations address cybersecurity proactively with comprehensive vulnerability scanning and incident recovery for systems and security awareness, control, feedback, and measurement programs for the employees.

2.3.2 ISFAM Maturity Model

The ISFAM maturity model "Cybersecurity Focus Area Maturity Model" [Spruit2014] is intended to be tailored and applied by small and medium-sized organisations (SME) that utilise ICT for their operations [Mijnh2016]. The model has been developed in collaboration with multiple SME and cybersecurity experts. It offers transparency and metrics to measure cybersecurity. Management and service/product owners who use the model benefit from awareness of cybersecurity and the understanding of how to manage it.

Comparable to the CYSFAM approach, in the centre of ISFAM is a maturity matrix that describes capabilities for a set of focus areas. The focus areas reflect the organisation and technical concerns of the organisation. The capabilities describe practices that the organisation employees to protect its operations. The capabilities are ordered according to the maturity they represent for the organisation. Figure 2 gives an overview of the structure of the ISFAM model.

Focus Area: Maturity Level:	0	1	2	3	4	5	6	7	8	9	10	11	12
Organizational													
1. Risk Management				A		B		C			D		
2. Policy Development			A		B						C		
3. Organizing Information Security		A			B					C		D	
4. Human Resource Security				A		B		C		D			
5. Compliance				A		B						C	
Technical													
6. Identity and access management					A		B		C		D		
7. Secure software development					A		B			C		D	
Organizational and Technical													
8. Incident management			A			B			C			D	
9. Business Continuity Management				A		B		C			D		E
10. Change Management				A		B		C		D			
Support													
11. Physical and environmental security						A		B		C			D
12. Asset Management			A				B			C		D	
13. Architecture				A		B			C		D		
	Design					*Implementation*		*Operational Effectiveness*			*Monitoring*		

Figure 2: ISFAM Maturity Model

ISFAM is applied for assessing an organisation, for planning capability improvements, and for tracking improvement progress. To assess the organisation the focus areas relevant for the organisation are chosen and YES/NO statements about the capability suggested for these focus areas evaluated. To plan improvements, the company selects capabilities that it aims to have institutionalised within the improvement timeframe. The selected capabilities are then assessed at the end of the timeframe, and the updated YES/NO statements reflect the maturity improvement of the company.

2.4 Employees' Cybersecurity Awareness Training

As described in D2.1 section 4.1.13, several offerings are available for cybersecurity awareness training. In contrast to the capability improvement frameworks, such training targets the individual employee and not the company as a whole. For example, such training may be used to encourage an employee to know and adhere to the organisation's baseline security configuration that has been established by following a capability improvement framework like CYSFAM. The cybersecurity awareness training is thus an important complement to capability improvement.

The following tables give an overview of the target audiences offered by existing cybersecurity awareness training products and important focus areas of these offerings. Table 3 covers the training of good practices, Table 4 compliance with regulations.

Table 3: Cybersecurity awareness training offerings for good practice.

Target	Employee							Developer	Operator	Manager	
Provider	General	Phishing	Social Engineering	Mobile Computing	Data Handling	BYOD	Privacy	Security Engineering	Privileged User	Risk Management	Insiders
SANS Securing the Human[3]	X	X						X	X		
Wombat Security Education Platform[4]	X	X	X	X		X					
PhishMe Simulator[5]		X									
Mediapro Security Awareness[6]	X	X	X	X	X	X	X	X	X	X	X

Table 4: Cybersecurity awareness training offerings for compliance.

Targeted Industry Employees	Healthcare		Retail	Utilities
Provider	American HIPAA	American Red Flag	American PCI DSS	American NERC CIP
SANS Securing the Human	X			X
Wombat Security Education Platform	X		X	
PhishMe Simulator				
Mediapro Security Awareness	X	X	X	

The employee training is an important tool to improve awareness of cybersecurity problems of SMEs and bring good practices to these organisations. The use of such training is thus an essential part of an organisation's capability improvement. To be useful for SMESEC, the training needs to be adapted to the context of European industry and the needs of SMEs. UOP and ATOS will be driving the definition of the SMESEC training modules. The SMESEC awareness and capability building approach outlined later in this document will provide the context in which the employee training is administered.

[3] https://securingthehuman.sans.org/security-awareness-training/overview
[4] https://www.wombatsecurity.com/security-education
[5] https://phishme.com/
[6] https://www.mediapro.com/courses/security-awareness/

3 SME Challenges for Adopting Good Practice

3.1 Literature

Much research was devoted to understanding the hurdles for adopting good cybersecurity practice. This section reports on the results of a keyword-based search for peer-reviewed papers that investigated this topic.

The research literature analysed four adherence goals. The adherence goals target the owners, managers, and employees of the SME and concern compliance with policies, cybersecurity culture, human behaviour, and the employees' cybersecurity awareness and belief. Table 5 gives an overview.

Table 5: Adherence goals

Goal	Target
Employee compliance with requirements	Employees
Promoting cybersecurity culture	SME owners
Improving security behaviour	Employees, managers
Improving employees' cybersecurity awareness and belief	Employees

Several studies researched adherence to good cybersecurity practices in SMEs. The categories of factors that matter includes the knowledge topics of cybersecurity awareness and expertise, the resources available for cybersecurity, the work culture, the use of cybersecurity technology, and the organisational topics of management leadership and governance and employee compliance. Table 6 characterises these factors and possible consequences.

Table 6: Factors influencing adoption and adherence to good cybersecurity practice.

Factor	Characterisation	Consequences
Cybersecurity awareness	A small firm may not fully understand cybersecurity risks and controls. Some SME owners do not see the link between business strategy and ICT or cybersecurity. Employees believe cybersecurity awareness is not an issue. They doubt that they will benefit from security technologies.	SMEs benefit from fact-based information about the criticality of cybersecurity threats for the SME.
Cybersecurity expertise	SMEs possess a weak understanding of the cybersecurity concerns, technologies, and control measures. There is a variation in awareness, training, and education needs of individual employees. SMEs tend to ignore the risk of the uninformed employee and focus on external threats.	Cybersecurity expertise is of critical value and should be offered to any employee.
Resources for cybersecurity	SMEs have scarce resources and invest little funds and time in cybersecurity. An SME can lack the resources required to coordinate and implement cybersecurity or offer security awareness, training and education.	Cybersecurity expertise should require little investment for the SME. Also, the SME should be assisted in the implementation of cybersecurity.

Work culture	The work environment is busy and hectic with a heuristic-based management style. Employees have multiple roles, duties, and, consequently, a variety access. Some employees would not report their mistakes to the management. The national culture may influence the SME's cybersecurity culture.	SMEs benefit from a trusted external knowledge repository with opportunities for Q&A. Results from one nation may not be transferable to another one.
Cybersecurity technology	SMEs do not fully cover the technological aspect of cybersecurity.	SMEs benefit from a reasonable tooling framework that is reasonably protected.
Management leadership	SME owners only review cybersecurity needs occasionally. Few incident reports are produced and read.	SMEs benefit from news about cybersecurity threats.
Governance	SMEs are unlikely to have yet reached the stage of policy, procedure, and responsibility definition. Many SMEs and IT professionals lack awareness about cybersecurity standards and policies. A small company sise may not require documentation of cybersecurity. SMEs are unlikely to assess risks or develop cybersecurity policies.	An SME benefits from template policies that can be configured to the SME's context.
Employee compliance	Organisation' sise is unlikely to have any important effect on employee policy compliance intentions.	Results concerning cybersecurity users may be transferred from studies about any company sise.

There is no agreement in the research community about the special character of SMEs in comparison to large companies. While the factors described in Table 6 were developed for SMEs specifically and by studying SMEs, work that aimed at comparing SMEs with large-scale companies tended to find no differences. Only one out of three papers suggested that company sise may be a factor influencing the adoption and adherence to cybersecurity. As a result, it may be possible to transfer owner, manager, and employee-oriented results from any cybersecurity study to the SMEs context. This conjecture needs to be validated during the SMESEC work, however.

Table 7 presents, for each paper, the challenges of SMEs for adopting and adhering to good cybersecurity practice. Some papers explicitly studied SMEs, and the others compared organisations of multiple sises, including small and medium sises.

Table 7: Categorisation and data extracted from the papers.

Paper	Context	Categories	Challenges
Gundu et al. (2012)	SME	Work Culture, Resources, Awareness	-Employees have multiple roles with a variety access. There is little differentiation of duties in SMEs and, consequently, little control over access to information. -In comparison to large organisations, SMEs have scarce resources. -Engineering SMEs tend to ignore the risk of the uninformed employee and is concerned with external threats. Employees believe cybersecurity awareness is not an issue for them.
Zec et al. (2015)	SME	Resources, Awareness, Work Culture, Technology, Governance	-Low financial investments in cybersecurity. -Ignorance of the cybersecurity domain. -In some SMEs, IT professionals would not report their mistakes to the management. -SMEs have unequal treatment to the organisational, technical, psychological aspects of cybersecurity. The technological aspect is not fully covered by most of the SMEs. -Absence of internal cybersecurity policy in SMEs. Also, the awareness about the cybersecurity standards and policies is low for IT professionals. Security measures, particularly in SMEs are not considered seriously.

Paper	Context	Categories	Challenges
Browne et al. (2015)	SME	Work Culture,	-Small firms are often characterised by "brevity and high levels of fragmentation", and the work environment is invariably busy and hectic, and decision making typified by a heuristic-based management style.
Dojkovski et al. (2010)	SME	Awareness, Work Culture, Resources, Expertise, Governance, Leadership	-SMEs may lack the cybersecurity knowledge, skills and behaviours. Lack of security and risk awareness by SME owners. -The Australian culture may have an influence on the SME's cybersecurity culture (SME owner attitude and behaviour). -Inadequate resourcing for cybersecurity management, particularly worker cybersecurity skills, budget and time. An SME can lack the resources required to coordinate and implement cybersecurity or offer security awareness, training and education (support e-learning). - Most SMEs in developed countries lack formal policies. Without expertise, a small firm does not fully understand cybersecurity risks and controls and is unlikely to perform risk assessments or develop cybersecurity policies. SME owners do not see the link between business strategy and IT and may extend this belief to security technologies. Some doubt that they will benefit from security technologies. -SME owners only review cybersecurity needs occasionally. There are just few incident reports produced and read.
Kaur, Mustafa (2013)	SME	Governance	SMEs are not prepared to adopt cybersecurity simply because a documentation of cybersecurity is not required due to the company's small sise.
Dojkovski et al. (2006)	SME	Expertise, Resources, Governance,	-Many SMEs possess a weak understanding of cybersecurity, security technologies and control measures. In SMEs, there is likely to be a variation in awareness, training and education needs for individual employees. -SMEs lack the funds, time and specialised knowledge needed to coordinate cybersecurity or offer cybersecurity awareness, training and education. -SMEs are unlikely to have yet reached the stage of policy, procedure, and responsibility definition.
Knapp et al. 2009	SME vs large		-Not all aspects of the presented model will apply equally to all organisations (sise can be an important factor, e.g. for deciding whether to establish a cybersecurity office).
Herath, Rao (2009)	SME vs large	Compliance	-Organisation' sise did not have an important effect on employee policy compliance intentions.
Bulgurcu (2010)	SME vs large	Expertise, Compliance	-The authors have not found any important impact of control variables such as level of education and technology knowledge, the sise of organisation, industry type of organisation, or information intensity of organisation on an employee's intention to comply with the ISP.

To approach and motivate SMEs, researchers proposed a variety of goals. Many goals concern the employees' cybersecurity awareness and behaviour. Other goals concern the company strategy, manager behaviour, and organisational transformation. Table 8 shows these goals and motivations that should be cultivated. These goals and motivations can be used to guide a SMESEC awareness and capability improvement program to assist the SMEs.

Table 8: Cybersecurity goals and motivation

Paper	Target	Goal	Motivation
Li et al. (2014)	Employee awareness, behaviour	Improve employees' awareness, behaviour, and belief	Employees' awareness, skills, and behaviour are critical to defending against cyber risks.

Paper	Target	Goal	Motivation
Kaur, Mustafa (2013)	Employee awareness	Improve awareness by creating and maintaining security-positive behaviour (connect knowledge, attitude, and behaviour with awareness).	Lack of awareness exposes the SME to significant risk. The development and adoption of policy should be used as an opportunity to raise awareness.
Herath, Rao (2009)	Employee behaviour	Improve the understanding of employee compliance to ISP.	Security behaviours can be influenced by both intrinsic and extrinsic motivators. Pressures exerted by subjective norms and peer behaviours influence employee cybersecurity behaviours.
Gundu et al. (2012)	Employee behaviour	Cultivate positive security behaviours towards policy compliance and positive security culture.	A cybersecurity policy does not guarantee that employees understand their role. Influencing the employees' intention affects their knowledge and behaviour but not necessarily their attitude.
Zec et al. (2015)	Employee behaviour	Examine how employees take decisions for cybersecurity by measuring their level of guilt and shame proneness.	Guilt and shame influences individuals' security thinking and decision-making.
Cheng et al. (2013)	Employee behaviour	Explain employees' violation of cybersecurity policies.	An improved understanding of employee behaviour leads to improved manageability of adherence.
Bulgurcu (2010)	Employee behaviour	Motivate the employee to comply with ISP.	Employees' adherence to organisational policies is essential to successful organisational functioning.
Browne et al. (2015)	Strategy, manager behaviour	Highlight the SME's priorities and predict managers' behaviour for assessing security concerns and implementing responses.	The priorities and manager behaviour affect attitudes and behaviours of small firms.
Dojkovski et al. (2010)	Organi-sational transfor-mation	Enable an effective cybersecurity culture (integrate behaviour modification and cultural change with important initiatives).	SMEs face challenges developing a cybersecurity culture. The inclusion of cybersecurity in other initiatives cultivates and reinforces desired behaviours.
Dojkovski et al. (2006)	Organi-sational transfor-mation	Foster a cybersecurity culture in SMEs together with the SME owners.	Management commitment and leadership are important influencing factors and should be reinforced.
Knapp et al. 2009	Organi-sational transfor-mation	Describe a cybersecurity policy process model at the organisational level that is comprehensive and results in an enforceable cybersecurity policy.	The most important of the controls to protect valuable information is the cybersecurity policy.

3.2 Experiences of SMESEC Partners

As a second objective, we wanted to understand how SMEs react to the CYSFAM model of cybersecurity awareness and capability improvement framework. All four SMESEC use case SMEs were invited to self-assess, plan, and track improvements to the CYSFAM model. After the self-assessment and planning, each SME was invited to fill out a short questionnaire to capture their experience and recommendations.

We here give an overview of experiences of the four SMESEC use case SMEs in using CYSFAM for self-assessment, capability improvement planning, and improvement tracking. To ensure the anonymity of the individual use case SME, we use the identifiers SME1, SME2, SME3, and SME4.

Among the four received CYSFAM Assessment, SME2 has the most completed maturity levels (13 completed levels in different focus areas), and SME4 has the least (no completed level). Among all four participating SMEs, SME2 is the one who has the longest experience of managing cybersecurity. Moreover, for the "Mobile Security" focus area, none of the four questionnaires reports any capabilities. And for "Social Engineering Controls" only SME3 has achieved the level A.

Table 9 presents the focus areas achieved in the CYSFAM self-assessment. A maturity level is considered to be reached if all capabilities belonging to it are fulfilled.

Table 9: CYSFAM self-assessment results by SME.

Focus Area	SME1	SME2	SME3	SME4
Server Protection	-	A	-	-
End-user Controls	-	A	-	-
Social Engineering	-	-	-	-
Network Security	A (also C)	A (also C)	A	-
Web Application Security	-	B	A	-
Cybersecurity Incident Management	-	-	-	-
Cyber Security Awareness	-	B	-	-
Cryptography	-	-	A	-
Cybersecurity Governance	-	B (also D)	-	-
Mobile Security	-	-	-	-
Vulnerability Management	-	A (also C)	-	-

As Table 9 shows, hardly any maturity level was achieved by any SME before the use of CYSFAM. Given that CYSFAM has been created as a collection of good practices, the results indicate that hardly any good cybersecurity practice was institutionalised in the SME. This result is consistent with the results obtained by other research that has been described in section 3.1. There is thus much room for SMESEC to bring good practices into the SMEs.

To understand the SMEs' perception of the CYSFAM framework for self-assessment and improvement planning, the SMEs were asked to judge the strengths and weaknesses of the framework. The SMEs determined more weaknesses than strengths.

The strengths revolved around the key ideas of CYSFAM. Appreciated was the structuring the questionnaire into focus areas that allowed division of work and the accuracy of how cybersecurity capabilities were described.

The weaknesses revolved around CYSFAM organisational assumptions and the complexity, structure, and scope of the CYSFAM questionnaire.

- The organisational structure of SME1 and the sise of SME3 do not match the assumptions of CYSFAM. As a result, it was difficult to define the assessment team, and some of the CYSFAM capabilities were difficult to apply.
- The assessment questionnaire was too complex for SME1. Recommendations were given on how to administer the assessment incrementally in steps (see Table 11 below).

- The questionnaire structure and scope were criticised by SME2, SME3, and SME4. Recommendations were given on how to restructure the questionnaire and about the addition of risk management and computer forensics capabilities.

Table 10 shows strengths and weaknesses reported by the four SMESEC use case SMEs.

Table 10: Strengths and weaknesses of CYSFAM according to SMEs.

SME	Strengths	Weaknesses
SME1	-Ability to divide work when self-assessing.	-Organisational structure: CYSFAM assumes an organisational structure that does not meet the structure of SME1. -Questionnaire complexity: The CYSFAM questionnaire is too complex for SME1.
SME2	-	-Questionnaire structure: the technical compliance checking seems to refer to the application development, but here it is in the Servers Protection section. -Questionnaire scope: in the governance section, we miss some questions regarding the methodology of risks.
SME3	-	-Organisational structure: CYSFAM assumes an organisational structure that does not meet the small sise of SME3. -Questionnaire structure: the section Network Security should be divided into Internal Company Network and Internal Cloud Network.
SME4	-Very well described	-Questionnaire scope: Computer forensics section missing.

When being asked for recommendations and wishes, the four SMESEC use case SMEs suggested again approaches for handling CYSFAM complexity and for restructuring and rescoping the CYSFAM questionnaire. New were suggestions about the improvement methodology and guidance.

- The assessment questionnaire is too complex for SME1. Recommendations were given of how to administer the assessment incrementally in steps.
- The questionnaire structure and scope were criticised by SME2, SME3, and SME4. Recommendations were given of how to restructure the questionnaire and about the addition of application development, risk management, computer forensics, IoT security, and Cloud security, Dos/DDoS, DB injection, and Man-in-the-middle protection capabilities.
- SME1 and SME4 suggested enhancements to the capability improvement methodology. Assuming a definition of the organisation's assets and practices, they would appreciate the indication of a fast ramp-up of cyber protection. The improvements should be supported by indicating budgets, minimising efforts, and feedback for calibrating the right amount of cybersecurity. Also, recommendations for procedures, policies, templates, and tools would be appreciated.

Table 11 shows a summary of recommendations and wishes of the SMESEC use case SMEs.

Table 11: Recommendations and wishes from the participating SMEs.

SME	Recommendations	Wishes
SME1	-Do self-assessment and improvements step-wise in parallel to the maturation of the company.	-Indicate the biggest opportunities for improvements (“security holes”). -Indicate budgets for improvements. -Minimise the effort to be invested for improvements. -Offer feedback for calibrating the right amount of cybersecurity.

SME	Recommendations	Wishes
SME2	-Restructuring of the questionnaire by adding a section on application development capabilities. -Addition of risk management capabilities.	-
SME3	-Restructuring of the questionnaire by dividing network security into internal company network and internal cloud network.	-Addition of DoS and DDoS attacks protection on all systems and services accessible from the Internet. -Addition of DB Injection protection. -Addition of Man-in-the-middle protection.
SME4	-Company and solution-specific planning of cybersecurity. -Addition of computer forensics capabilities. -Improvement of IoT security. -Improvement of Cloud security.	-Guidance for improving cybersecurity procedures and policies. -Guidance for acquiring templates and tools.

The rest of this chapter describes the detailed results for each of the four participating SME. The results are being used for the SMESEC capability improvement approach, the "SMESEC Cybersecurity Roadmap for SME."

3.2.1 Experience of SME1

Table 12 gives a number overview of the CYSFAM self-assessment performed by the SME. The CYSFAM assessment grid was used for self-assessment by two members of the SME.

Table 12: CYSFAM self-assessment by SME1 (shaded cells: fully achieved maturity)

Cybersecurity Maturity Model	A	B	C	D	E
Organisational and Technical					
Server protection	2/4	0/4	0/4	1/4	
End-user Control	2/4	2/4	0/4	0/3	
Social Engineering Controls	0/2	0/2	0/2	0/1	
Network Security	3/3	1/3	3/3	0/3	
Web Application Security	1/2	0/2	0/2	1/2	
Organisational					
Cybersecurity Incident Management	0/4	0/4	0/4	0/4	
Cybersecurity Awareness	0/4	0/4	0/4	0/3	0/1
Cryptography	0/4	0/4	0/4	0/4	
Cybersecurity Governance	0/4	1/4	0/4	0/2	
Mobile Security	0/4	0/4	0/4	0/4	
Vulnerability management	0/2	0/2	0/2	0/2	

The SME members had the following comments about their CYSFAM-based self-assessment and improvement planning. Two questions for clarification were raised. Four statements were given that would allow an expert to confirm or disconfirm the appropriateness of the fulfilment of a CYSFAM statement. One statement described a degree of fulfilment. One statement concerned planning-related information. Table 13 gives an overview.

Table 13: SME's comments or questions about CYSFAM statements.

CYSFAM Statement	SME Comment or Question	Type
The deployment of patches is tested and approved at least once before deployment in the production environment.	What if this is manual?	Question for clarification
The organisation has an (operational) method to alter ACLs, rules, signatures, blocks, and so forth quickly in case of an attack.	ACL?	Question for clarification
A SIEM solution is in place.	Three monitoring services are being used for the physical infrastructure.	Seeking confirmation
Using local-administrator rights is an auditable event.	Login to machines is auditable	Seeking confirmation
The organisation has established a Senior Management committee that takes an active interest in cybersecurity matters.	We consider SMESEC team as the security committee.	Seeking confirmation
The organisation embraces management practices to foster a productive work environment (e.g. decreasing stress and increasing self-care).	But we already have a stress free working environment	Seeking confirmation
The organisation automates all testing (not only security-testing but also other test-disciplines, such as regression testing).	Partially	Degree of fulfilment
The defence against Social Engineering threats is an integral part of the organisations' Security Management process.	But we would like it to be	Planning

The SME was also asked to share their experiences of using CYSFAM for self-assessment and improvement planning. Perceived good was the possibility to divide assessment work. Improvement opportunities were found in the relaxing of assumptions about the organisational structure, in the handling of cybersecurity jargon, and in the simplification of the questionnaire. The attractiveness of the approach could be increased by improving the guidance, predictability, and efficiency of the improvements and offering feedback to calibrate the "amount" of cybersecurity to implement.

Table 14 gives an overview of the SME's perceived strengths, limitations, and recommendations for an improved approach for SMEs.

Table 14: SME's perceived strengths and weaknesses of CYSFAM, and recommendations for improvement.

Category	Statement	Theme
Strength	The categorisation of capabilities that can be assigned to different teams to check and manage - The extensive list of capabilities including the user factor (social engineering)	Work division
Weakness	It is assumed that a company already has a cybersecurity assessment team (you ask for its expertise in the title of these documents). The security experts of small companies are their developers.	Assumed organisational structure
	We think that the questionnaire is too complex for small enterprises (even from the first questions).	Questionnaire Complexity
	After a point, there is no point in answering no to everything.	Questionnaire Complexity

Category	Statement	Theme
Recommen-dation	For validating out assumption we asked some small start-ups and SMEs, near our geographic location, one or two questions randomly selected from the model (without sharing the document, since it is confidential). Some people (yes with active companies) didn't even know what the terms SIEM or CIRT mean.	Cybersecurity jargon
	We would suggest having a first section with "increasing complexity" questions to check the respondent's security awareness level. Then, based on this do one of the following: - For the people with some expertise: follow with the questionnaire as it is. - For the less experienced people give instructions on how to start with security (contact an expert, read specific topics and instructions etc.) If you plan to use this questionnaire and identify the responder's awareness level directly from the given answers, we believe that the questionnaire it is too complex, and people will simply give up after the first few questions, and won't bother with it again.	Questionnaire Complexity
	We would suggest to "activate" questions based on previous answers, e.g.: "A SIEM solution is in place" → if YES activate question: The SIEM implementation includes events that were identified during a risk assessment	Questionnaire Complexity
Wishes	(top 1) Given a very specific budget, identify the biggest "security holes" of our company and cover them.	Improvement guidance and predictability
	(top 2) For the above wish, require the minimum involvement of our company's employees.	Improvement efficiency
	(top 3) Be convinced of the "amount" of security we need to implement.	Improvement feedback

3.2.2 Experience of SME2

Table 15 gives a number overview of the CYSFAM self-assessment performed by the SME. The CYSFAM assessment grid was used for self-assessment by one member of the SME.

Table 15: CYSFAM self-assessment by SME2 (shaded cells: fully achieved maturity)

Cybersecurity Maturity Model	A	B	C	D	E
Organisational and Technical					
Server protection	4/4	2/4	2/4	1/4	
End-user Control	4/4	3/4	2/4	1/3	
Social Engineering Controls	1/2	0/2	0/2	0/1	
Network Security	3/3	2/3	3/3	2/3	
Web Application Security	2/2	2/2	1/2	1/2	
Organisational					
Cybersecurity Incident Management	3/4	1/4	0/4	0/4	
Cybersecurity Awareness	4/4	4/4	1/4	1/3	0/1
Cryptography	2/4	2/4	0/4	0/4	
Cybersecurity Governance	4/4	4/4	2/4	2/2	
Mobile Security	0/4	0/4	0/4	0/4	
Vulnerability management	2/2	1/2	2/2	0/2	

The SME members had the following comments about their CYSFAM-based self-assessment and improvement planning. Two questions for clarification were raised. Four statements were given that

would allow an expert to confirm or disconfirm the appropriateness of the fulfilment of a CYSFAM statement. Table 16 gives an overview.

Table 16: Strengths and weakness of CYSFAM according to SMEs by CYSFAM question.

CYSFAM Statement	SME Comment or Question	Type
The A technical compliance checking solution is in place.	Do you refer to technical compliance with the security required or with the general functionality? Do you mean, for example, Quality Assurance techniques to check that the solution implemented matches the security specification?	Question for clarification
The organisation embraces management practices to foster a productive work environment (e.g. decreasing stress and increasing self-care).	What kind of practices? Nice environment? Or specific activities?	Question for clarification
Patch management is tool-supported (patch-management suites).	APT or YUM tools for package management in servers	Seeking confirmation
A SIEM solution is in place.	Combination of Splunk, OSSEC, and other appliances that generate logs	Seeking confirmation
The deployment of patches is tested and approved at least once before deployment in the production environment.	Depends on the criticism [probably: criticality] of the [supported service].	Seeking confirmation
Technical compliance checking is performed with the assistance of automated tools (with a reporting functionality)	Sonar and Jenkins tools are used to detect errors when changes are done.	Seeking confirmation

The SME was also asked to share their experiences of using CYSFAM for self-assessment and improvement planning. No strengths were perceived. Improvement opportunities were found in the scope and structure of the CYSFAM questionnaire. In particular, risk management practices were suggested to be added.

Table 17 gives an overview of the SME's perceived strengths, limitations, and recommendations for an improved approach for SMEs.

Table 17: SME's perceived strengths and weaknesses of CYSFAM, and recommendations for improvement.

Category	Statement	Theme
Strength	-	-
Weakness	The technical compliance checking seems to refer to the application development, but here it is in the Servers Protection section.	Questionnaire structure
	In the governance section, we miss some questions regarding the methodology of risks.	Questionnaire scope
Recommendation	Should it be a section for the application development practices? Or, could we say that this is out of the scope of the assessment?	Questionnaire scope
	We recommend adding the following: - The organisation has defined a risk assessment methodology - The organisation has identified the risks related to the system - The organisation has defined the context for the risk assessment - The organisation has a monitoring system in place to maintain regular surveillance over the risks and threats identified - Responsibilities for monitoring and review are clearly defined	Questionnaire scope
Wishes	-	-

3.2.3 Experience of SME3

Table 18 gives a number overview of the CYSFAM self-assessment performed by the SME. The CYSFAM assessment grid was used for self-assessment by one member of the SME.

Table 18: CYSFAM self-assessment by SME3 (shaded cells: fully achieved maturity)

Cybersecurity Maturity Model	A	B	C	D	E
Organisational and Technical					
Server protection	2/4	2/4	1/4	0/4	
End-user Control	2/4	3/4	1/4	0/3	
Social Engineering Controls	0/2	0/2	0/2	0/1	
Network Security	3/3	2/3	2/3	1/3	
Web Application Security	2/2	0/2	0/2	1/2	
Organisational					
Cybersecurity Incident Management	0/4	0/4	0/4	0/4	
Cybersecurity Awareness	0/4	0/4	0/4	0/3	0/1
Cryptography	4/4	1/4	0/4	0/4	
Cybersecurity Governance	0/4	0/4	0/4	0/2	
Mobile Security	0/4	0/4	0/4	0/4	
Vulnerability management	1/2	0/2	0/2	0/2	

The SME did not give any comments or ask questions about the CYSFAM-based self-assessment and improvement planning.

The SME was also asked to share their experiences of using CYSFAM for self-assessment and improvement planning. No strengths were perceived. Improvement opportunities were found in the relaxing of assumptions about the organisational structure and the questionnaire structure. The attractiveness of the approach could be increased by adding guidance for DoS and DDoS protection, DB injection protection, and Man-in-the-middle protection.

Table 19 gives an overview of the SME's perceived strengths, limitations, and recommendations for an improved approach for SMEs.

Table 19: SME's perceived strengths and weaknesses of CYSFAM, and recommendations for improvement.

Category	Statement	Theme
Strength	-	-
Weakness	Scalability to really small companies is very low	Assumed organisational structure
	In my opinion, these (Network Security) should be divided into two sections	Questionnaire structure
Recommendation	(Network Security), One section for internal company network and second for internal cloud network. In our company, these are two different policies.	Questionnaire structure
Wishes	(Top 1) DoS and DDoS attacks protection on all systems and services accessible from Internet (VPN, Logging to our system that we provide as a service to our customers)	Guidance for DoS and DDoS protection
	(Top 2) DB Injection protection, as a provider of Web apps we are always very afraid of Injections	Guidance for DB injection protection
	(Top 3) Man in the middle protection – Men analysing and	Guidance for Man-in-

Category	Statement	Theme
	manipulating JavaScript in server <> End-user communication	the-middle protection

3.2.4 Experience of SME4

Table 20 gives a number overview of the CYSFAM self-assessment performed by the SME. The CYSFAM assessment grid was used for self-assessment by one member of the SME.

Table 20: CYSFAM self-assessment by SME4 (shaded cells: fully achieved maturity)

Cybersecurity Maturity Model	A	B	C	D	E
Organisational and Technical					
Server protection	0/4	1/4	0/4	0/4	
End-user Control	0/4	1/4	0/4	0/3	
Social Engineering Controls	0/2	0/2	0/2	0/1	
Network Security	0/3	1/3	0/3	0/3	
Web Application Security	1/2	0/2	0/2	0/2	
Organisational					
Cybersecurity Incident Management	0/4	0/4	0/4	0/4	
Cybersecurity Awareness	0/4	0/4	0/4	0/3	0/1
Cryptography	0/4	0/4	0/4	0/4	
Cybersecurity Governance	0/4	0/4	0/4	0/2	
Mobile Security	0/4	0/4	0/4	0/4	
Vulnerability management	0/2	0/2	0/2	0/2	

The SME had the following comments about their CYSFAM-based self-assessment and improvement planning. Three statements were related to the acquisition of templates and tools. Three statements were given that would allow an expert to confirm or disconfirm the appropriateness of the fulfilment of a CYSFAM statement. One statement described a degree of fulfilment, and two statements concerned planning-related information. Table 21 gives an overview.

Table 21: Strengths and weaknesses of CYSFAM according to SMEs by CYSFAM question

CYSFAM Statement	SME Comment or Question	Type
The organisation's baseline security configuration is described	We don't have a baseline security configuration. We want to create it in SMESEC.	Acquire template
Patch management is tool-supported (patch-management suites).	We don't have patch management tools	Acquire tools
A SIEM solution is in place	We would like to install one in the cloud	Acquire tools
The deployment of patches is tested and approved at least once before deployment in the production environment	We have a staging environment where patches are applied and tested before going to production	Seeking confirmation
The organisation operates all critical infrastructural services (DNS, file, mail, web, database) on a separate physical or virtual machine.	We use separate virtual machines for each critical infrastructure service.	Seeking confirmation
The organisation has implemented Version Control in its Application Change Management process	Bitbucket	Seeking confirmation
Cyber Security Incident Management (all	We don't have a CIRT	Degree of

CYSFAM Statement	SME Comment or Question	Type
capabilities).		fulfilment
The compliance or audit standards that the organisation needs to adhere to are identified.	We are in this process	Planning
The organisation runs scheduled vulnerability scans on all production machines on their network.	We have done some tests, but nothing has been scheduled yet as we are waiting to create the cybersecurity policy first	Planning

The SME was also asked to share their experiences of using CYSFAM for self-assessment and improvement planning. Perceived good was the accuracy of the questionnaire. Improvement opportunities were found in the scope of the questionnaire. Computer forensics should be added, and guidance for IoT security and Cloud security be enhanced. The SME hopes to receive guidance for improving cybersecurity procedures and policies and for acquiring templates and tools.

Table 22 gives an overview of the SME's perceived strengths, limitations, and recommendations for an improved approach for SMEs.

Table 22: SME's perceived strengths and weaknesses of CYSFAM, and recommendations for improvement.

Category	Statement	Theme
Strength	Very well described	Accuracy of the questionnaire
Weakness	Computer forensics section [missing]	Questionnaire scope
Recommendation	Add computer forensics section to the grid involving disk imaging, memory imaging, network forensics, legal procedures, among others	Questionnaire scope
Wish	(Top 1) A general cybersecurity plan for the solution and the company	Improvement guidance
	(Top 2) Strengthen IoT security	Guidance for IoT security
	(Top 3) Strengthen Cloud security	Guidance for Cloud security
Comment	We would like that this project helps us to create the proper cybersecurity documents, procedures and policies so we can have them in place as soon as possible	Improvement guidance

4 SMESEC Awareness Roadmap

Cybersecurity is somewhat like quality management. Slightest changes may affect the security of a product. In this context, not only the product itself is defining the level of security achieved. Surrounding effects such as shared infrastructures, changing regulatory environments, shifted public perception, or new threats are factors too which may have a drastic impact on the security of a system.

The improvement or maintenance of a certain security standard is thus a demanding task for an SME. Keeping track of the parts is very hard as there is often not enough expertise within the company to identify all weaknesses of the product. SMESEC aims here to give a framework enabling SMEs to keep track of all relevant parts and support them in analysis and scoring.

This section describes the SMESEC approach to awareness and capability building. It also describes the FHNW CYSEC tool for guiding the SME in awareness and capability building and obtaining feedback on the SMEs' experiences for iterative tailoring of the SMESEC framework and adaptation of the cybersecurity practices to the SME context.

4.1 Awareness and Capability Building

SMESEC helps SMEs become aware of threats and build capabilities to counter these threats with a threat-oriented incremental approach. The threat-orientation ensures that the SME understands the value of the actions that SMESEC encourages. The incremental approach ensures that capability-building is lightweight and the SME is under control of when to stop.

Supporting the capability-building is guidance for allowing the SME to improve the management of cybersecurity. Such manageability is important to sustain built cybersecurity capabilities, to spread the capability across the organisation in a consistent fashion, and to accelerate the building of further capabilities. The manageability improvement actions are again incremental and oriented around the characteristics of the SME, including its asset and organisational structure. This orientation allows the SME to put a focus on the critical parts of the SME that are to be protected and improve the other parts at later stages.

Figure 3 shows the stepwise processes followed to build capabilities and manageability incrementally.

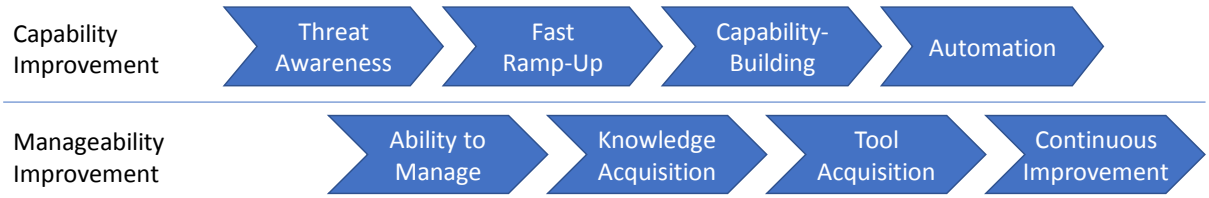

Figure 3: SMESEC capability improvement process: capability and manageability improvement.

Capability improvement starts with threat awareness, allowing an SME to select those threats that are most critical first. Once a threat is selected, SMESEC encourages practices that allow fast ramp-up of cybersecurity capabilities with minimal effort and large positive impact on the SME. The ensuing capability-building step then strengthens the initially built capabilities and allows specialisation for the

SME's threat situation. The final automation step focusses on efficiency for the repeated applications of the capabilities.

Table 23 defines the initially planned set of SMESEC means for capability improvement. Threat awareness is being addressed by SMESEC dissemination, which routes SMEs to the member section of the SMESEC homepage. Fast ramp-up will be offered by guidance for patch management, access control and audit, and malware scans. These practices will be further strengthened and complemented with further practices for capability-building. The SMESEC platform will offer advice that allows the SME to prioritise and select the relevant practices and to measure the expected impact of each practice. The adoption and use of the practice will be supported by practice-specific training and templates. Feedback will be offered to the SME for calibrating the approach chosen to implement a practice. The final means for capability improvement will be references to tools, including the SMESEC tools, for accelerating the repeated application of the practices in the SME context.

Table 23: Initial themes for capability improvement

Means	Value	Relevance
SMESEC Dissemination	Raises awareness about threats and points to SMESEC framework for solutions addressing these threats	Threat Awareness
Patch Management	Addresses Denial of Service, Vulnerable Components, Broken Authentication, Injection, XSS, Sensitive Data, Object References, CSRF, Redirects and Forwards, and Access Control	Fast Ramp-Up
Access Control and Audit	Addresses Broken Authentication, Malicious Insiders, and Missing Access Control	Fast Ramp-Up
Malware Scans	Reduces threats	Fast Ramp-Up
Code Inspection	Reduces Denial of Service, DB injection, and identification of security holes.	Fast Ramp-Up
User Training	Establish cybersecurity awareness, knowledge and good behaviour	Fast Ramp-Up
Absorption Networks	Addresses Distributed Denial of Service	Capability-Building
Network Controls	Reduces threats	Capability-Building
Intrusion Prevention	Reduces Denial of Service and DB Injection threats	Capability-Building
Credential Management	Addresses T04 Security Misconfiguration, T09 Malicious Insiders, and T13 Missing Access Control	Capability-Building
Second Opinion Defence	Mitigates tool-, service-, and method-specific weaknesses	Capability-Building
Security Engineering	Engineering of assets to prevent misuse and malicious behaviour.	Capability-Building
Application Change Management	Management of assets to prevent accidental introduction of vulnerabilities.	Capability-Building
Compliance Audits	Ensures implementation of security baseline	Capability-Building
Standards Compliance	Risk management and satisfaction of customer requirements	Capability-Building
SMESEC Tools	Hardens the cybersecurity measures, accelerates, and reduces operational cost	Automation

Table 24 defines the initially planned set of SMESEC means for manageability improvement. Manageability improvement starts with the SME's ability to manage cybersecurity. Initial steps are the offering of the CYSEC cybersecurity coach, which allows the SME to declare the assets, initiate vulnerability scans, and define security baselines. SMESEC also offers the use of the SMESEC SIEM for security information and event management. SMESEC will also offer guidance for managing cybersecurity in the medium-sized organisation, which benefits from CIRT, budgeting and funding, and suitable governance approaches. Knowledge acquisition will be tailored to the capabilities to be

built by the SME. Similarly, the tool offering will be tailored to the automation choices by the SME. Continuous improvement, finally, will allow the SME to capture lessons-learned and adapt the guidance to the specific needs of the cybersecurity users and to offer feedback and suggestions to the cybersecurity community.

Table 24: Initial themes for manageability improvement (ME: medium-sized enterprises)

Means	Value	Relevance
Cybersecurity Coach	Guidance in awareness and capability improvement	Ability to Manage
Asset Management	Threat manageability	Ability to Manage
Vulnerability Scans	Discovery of threats	Ability to Manage
Security Baseline	Definition of SME's cybersecurity practices	Ability to Manage
SIEM	Security information and event management	Ability to Manage
CIRT Team and Process	Offers guaranteed response to security-relevant events.	Ability to Manage (ME)
Budgeting and Funding	Offers capacity to build security and respond to security-relevant events.	Ability to Manage (ME)
Governance	Establishes autonomy and accountability in the management of cybersecurity.	Ability to Manage (ME)
Training Modules	Access to knowledge	Knowledge Acquisition
Feedback on Capability Implementation	Q&A and calibration of cybersecurity	Knowledge Acquisition
SMESEC Tools	Ability to automate	Tool Acquisition
End-user programming of CYSEC	Tailoring of cybersecurity coaching with contents and automation that matters to the user.	Continuous Improvement
Feedback and Suggestions for SMESEC	Improvement of the SMESEC approach.	Continuous Improvement

The adaptiveness of the SMESEC framework to the evolving needs of the user SME will be achieved with a rule-based approach of suggesting improvements and monitoring adherence to the recommendations. The role-based approach will be based on a goal model of how cybersecurity capabilities are being built, allowing inference and suggestions of alternatives if adoption and adherence turn out to be too difficult for the SME.

The overall aim is to offer support for the SME to improve cybersecurity step-by-step by focusing on the most important security holes and minimizing the SME's perceived complexity. With the chosen capability improvement approach, cybersecurity awareness and capability-building will get the form of the Plan-Do-Check-Act (PDCA) cycles that are suggested by ISO/IEC 27'001. From the perspective of the cybersecurity community, these cycles resemble the cycles of action research and enable the testing and iterative improvement of cybersecurity advice and tools.

The approach also allows the evolution of the portfolio of practices offered to address cyber threats. Some of the threats are fast changing, for example, due to new software and library releases, and others are slower, for example, due to changes in regulations. The SMESEC platform will allow the SME to be in control for adapting practices and tools. The SMESEC platform will also allow bidirectional communication between the SME to learn from each other and adapt to the evolving needs.

4.2 Recommender and Adherence Monitor

The SMESEC framework will offer the FHNW CYSEC tool for guiding the SME with capability improvements and for monitoring adherence to the recommendations. The CYSEC tool will allow automating advice, tailoring the advice to each SME, and offer feedback to improve how cybersecurity is handled. The CYSEC tool aims at approximating the role of a cybersecurity advisor with automated digital means in an attempt of reducing the cost of cybersecurity capability-building for the SME and scaling the cybersecurity community's ability to interact with SMEs and learn.

The FHNW CYSEC tool will consist of four major components: a capability advisor for recommending improvements to the SME, good practices, templates, and tools for building capabilities, an adherence monitor to know whether the recommendations have been followed, and a bot to offer answers to questions and feedback. CYSEC will be used to automate the interaction with the SME, allow cybersecurity community to understand SME behaviour and rationales, and support SME-managed self-adaptation and community-driven evolution. Figure 4 gives an overview of the CYSEC components and context.

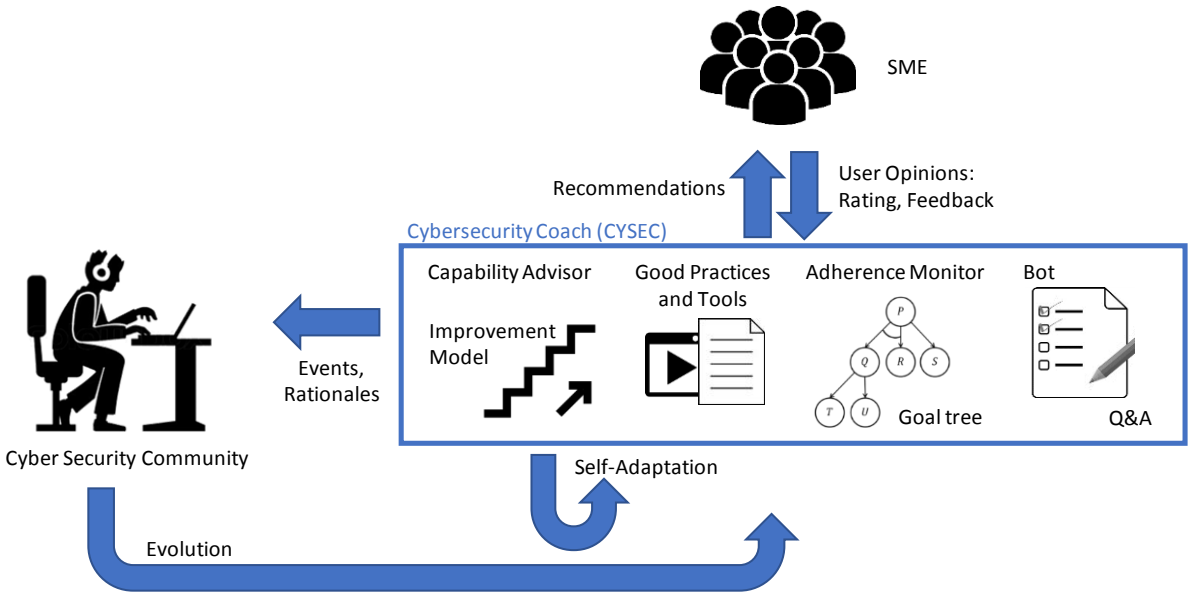

Figure 4: CYSEC Tool

The capability advisor will be based on a questionnaire interface that allows orchestration of the capability and manageability improvement processes. It contains information about the cybersecurity capabilities shown in Table 23 and Table 24, reference to good practices, templates, and tools, and will be parametrised with the dependencies among capabilities to enable the SME's stepwise, guided exposure to cybersecurity.

The good practices, templates, and tools will initially be based on the SMESEC partners' training and the tools included in the SMESEC framework. For the training, UOP, ATOS, and FHNW will have a leading role. The tools will be based on the results of WP3. The good practices, templates, and tools offering will be complement with open source assets and references to offerings external to the SMESEC consortium where applicable.

The adherence monitor is based on a model of the orchestration logic that is encoded as a goal model. Goal models, in comparison to other rule-based approaches, have the advantage that they allow inference and backtracking to alternative tactics for goal achievement if an initial tactic turns out to be failing. The adherence monitoring will be implemented as a goal monitor that observes goal achievement states and decides about the recommendations shown to the SME. Its outputs are used by the capability advisor for self-adaptation and by the cybersecurity community to support the evolution of the SMESEC approach.

The bot encodes the dialogue with the SME that is needed to offer feedback on capability calibration, offer answers to questions, and understand the SME's rationales for adherence, respectively non-adherence to capability recommendations. The bot can also be used to initiate proactive interaction with the SME end users, e.g. for issuing reminders or establishing a dialogue between a cybersecurity community member and the SME.

The CYSEC tool will be deployed in two alternative modes, an on-premise and a cloud-based mode. The on-premise mode allows an SME to keep all its cybersecurity-related data offline and private. Updates and data transfers to the SMESEC cloud are initiated and controlled by the SME. The SMESEC cloud deployment offers CYSEC as a Software-as-a-Service. Also, it acts as the master deployment for aggregating capabilities and feedback data.

5 Awareness and SMESEC Validation Plan

5.1 Industry-Level Awareness: SMESEC Dissemination

In WP6, the SMESEC consortium has been developing a dissemination plan to raise awareness about cyber threats among European SME. The plan is based on a segmentation of European SME and identification of stakeholders that can help inform the SME about the cyber threats. The awareness that is generated is utilised to guide SMEs to SMESEC.EU, which offers the portal for accessing cybersecurity knowledge and the SMESEC framework that can help SME to build cybersecurity capabilities. To achieve these goals, the SMESEC dissemination team develops messages, channels, and material to reach European SMEs, raise awareness, and win their interest, desire to try the SMESEC framework, and action to build cybersecurity capabilities.

According to D6.1, SMESEC dissemination is based on the cornerstones shown in Table 25.

Table 25: Cornerstones of SMESEC dissemination (WP6)

Cornerstone	Elaboration
SME Verticals	SMEs in the SMESEC use case verticals IoT, Smart City, Smart Grid, and e-Voting. Verticals added during the open call, representing the market of European SMEs.
SME Horizontals	Product, service, and project businesses. Young technology start-ups and established medium-sized enterprises.
Events Participation, Scientific Publication, Press, Social Media	Placement of consistent SMESEC messages for the target audiences in industrial channels, academic forums, policy, and standardisation.

SMESEC dissemination will pursue multiple milestones for developing a community of SMEs that are aware of cyber threats and bring the SMESEC framework into use for validation and exploitation. Table 26 gives an overview.

Table 26: Milestones for SMESEC dissemination (WP6)

Milestone	Timing	Elaboration
Cyber threat awareness	Year 1	During this phase, SMESEC dissemination will raise awareness of cyber threats for SMEs. At the same time, the SMESEC brand will be established with the values of trust in SMESEC, respect for the expertise of the SMESEC consortium, and simplicity of the SMESEC framework.
Interest in SMESEC	Year 2	During this phase, SMESEC dissemination will communicate results of the SMESEC project and endorsements of SME that were using these results. SMEs will get the opportunity to register in the SMESEC community and apply for the open call.
Adoption of SMESEC	Year 3	During this phase, SMESEC dissemination will communicate results of SMESEC validation to encourage adoption of the SMESEC framework. More SMEs will register in the SMESEC community and enable broad adoption of the framework.

The deliverable D6.1 elaborates on the dissemination strategy and plan.

5.2 Framework Validation: SMESEC Open Call

This section provides a brief description of the procedures SMESEC intends to follow for the realisation of the Open Call. According to the Description of Action, the Open Call will be prepared

during M20-M24, executed during M24-30, and analysed during M31-M36 in the context of Task 5.5. The steps and the procedures below describe an overview of the Call and provide a roadmap. These are the initial steps identified, and we may proceed with improvements, additions and fine-tuning before the activity takes place.

The process to publish the open call and evaluate the applications will be executed according to the following step-wise process:

1. Define requirements and regulations for applicants: definition of requirements and eligibility criteria for participants of the open call.
2. Finalise the open call: definition of a detailed guideline and frequently asked questions (FAQ) for the call.
3. Dissemination of the call: definition of a plan including dissemination targets, actions, and timeline and execution of the plan.
4. Expert evaluation of the application: establishment of the expert board and evaluation of the applications.

The requirements for the open call include those stated in Table 27. The applications will be ranked according to the value they offer to the SMESEC project based on these requirements.

Table 27: Requirements for the open call

Requirement	Elaboration
SME Type	Definition of the type of SME eligible for the call.
Systems	Definition of the systems that are mandatory for the SME to have in place and need to be protected by SMESEC. Examples: web server, databases, network connectivity, and core services.
Deployment	The SME should create a detailed deployment plan of how the SMESEC framework is going to be deployed and integrated into their systems. The plan shall include a definition of the security features they expect from SMESEC.
Experience	SMESEC prioritises first-time users and SMEs that do not have a security platform for their SME and will benefit most from the SMESEC framework.
Exploitation Impact	Description of the SME's current impact along with an exploitation plan on how they can benefit with the integration of the security framework. The description includes a definition of participating in the call can benefit and increase the SME's impact in their respective field.
Financials	Financial statement or expected costs.

The eligibility criteria for the open call include those stated in Table 28. The applications must fulfil all eligibility criteria to be considered.

Table 28: Eligibility criteria for the open call

Criteria	Elaboration
Participation	Criteria that need to be met by an SME to be eligible to participate in this call. Examples: conflicts of interest, number of employees, participation in other calls and projects.
Privacy and Ethics	Implementation of the GDPR rules and implement the ethics screening requirements imposed on the SMESEC project. SMESEC will provide the eligible organizations with consent forms for the users that validate and teste the systems integrated with SMESEC. The selected organisations will provide information about their internal procedures for data management and ethics and about the process of cooperating with their national data protection authority.
Reporting	Financial and other reports to be included in the respective SMESEC deliverable.

The open call text should be formulated and finalised. Along with the open call, there should be a detailed guide of the call and a FAQ. The detailed guide of the call will contain the complete list of the requirements, eligibility criteria, and deadlines for reports or any other deliverables in a detailed step-

by-step guide on how to format and submit the application. The FAQ for the applicants should be included covering the most prominent requirements and steps of the application process along with items that are not discussed in the guide. The FAQ can also be revised during the application phase as SMESEC receives input and questions from the applicants.

The dissemination of the call will be managed with a publicity and public awareness plan. The plan will be detailed with timelines about the dissemination and publication of the open call so that the open call will reach as many SMEs as possible. The plan will include dissemination platforms, events, and places across Europe. The dissemination channels will be listed and used to publish the open call material. The channels include the SMEs' related public sites, projects, R&D boards, and innovation and entrepreneurship sites. To implement the dissemination in Europe, SMESEC organises or participates in SME innovation meetings and summits. These events should be spread across Europe, like the North, Centre, and South-Balkans.

The expert evaluation board will be set up with consortium members. The board will be responsible for the evaluation of the applications received for the open call. It will refine the requirements and eligibility criteria by defining the basic criteria for the evaluation and a scoring system with thresholds, weights, and final score for each application. The board will use meetings and teleconferences as applicable.

A timeline will be created with specific dates, milestones, and goals. A board should be in place to ensure that the respective dates and goals are met. The timeline will include both internal and external deadlines. Table 29 shows the targeted milestones.

Table 29: SMESEC open call milestones

Milestone	Type	Timing	Elaboration
Camera-ready	Internal	M20-M24	Here, the open call document should be ready. This may or may not include the guide of the call.
Publication	External	M20-M24	Here, the open call document will be published to the public.
Application Submission	External	M20-M24	Here, each application will have been collected by electronic means like a web-based submission system.
Acceptance	External	M20-M24	Here, the evaluation results will be published along with the protocol that will be used to contact the accepted applicant SMEs.
Reporting	External	M31-M36	Here, the SMEs will provide SMESEC with the report of using the SMESEC framework. The date will be set between M30 and M33 of the project. The reports will be used as the input for reporting about SMESEC evaluation and testing in the D5.5 deliverable.

5.3 Enabling Secure SME: SMESEC Evolution and Exploitation

SMESEC will evolve the SMESEC framework and the awareness roadmap that brings the SMESEC framework into use over multiple releases. Initially, the framework and roadmap described in section 4 are tested with the four SMESEC SME use cases. The validation will then be scaled with the open call described in section 5.2. At each stage, the framework and awareness roadmap are undergoing critical evaluation from the perspectives of its users, the SMEs. Each time, lessons are being collected about the created value impact and opportunities for improvement, comparable to the lessons about CYSFAM presented in section 3.2. These lessons are used to evolve the framework and awareness roadmap. The SMESEC consortium expects these results to be mature and ready for exploitation at the end of the SMESEC project.

Table 30 shows the milestones that are planned for evolving and exploiting SMESEC. The SMESEC description of action further elaborates the planned work.

Table 30: Milestones for SMESEC evolution and exploitation

Milestone	Timing	Elaboration
Initial Release	M18	The first version of the SMESEC framework and awareness plan are released to the SMESEC use case SMEs. The development and validation are coordinated in parallel.
Initial Validation I	M18	The SMESEC framework and awareness plan will have been evaluated, lessons-learned collected, and redesign planned. The development and validation are coordinated in parallel.
Second Release	M24	The second version of the SMESEC framework and awareness plan is released to the SMEs participating in the SMESEC open call. The evolution and validation are coordinated in parallel.
Internal Validation II	M24	The SMESEC framework and awareness plan will have been evaluated, lessons-learned collected, and redesign planned. The evolution and validation are coordinated in parallel.
Open Call	M32	The SMESEC framework and awareness plan will have been evaluated, lesson-learned collected, and redesign planned.
Third Release	M36	The third version of the SMESEC framework and awareness plan is released to the market of European SMEs.
Exploitation	M36 onwards	The SMESEC framework and awareness plan are being owned by the respective SMESEC partners and exploited for product, service, and project business beyond the SMESEC project.

6 Summary and Conclusions

This document described the SMESEC awareness roadmap. It described the awareness goals that SMEs should aim for, the SMEs' hurdles in adopting good cybersecurity practice, the cybersecurity capability improvement approach that SMESEC proposes, and the plan for validating the approach.

An analysis of existing surveys, standards, and frameworks has been used to identify awareness goals. The main cybersecurity threats that companies should be aware of have been outlined for web applications, mobile applications, and the internet of things. As described in D2.1, these threats should be prioritised according to the SMEs with which SMESEC collaborates.

An overview of the existing approaches has been given, including cybersecurity standards and cybersecurity capability improvement frameworks. None of these existing approaches targets SMEs. For that reason, tailoring is needed that addresses the SMEs' hurdles for adopting good cybersecurity practice.

To understand the hurdles for adopting good practice, we have reviewed relevant literature and let the four SMESEC use case SMEs experience the cybersecurity capability improvement framework CYSFAM. SMSEC should aim at helping SMEs to establish a good cybersecurity culture and help employees to become aware, comply, and behave. The challenges to overcome will be lacking cybersecurity awareness and expertise, lacking resources for cybersecurity, a buy and hectic work environment, and low maturity in cybersecurity leadership, governance, and employee compliance. The CYSFAM framework offers a good starting point for building a tool to assess, plan, and improve the cybersecurity capabilities of an SME. However, the framework needs to be lightweight with fast results and adapted to the threats that are prioriticed by the user SME.

This document has proposed a process and roadmap to improve the cybersecurity awareness and capabilities of SMEs. The process builds on the results of evaluating CYSFAM and offers threat awareness, fast ramp-up, capability building, and automation. Supporting the cybersecurity capability improvements are improvements of the SME to manage cybersecurity, including knowledge acquisition, tool acquisition, and continuous improvement.

The SMESEC open call will be used to validate the SMESEC approach with new SME that join the consortium. The requirements on the SME will include the characteristics of the SME, the systems it aims at protecting, the deployment of SMESEC. The eligibility criteria will include conflicts of interest, sise, involvement in EU projects, and willingness to comply with reporting. A preliminary overview of the SMESEC open call has been provided.

The results of this document will be used as an input for WP3 in support of the SMESEC security framework development. The CYSEC approach will be developed by FHNW and integrate UOP and ATOS training modules. Their use will be reported in D3.5 and D3.6. The document will also be used as a basis for piloting, for evaluating the adoption of tailored versions of the SMESEC cybersecurity framework with SMEs as outlined in WP4. The document will also be used as a basis for the open call, which is used to assess the SMESEC cybersecurity framework with the open call. D5.5 will report on the open call.

References

[OWASP 2013] The Open Web Application Security Project (OWASP), "OWASP TOP 10 – 2013: The Ten Most Critical Web Application Security Risks," https://storage.googleapis.com/google-code-archive-downloads/v2/code.google.com/owasptop10/OWASP%20Top%2010%20-%202013.pdf, 2013, accessed Sept 21, 2017.

[OWASP 2014] The Open Web Application Security Project (OWASP), "Internet of Things Top Ten," https://www.owasp.org/images/7/71/Internet_of_Things_Top_Ten_2014-OWASP.pdf, 2014, accessed Sept 21, 2017.

[OWASP 2016] The Open Web Application Security Project (OWASP), "Mobile Top 10 2016-Top 10," https://www.owasp.org/index.php/Mobile_Top_10_2016-Top_10, 2016, accessed Sept 21, 2017.

[ARMOUR 2016] Armour Consortium, "Experiments and Requirements," Deliverable D1.1, http://www.armour-project.eu/wp-content/uploads/2016/08/D11-ARMOUR-Experiments-and-Requirements.pdf.

[bsi100-1] BSI Standard 100-1 Cybersecurity Management Systems (ISMS) https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-1_e_pdf.pdf?__blob=publicationFile&v=1

[bsi100-2] BSI-Standard 100-2: IT-Grundschutz Methology https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-2_e_pdf.pdf?__blob=publicationFile&v=1

[Bsi100-3] BSI-Standard 100-3: Risk Analysis based on IT-Grundschutz https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-3_e_pdf.pdf?__blob=publicationFile&v=1

[Spruit2014] Spruit, M. & Röling, M. (2014). ISFAM: the information security focus area maturity model. 22nd European Conference on Information Systems, Tel Aviv, Israel.

[Mijnh2016] Mijnhardt, F., Baars, T., & Spruit, M. (2016). "Organisational characteristics influencing SME information security maturity." Journal of Computer Information Systems 56.2 (pp. 106-115).

[sipo2013] Elsevier, "Employees' adherence to cybersecurity policies", 2013, Mikko Siponen, M. Adam Mahmood, Seppo Pahnila http://www.sciencedirect.com/science/article/pii/S0378720613001237/pdfft?md5=7f3882c68be917b767dee28b2e59ba73&pid=1-s2.0-S0378720613001237-main.pdf&_valck=1

[bulg2010] MIS Quarterly, "Cybersecurity Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Cybersecurity Awareness", 2010, Burcu Bulgurcu, Hasan Cavusoglu, Izak Benbasat

[Gund2012] Gundu, T., & Flowerday, S. V. (2012, August). The enemy within: A behavioural intention model and a cybersecurity awareness process. In Cybersecurity for South Africa (ISSA), 2012 (pp. 1-8). IEEE.

[Zec2015] Zec, M., & Kajtazi, M. (2015, September). Examining how IT Professionals in SMEs Take Decisions About Implementing Cybersecurity Strategy. In ECIME2015-9th European Conference on IS Management and Evaluation: ECIME 2015 (p. 231). Academic Conferences and publishing limited.

[Brow2015] Browne, S., Lang, M., & Golden, W. (2015). Linking Threat Avoidance and Security Adoption: A Theoretical Model For SMEs. In Bled eConference (p. 35).

[Dojk2010] Dojkovski, S., Lichtenstein, S., & Warren, M. (2010, January). Enabling cybersecurity culture: influences and challenges for Australian SMEs. In ACIS 2010: Proceedings of the 21st Australasian Conference on Information Systems. ACIS.

[Kaur2013] Kaur, J., & Mustafa, N. (2013, November). Examining the effects of knowledge, attitude and behaviour on cybersecurity awareness: A case on SME. In Research and Innovation in Information Systems (ICRIIS), 2013 International Conference on(pp. 286-290). IEEE.

[Li2014] Li, L., He, W., Xu, L., Ivan, A., Anwar, M., & Yuan, X. (2014, August). Does explicit cybersecurity policy affect employees' cybersecurity behavior? A pilot study. In Enterprise Systems Conference (ES), 2014 (pp. 169-173). IEEE.

[Cheng2013] Cheng, L., Li, Y., Li, W., Holm, E., & Zhai, Q. (2013). Understanding the violation of IS security policy in organisations: An integrated model based on social control and deterrence theory. Computers & Security, 39, 447-459.

[Dojk2006] Dojkovski, S., Lichtenstein, S., & Warren, M. (2006, January). Challenges in fostering a cybersecurity culture in Australian small and medium sized enterprises. In ECIW2006: proceedings of the 5th European conference on Information Warfare and Security (pp. 31-40). Academic Conferences Limited.

[Knap2009] Knapp, K. J., Morris, R. F., Marshall, T. E., & Byrd, T. A. (2009). Cybersecurity policy: An organisational-level process model. Computers & Security, 28(7), 493-508.

[Hera2009] Herath, T., & Rao, H. R. (2009). Encouraging cybersecurity behaviors in organisations: Role of penalties, pressures and perceived effectiveness. Decision