



**Bridging the security, privacy, and data protection gap for  
smaller enterprises in Europe**

## **D1.1: The SENTINEL baseline**



This work is part of the SENTINEL project. SENTINEL has received funding from the European Union's Horizon 2020 Work Programme for research and innovation 2018-2020 under grant agreement n°101021659.

## Project Information

<b>Grant Agreement Number</b>	<b>101021659</b>
<b>Project Acronym</b>	SENTINEL
<b>Project Full Title</b>	Bridging the security, privacy, and data protection gap for smaller enterprises in Europe
<b>Starting Date</b>	1 <sup>st</sup> June 2021
<b>Duration</b>	36 months
<b>Call Identifier</b>	H2020-SU-DS-2020
<b>Topic</b>	H2020-SU-DS-2018-2019-2020 Digital Security and privacy for citizens and Small and Medium Enterprises and Micro Enterprises
<b>Project Website</b>	<a href="https://www.sentinel-project.eu/">https://www.sentinel-project.eu/</a>
<b>Project Coordinator</b>	Dr. George Bravos
<b>Organisation</b>	Information Technology for Market Leadership (ITML)
<b>Email</b>	gebravos@itml.gr

## Document Information

<b>Work Package</b>	
<b>Deliverable Title</b>	D1.1: The SENTINEL baseline
<b>Version</b>	1.0
<b>Date of Submission</b>	30/09/2021
<b>Main Author(s)/ Editor(s)</b>	Evangelia Kavakli (IDIR), Pericles Loucopoulos (IDIR), Yannis Skourtis (IDIR)
<b>Contributor(s)</b>	Artemios Geromitsos (INTRA), Daryl Holkham (TIG), Yorkvik Jacqmin (SHELL), Zoe Anna Kasapi (CECL), Leonidas Kallipolitis (AEGIS), Christopher Konialis (CG), George Nikitakis (STS), Thomas Oudin (ACS), Spyros Papastergiou (FP), Georgios Tsirantonakis (TSI), Philippe Valoggia (LIST)
<b>Reviewer(s)</b>	Paulo Figueiras (UNINOVA), Ruben Costa (UNINOVA), Tatiana Trantidou (ITML)

Document Classification							
<b>Draft</b>		<b>Final</b>	X	<b>Confidential</b>		<b>Public</b>	X

History			
Version	Issue Date	Status	Distribution
<b>1.0</b>	07/09/2021	Draft	Confidential
<b>1.1</b>	22/09/2021	Draft	Confidential
<b>1.2</b>	24/09/2021	Draft	Confidential
<b>1.3</b>	27/09/2021	Draft	Confidential
<b>2.0</b>	28/09/2021	Final	Public

## Table of Contents

List of Figures .....	6
List of Tables .....	6
Abbreviations .....	7
Executive Summary .....	9
1 Introduction .....	10
1.1 Purpose of the Document .....	11
1.2 Structure of the Document .....	11
1.3 Intended readership .....	12
2 Cybersecurity for privacy: Challenges .....	14
2.1 Introduction .....	14
2.2 SME-specific challenges and barriers to adoption .....	14
2.3 Cybersecurity and personal data protection needs .....	17
2.3.1 Generic key concepts for requirements .....	17
2.3.2 Assets and Threats .....	18
2.4 Cybersecurity in the Cloud .....	22
2.4.1 Cloud focus areas .....	22
2.4.2 Cloud threats .....	27
2.4.3 Matching Cloud concepts and architectures with threats .....	31
2.5 Legal Considerations .....	32
2.5.1 The concept of personal data .....	32
2.5.2 Basic principles of data processing for SMEs .....	33
2.5.3 Innovations of the General Data Protection Regulation .....	34
2.6 Summary: Generic and technical requirements .....	37
3 Cybersecurity for privacy: Managing risk .....	38
3.1 Introduction .....	38
3.1.1 Common misconceptions .....	38
3.1.2 Recommendations for boosting cyber awareness .....	39
3.2 Assessing risk .....	40
3.2.1 SMEs and information security risk .....	40
3.2.2 ENISA's methodology for the security of personal data processing .....	40
3.3 Mitigating risk .....	47
3.3.1 Introduction .....	47

3.3.2	Organisational measures for personal data protection .....	48
3.3.3	Technical measures for personal data protection .....	50
3.4	Summary: Responding to the challenges .....	54
4	The SENTINEL digital platform .....	55
4.1	Introduction .....	55
4.2	The SENTINEL architecture .....	55
4.2.1	An overview of the framework's structure and functionality .....	55
4.2.2	Front-end components .....	56
4.2.3	Self-assessment and training portal .....	57
4.2.4	Digital core .....	57
4.2.5	Observatory .....	58
4.2.6	SENTINEL cybersecurity and personal data protection components .....	58
4.3	Using SENTINEL: a sample scenario .....	60
4.4	SENTINEL contributed components .....	61
4.4.1	Security Infusion .....	61
4.4.2	Identity management system .....	63
4.4.3	GDPR self-assessment methodology .....	65
4.4.4	MITIGATE: evidence-driven risk assessment .....	68
4.4.5	Security and privacy assurance platform .....	70
4.4.6	Cyber Range .....	72
4.4.7	Forensics Visualisation Toolkit .....	73
4.5	Summary: SENTINEL's technological innovation .....	75
5	SCORE: The SENTINEL RE methodology .....	76
5.1	Introduction .....	76
5.2	The SCORE meta-model and its modelling views .....	77
5.2.1	The SCORE conceptual foundation .....	77
5.2.2	The SCORE modelling .....	80
5.3	The SCORE way-of-working .....	83
5.4	Summary: SENTINEL RE methodology .....	86
6	Demonstrating the use of SCORE on the pilot cases .....	86
6.1	Introduction .....	86
6.2	The business cases .....	87
6.2.1	TIG pilot needs .....	87
6.2.2	CG pilot needs .....	89

6.3	Application of SCORE to the TIG case.....	91
6.3.1	Identify TIG Current Situation.....	92
6.3.2	Risk analysis.....	96
6.3.3	Design TIG Future Situation.....	97
6.3.4	Assess Satisfiability of Change Goals.....	99
6.4	Application of SCORE to the CG case .....	99
6.4.1	Identify CG Current Situation .....	99
6.4.2	Risk analysis.....	103
6.4.3	Design CG Future Situation .....	103
6.4.4	Assess Satisfiability of Change Goals.....	104
6.5	Summary: A practical approach for eliciting user requirements.....	104
7	Conclusions .....	106
7.1	Reflections on objectives attained and related KPI.....	106
7.2	The way forward .....	108
7.2.1	Tool support for SCORE .....	109
7.2.2	Ontologies .....	110
7.2.3	Using patterns for best business practice in CS for privacy for SMEs .....	111
	Acknowledgments.....	112
	References .....	113
	Appendix I Objectives for Deliverable D1.1 .....	118
	Appendix II Questionnaire for business centric information gathering .....	119
	Appendix III Questionnaire for technology centric information gathering .....	123
	Appendix IV Expanded list of high-level requirements.....	125

## List of Figures

Figure 1. The envisioned SENTINEL conceptual architecture .....	55
Figure 2. A CyberRange work zone .....	72
Figure 3. The top-level SCORE concepts.....	78
Figure 4. Detailing Level 0 SCORE concepts.....	78
Figure 5. The SCORE way of working.....	84
Figure 6. TIG current goals and related capabilities .....	92
Figure 7. TIG current capabilities and perceived threats .....	93
Figure 8. Current TIG actors and their dependencies and potential vulnerabilities .....	94
Figure 9. TIG informational model.....	95
Figure 10. Inter-model relationships between TIG models of the current situation.....	96
Figure 11. TIG change goals.....	97
Figure 12. TIG desired capabilities.....	98
Figure 13. Tracing threat mitigation.....	99
Figure 14. CG current capabilities and perceived threats .....	100
Figure 15. CG current goals and related capabilities .....	101
Figure 16. CG current actors and their dependencies and potential vulnerabilities.....	102
Figure 17. CG informational model.....	102
Figure 18. CG change goals .....	103
Figure 19. CG desired capabilities .....	104

## List of Tables

Table 1. Matching threats with Cloud concepts and architectures .....	31
Table 2. Generic and technical requirements for cybersecurity and personal data protection....	37
Table 3. Threat likelihood per area.....	46
Table 4. Threat probability level .....	46
Table 5. Risk level evaluation, per threat.....	47
Table 6. SENTINEL proposed components and modules mapping.....	58
Table 7. Mapping generic requirements to SI component .....	62
Table 8. Mapping generic requirements to IdMS component.....	64
Table 9. Associating SME activities with risk level for compliance.....	66
Table 10. Requirements overview for the GDPR self-assessment methodology .....	67
Table 11. Mapping generic requirements to GDPR assessment methodology component.....	67
Table 12. Mapping generic requirements to MITIGATE component .....	69
Table 13. Mapping generic requirements to SPAP component .....	71
Table 14. Mapping generic requirements to CyberRange component .....	73
Table 15. Mapping generic requirements to FVT component .....	74
Table 16. Graphical notation used in capability modelling .....	80
Table 17. Graphical notation used in goal modelling .....	81
Table 18. Graphical notation used in actor-dependency modelling.....	82
Table 19. Graphical notation used in informational object modelling .....	83
Table 20. SCORE process questionnaire.....	85
Table 21. Overview of TIG businesses.....	87
Table 22. TIG types of data.....	88

## Abbreviations

Abbreviation	Explanation
<b>2FA</b>	Two Factor Authentication
<b>ACL</b>	Access Control List
<b>API</b>	Application Programming Interface
<b>BCP</b>	Business Continuity Plan
<b>CCM</b>	Cloud Controls Matrix
<b>CIA</b>	Confidentiality, Integrity, Authenticity
<b>CORE</b>	Capability Oriented Requirements Engineering
<b>CS</b>	Cybersecurity
<b>CSP</b>	Cloud Service Provider
<b>DCV</b>	Dynamic Capability View
<b>DDoS</b>	Distributed Denial of Service
<b>DoS</b>	Denial of Service
<b>DoA</b>	Description of Action
<b>DPIA</b>	Data Protection Impact Assessment
<b>DPO</b>	Data protection Officer
<b>ENISA</b>	European Union Agency for Cybersecurity
<b>FVT</b>	Forensics Visualization Toolkit
<b>GDPR</b>	General Data Protection Regulation
<b>IAM</b>	Identity and Access Management
<b>ICMP</b>	Internet Control Message Protocol
<b>IDMS</b>	Identify Management System
<b>IaaS</b>	Infrastructure as a Service
<b>IoT</b>	Internet of Things
<b>IPS</b>	Intrusion Prevention System
<b>IR</b>	Incident response
<b>ISMS</b>	Information Security Management System
<b>IT</b>	Information Technology
<b>KPI</b>	Key Performance Indicator
<b>LDAP</b>	Lightweight Directory Access Protocol
<b>MiTM</b>	Man in The Middle
<b>MEs</b>	Micro Enterprises
<b>MFA</b>	Multifactor Authentication
<b>NIST</b>	National Institute of Standards and Technology
<b>NFR</b>	Non-Functional Requirements
<b>NTP</b>	Network Time Protocol
<b>OT</b>	Operational Technology
<b>PaaS</b>	Platform as a Service
<b>PDP</b>	Personal Data Protection
<b>PET</b>	Privacy Enhancing Technologies
<b>RASE</b>	Risk Assessment for Small Enterprises
<b>RBV</b>	Resource Based View
<b>RE</b>	Requirements Engineering
<b>SaaS</b>	Software-as-a-service
<b>SCORE</b>	Security Capability Oriented Requirements Engineering
<b>SDLC</b>	Software Development Life Cycle

<b>SecaaS</b>	Security-as-a-Service
<b>SLA</b>	Service Level Agreement
<b>SMEs</b>	Small and Medium Enterprises
<b>SPAP</b>	Security and Privacy Assurance Platform
<b>SSH</b>	Secure Shell
<b>TOMs</b>	Technical and Organisational Measures
<b>UDP</b>	User Datagram Protocol
<b>VM</b>	Virtual Machine
<b>XSS</b>	Cross-Site Scripting



## Executive Summary

Deliverable D1.1 (*The SENTINEL Baseline*) has been produced within Work Package (WP) 1 (*SENTINEL Baseline: Setting the Methodological Scene*) of the SENTINEL project under task T1.1 (*The SENTINEL Requirements Engineering Methodology*). The aim of this task was to investigate and to report on the parameters that drive the needs for data privacy and compliance processes in SMEs and to define the relevant **Requirements Engineering (RE) methodology**.

Over 25 million European Small to Medium size Enterprises/ Micro Enterprises (referred to henceforth collectively as SMEs), central within EU enterprise policy, face multiple challenges related to personal data protection; ranging from awareness to a clear and practical roadmap to compliance, the most prominent one is the fact that, unlike larger enterprises, SMEs lack access to enterprise-grade cybersecurity (CS) technology and capacity-building for compliance, making them increasingly often victims of costly data breaches. SENTINEL aspires to bridge this gap by boosting SMEs capabilities in this domain through innovation at a cost-effective level.

Contemporary CS and privacy architectures, consist of diverse collections of components which increase the severity of the framework to ensure integrity, and at the same time prohibits the smooth adaptation, incorporation and utilisation of digital solutions, leading to a complex set of requirements that need to be modelled and understood.

This deliverable meets the aim of Task T1.1 along two dimensions.

*Firstly*, concerning the needs of SMEs, the report clearly identifies and discusses the specific challenges to SMEs that drive their requirements for an improved, customised and usable way of dealing with their CS for privacy. These challenges are discussed in the context of organisational, legal and technical concerns. Particular attention is paid to the challenges presented to SMEs due to their increasing desire for migration towards the Cloud. Eleven major cloud threats to SMEs are presented in depth and the association between these threats and cloud concepts and architectures is succinctly juxtaposed and presented in a table that could serve as a pivotal reference point. The challenges, threats and needs, result in a set of major generic and specific requirements, which are also presented in a concise tabular form. The tables are used to associate SENTINEL components with system requirements and to inform the ontology for the overall Requirements Engineering methodology.

*Secondly*, concerning the definition of the SENTINEL RE methodology, the report presents a methodology, developed for SENTINEL, that is innovative, generic, and dedicated to CS for privacy needs of SMEs. The methodology is presented along two dimensions: its foundational concepts; and its process to be followed using these concepts. The backdrop to the way of working is a set of user-facing questions that link the methodology to the ENISA guidelines. To demonstrate its applicability the methodology was applied on both of the pilot cases identified in the DoA.

# 1 Introduction

Security is the sum of quality attributes such as availability, safety, or robustness of an information system or product. It contributes toward ensuring that processing, storing, and communicating information sufficiently protects confidentiality, integrity, and authenticity (a triad often referred to as CIA). In order to protect systems, it is vital that security requirements are identified and systematically realized into security measures that meet these requirements. Enterprises, regardless of their size, must manage the CS risks to improve the security and resilience of their assets. In the case of SMEs additional challenges present themselves because of lack of resources and of relevant in-house expertise (Benz and Chatterjee, 2020).

The work of WP1 contributes to the overall SENTINEL specific objective “**S.O. 2** Provide scientific and technological advances ... towards the comprehensive digital Privacy and PDP compliance framework for SMEs/MEs” and meets the related key performance indicator (KPI) “**KR-2.1** Innovative customized RE-related models deployed with respect to security- and data privacy-aware mechanisms ensuring data protection in SMEs/MEs”.

This document reports on a number of contributions corresponding to the objectives of task T1.1. Specifically:

**Challenges and threats to SMEs:** It introduces the specific challenges faced by SMEs with respect to CS and personal data protection, focusing on generic and high-level security requirements and identifies the major threats to CS and privacy which SMEs face in their operating environment, both internal and external. It also introduces the challenges presented to SMEs by the adoption of the Cloud, as well as the threats which arise and the critical focus areas in the domain. It provides an overview of the legal landscape for protecting personal data, focusing on the basic principles and requirements of the General Data Protection Regulation (GDPR), including special provisions and exemptions for SMEs. The introduced challenges and threats give rise to both generic and specific requirements which are presented in a referenceable manner in such a way so as to relate these to the SENTINEL components.

**Assessing and managing risk:** It presents the concept of information security risk. It mentions common myths believed by SME stakeholders towards CS and personal data protection (interpreted as compliance with the GDPR) and recommends measures for increased cyber awareness. This is followed by an exposition of the concept of evaluating risk when SMEs process personal data, addressing: identifying the personal data processing environment and operations, assessing impact (DPIA), defining threats’ likelihood and, eventually, calculating the level of risk. Finally, it analyses both organisational and technical measures for personal data protection assorted by their assigned impact level(s).

**Requirements for the SENTINEL platform:** It presents the desired functionalities of the SENTINEL platform. These functionalities will be realised through a combination of component capabilities of the SENTINEL participants’ technical and methodological assets and new components to be developed within the project. For each component a summary of its functionalities is presented and very importantly a mapping is presented with respect to the component’s functionality in addressing generic and specific requirements. This mapping is clearly done using the table mentioned in the paragraph above (“Challenges and threats to SMEs”). In this first phase of the project, we focus on an abstract definition of generic

requirements specific to SMEs. These will be tailored in later phases, to define the way that these requirements will be realised by the SENTINEL platform as an integration of all the components which are presently defined as standalone.

**The SENTINEL RE methodology:** It reports on the developed methodology whose purpose is to establish a generic process specifically targeting SMEs to address their needs and capabilities in such a way so as to enable these companies to yield the benefits of using the SENTINEL digital framework. This methodology satisfies one of the main ambitions of the project (see DoA) namely, “*a generic RE methodology specifically targeting SMEs to address their specific needs and capabilities in such a way so as to enable these companies to yield the benefits of using the SENTINEL framework*”. A full exposition of the SENTINEL RE methodology is presented in this report, including its underpinning conceptual foundation and the way of working. To demonstrate the feasibility of the methodology it also reports on the way that the theoretical foundations were applied on two pilot cases, one on social care business and another on genomic medicine.

## 1.1 Purpose of the Document

The purpose of this document is to report on the results produced from work that was carried out in task T1.1 whose aims are: (a) to gain insight into the parameters that drive the needs for data privacy and compliance processes in SMEs and (b) to define the relevant RE methodology.

## 1.2 Structure of the Document

The rest of this document is organised into 6 sections: (i) it considers the challenges faced by SMEs in the CS and PDP domain, (ii) it reports on current state-of-the-art for assessing and managing risk for SMEs, (iii) it positions the technological and methodological assets of SENTINEL, (iv) it introduces the RE methodology specifically developed for the SENTINEL project, (v) it demonstrates the use of this methodology using examples from the two pilot cases and (vi) it concludes by reflecting on achievements to date and proposes future developments based on the results reported in this deliverable. These 6 sections are aligned to the WP1 objectives and T1.1 key issues as defined in the DoA (see Appendix I Objectives for Deliverable D1.1). Specifically:

**Section 2** focuses on the *challenges* faced by SMEs regarding CS for privacy requirements. To this end, it addresses the following objectives and T1.1 aims to:

- Describe in detail and continuously monitor the scientific (academic and industrial) and end-user needs and challenges for secure and trustworthy solutions for SMEs.
- Identify common and most important challenges with respect to the implementation of CS facilitators that can affect the environment’s operation.
- Identify the environment’s fundamental utilities and processes that must be facilitated by combinations of tools, technologies and services related to data privacy and compliance.
- Define the usage characteristics of the environment.

**Section 3** examines the current state-of-the-art *in assessing and managing risk* for personal data protection (PDP), for meeting the challenges described in Section 2. To this end, it aims to:

- Synthesise and present the current state-of-the-art from the viewpoint of the project's highlighted problems.

**Section 4** introduces the proposed SENTINEL architecture and provides a summary of the *background SENTINEL assets* to be deployed and those to be extended within the project in order to provide innovative solutions to the challenges described in Section 2. To this end, this section aims to:

- Identify fundamental data protection utilities that must be deployed, including their individual configurations.
- Define the SENTINEL technological innovation.
- Define basic AI-enabling levels and principles to support the envisioned SENTINEL offerings.

**Section 5** introduces 'SCORE', the *SENTINEL RE methodology*, that is specifically developed for the SENTINEL project, in order to establish the SENTINEL baseline (the overarching WP1 objective). To this end, this section aims to:

- Define the RE methodology.

**Section 6** demonstrates the way that SCORE may be applied using examples from the two pilot cases. The inclusion of the section is to demonstrate the feasibility of the SCORE methodology. It also acts as precursor to task T6.1 during which the detailed requirements of the pilot cases will be elicited and represented. Therefore, this section contributing to the following aim:

- To gain insight into the parameters that drive the needs for data privacy and compliance processes in SMEs.

Finally, **Section 7**, concludes this document with a review of contributions to meeting all stated objectives in the DoA, presents a reflective discussion on findings, discusses the way that the results of T1.1 meet the stated KPI in the DoA, and outlines a plan on the way that this deliverable could contribute to further work in the SENTINEL project.

In addition to summarising in Appendix I, all WP1 objectives and key issues investigated within T1.1, this report includes two additional Appendices. Appendix II gives details of a questionnaire designed within T1.1 for the purpose of assembling information from business users about their needs for CS. Appendix III reports on a similar questionnaire that was designed specifically for technology providers addressing CS for privacy issues. Information that was gathered from the two questionnaires was analysed and provided a backdrop to the development of the SENTINEL RE methodology. Finally, Appendix IV provides a detailed description of the high-level CS and PDP requirements for SMEs presented in Section 2 and utilised in Section 4, that will eventually lead to a mapping between the actual end-user requirements and their realisation in the SENTINEL digital platform.

### 1.3 Intended readership

This document is intended for both consortium members and external to the project stakeholders. Project members from the two commercial entities with the two pilot cases will gain an understanding on how their requirements could be captured and represented observing also that

they have already actively participated in the demonstration of the RE methodology (see Section 5) but also being prepared for the work to be carried out later on in Work Package 6.

A different set of consortium members, involved in the implementation of the SENTINEL digital platform will benefit from understanding how the functionalities of their own asset will address generic and specific requirements that are analysed and detailed in this report. These stakeholders will also gain an understanding of the missing parts of the proposed digital platform, the kinds of functionality that these missing parts will need to satisfy and how all components, background as well as new ones, will successfully be integrated into an architecture that will meet the overarching objective of the platform. Finally, stakeholders, external to the project, will be informed on the way in which SENTINEL assists in the capture and representation of their SME CS for privacy requirements. This will be especially beneficial in Work Package 7, during the dissemination and communication phase of the project.

## 2 Cybersecurity for privacy: Challenges

A core SENTINEL ambition is to provide tangible benefits for SMEs looking to improve their security situational awareness and adopt measures towards the protection of personal data for their customers, employees, partners, beneficiaries, etc. This is proposed, having in mind the concept that, security and data breaches are a risk not just to the SME's assets and reputation but, more critically, to the fundamental rights and freedoms of individuals, which constitute core EU values, protected under the GDPR. In this section we attempt to map the challenges which SMEs face in their quest to protect personal data, to better inform SENTINEL's RE Methodology and relevant processes.

### 2.1 Introduction

SMEs are an important driver for innovation and growth in the EU and act as a catalyst for digital growth (ENISA, 2021). SMEs with limited personnel and resources face difficulties in understanding the risks associated with the development of their technologies and their impact. Despite the constant adaptation of new technologies, especially during the COVID-19 crisis, the level of SMEs information security and privacy standard adoption is relatively low (ENISA, 2015).

During the COVID-19 pandemic many SMEs transferred a large portion of their work online by using Cloud services or other means, as well as by enabling remote work. This caused an increase in CS challenges in the need for a consistent and iterative approach for identifying, assessing and managing risk.

One of the biggest risks SMEs face is the exposure of users' personal data (data breach), which could lead to the loss of the reliability and trust between the company and its customers and, more importantly, adversely affect the freedoms and rights of the individuals whose data is exposed including, for example, in the case of identity theft or fraud, financial loss, physical or psychological harm, humiliation, damage to reputation or even threat to life (ENISA, 2016). In a recent ENISA study, investigating 249 SMEs EU-wide for their overall CS awareness and related concerns, 80% of the surveyed companies reported that CS issues would have a serious negative impact on their business within a week of the issues happening, and 57% saying they would most likely become bankrupt or go out of business (ENISA, 2021). From this we can draw several conclusions about both the general outlook and the specific challenges SMEs face, so that these could be appropriately related to scientific responses explored in Section 3 and to the SENTINEL background expertise described in Section 4.

### 2.2 SME-specific challenges and barriers to adoption

In the same study, ENISA identified the major CS and PDP **challenges** which these enterprises face, based on an EU-wide survey. These are many and of varying types, although a prevalent theme evident among them is **the lack of SME management motivation and support**. Undoubtedly, when management is aware and motivated towards CS, it will commit to the necessary budget, allocation of resources and the oversight for the effective implementation of these guidelines and practices. Another prominent aspect is the **lack of understandable and workable guidelines for SMEs** in coping with these challenges.



The study files these challenges under eight categories:

- **Lack of cybersecurity awareness;** this is best exemplified by the dominance of cyberattacks relying on social engineering and phishing. Unlike the common perception where CS is just a concern for IT personnel, it is now evident that CS should be part of the company culture while employees should be regularly trained and aware of the implications of the riskiest cyber threats for their organisation.
- **Inadequate personal data security;** The types of personal data and information processed by SMEs are numerous: personnel records, customer and subscriber information, health records, production details, procurement details, financial data, policies, procedures, and many more. A core obligation for all businesses, including of course SMEs (acting either as data controllers or data processors) within **GDPR** is that of the **security of personal data**. Security, in this sense, equally covers, equally, confidentiality, integrity and availability and should be considered following a risk-based approach (ENISA, 2016) where the higher the risk, the more rigorous the measures that the SME needs to take. These measures may include privacy-enhancing technologies such as encryption and anonymization/pseudonymization as well as a plethora of technical and organisational measures which we will examine later in this report. In any case, the lack of an up-to-date and enforced security policy for protecting personal data, including a backup up policy, an always-up-to-date endpoint security solution on all devices, using unpatched software etc, could all make the SME an easy target for cyberattacks and jeopardize the personal data under its control.
- **Inadequate budget;** CS awareness and dedicated employee training, the implementation and testing of robust CS controls, engaging external CS experts, implementing dedicated CS solutions, such as advanced application firewalls or integrated security information and event management systems, can all be large and daunting investments for SMEs. On the other hand, when SMEs adopt Cloud-based SaaS software, they rely on the CS offered by the provider, a proposition that is, the least to say, opaque and unaccountable, especially when it comes to storing and processing personal data. Finally, it's management's prevalent view of CS primarily as a cost factor, not an investment in the business; a view which stems from the lack of understanding of the negative impact of a potential severe security or data breach. Management of all levels should be motivated to understand the risks posed by cyber threats and allocate the necessary resources.
- **Lack of cybersecurity experts;** CS cannot be addressed with partial measures, the occasional installation of security software or the sporadic check by IT personnel who have their attention on a myriad other daily obligation. It requires specialised expertise and rigorous daily application to enforce. SMEs' only options are to either hire dedicated CS specialists or to rely on the regular support of external consultants or domain experts, both of which can be costly and hard-to-find. In ENISA's study, SMEs demonstrated a) a clear shortage of skills and b) not having assigned a dedicated Information Security Officer in their organisation, instead generally delegating information security tasks to the IT department.
- **Lack of suitable cybersecurity guidelines specifically designed for and targeted to SMEs;** Even though a variety of documentation for CS and privacy has existed, either in

the form of comprehensive standards such as the ISO 27001 (ISO/IEC, 2018) or as whitepapers or guidelines addressing specific CS requirements, these often address larger enterprises with an existing management framework, able to implement the range of these objectives with the help of external experts. On the other hand, when CS guidance specifically targeted to SMEs is issued, either at the national or the EU level, it usually fails to reach or motivate individual businesses.

- **Cyber perimeters extending beyond SMEs' control;** Teleworking is an established practice which, by itself, poses several CS challenges, such as configuring and managing VPNs and securing communications over unsecure networks. However, with the advent of COVID-19, SME network perimeters have been effectively extended beyond business premises and into employees' homes. To make matters worse, employees, in an effort to be productive, may use personal mobile devices and cloud services for email or for sharing sensitive SME data. Most SMEs may have not configured complex and costly VPN technology to allow for secure remote access or, if they have, these solutions are not comprehensive, secure or inclusive enough. This results in staff becoming frustrated with the experience and, in an effort to get work done, relying on personal cloud services.
- **Moving to the Cloud;** Undoubtedly, SMEs have much to gain from subscription-based Cloud services and SaaS offerings, which offer them a unique combination of a) only paying for the features they require; b) controlling costs on a monthly basis and c) not having to maintain complex and costly on-premises infrastructure and to perform risky installations, maintenance and updates. However, despite these benefits, SMEs often do not fully understand the associated risks, the most glaring being the fact that their data, including sensitive personal data, resides in infrastructure outside their control and can be more easily exposed to the public Internet, along with the associated administrative interfaces etc. Another aspect of Cloud adoption, further fuelled by the COVID-19 pandemic, is SMEs being more motivated than ever before to "set up shop" online. This has often been done hastily, with SMEs implementing online presence almost "overnight". Especially when **e-commerce** is involved, the risks multiply, since even the simplest e-shops maintain customer data, order history etc. A substantial investment in time and money is therefore required for the services, and the associated processed personal data to be secured. *Due to its significance, we shall dedicate Section 2.4 of this report to this challenge.*
- **Lack of support from management;** As with any endeavour, efforts towards CS strengthening and best practices are doomed to fail without rigorous management support. And unlike large organisations, who can dedicate senior management and lots of resources towards security, SMEs rely on the founder or senior manager's security awareness, perception and personal experience for developing their CS culture. This results in strikingly low CS awareness among SMEs, with management thinking their business is "too small for cyber criminals". This however couldn't be further from the truth. Organisations and companies of all sizes are attacked all the time. SMEs are often favoured by cyber criminals since a) the attackers look to exploit vulnerabilities at scale, without regard for the company size; b) SMEs traditionally have lower security controls in place and c) SMEs can be an ideal entry point towards larger and more valuable companies up the supply chain. It is eventually management's responsibility to instil



employees with a vision for cybersecurity's value and monitor and motivate them towards upholding the SME's security policies.

The SENTINEL project has been designed to address these challenges at their core by mapping every high-level challenge or barrier to a specific set of participant SME CS requirements which, in turn, will be addressed by specific components of the SENTINEL platform. However, since SENTINEL's promise for a participant company is a set of CS- and privacy-enhancing software tools along with a dynamic policy document and a set of guidelines/recommendations, it is ultimately up to the SME's management to dedicate the resources and enact the commitment to monitor and enforce such a policy.

## 2.3 Cybersecurity and personal data protection needs

Over 80% of the surveyed SMEs (ENISA, 2021) process “critical” information which, if exposed would place their owners, as well as the SME itself, under significant risk. Another finding is the ever-increasing use of the Cloud and software-as-a-service (SaaS) solutions which are perceived as a balanced solution to many SME requirements, while keeping costs under control. Finally, a good proportion of SMEs have introduced new technologies in their line of work, especially in response to the COVID-19 pandemic, e.g., for teleworking or e-commerce, without, however, taking into consideration the security improvements and configurations required to ensure the safety and robustness of these solutions.

In the remainder of this subsection we present the key issues underpinning the needs of SMEs for CS, privacy and personal data protection. Specifically, Section 2.3.1 presents the generic requirements while Section 2.3.2 deals with the key concepts which can help formulate the necessary vocabulary/ontologies and drive the requirements for SMEs for privacy and personal data protection.

### 2.3.1 Generic key concepts for requirements

SMEs, just as any type and size of organisation, can assume a set of “non-functional” or “quality” CS requirements. These outline the key concepts employed both for presenting the challenges and threats for SMEs and providing the building blocks for the SENTINEL RE Methodology.

- **Confidentiality:** To protect assets from being exposed to unauthorized parties, for example in the case of a data breach.
- **Integrity:** To only allow modification of assets by authorized individuals.
- **Availability:** To ensure the continuous availability of the SME services and data to authorised users.
- **Non-repudiation:** To provide the assurance that the ownership, validity or authenticity of certain data or logged activities cannot be disputed.
- **Usability:** To provide CS, privacy and personal data protection that are easy and intuitive to use.
- **Cost-effectiveness:** To provide CS, privacy and personal data protection solutions at a cost-effective level for the participant SMEs.
- **Scalability:** To deploy scalable CS, privacy and personal data protection solutions which can effectively support the SME as its business and requirements grow.

### 2.3.2 Assets and Threats

An **asset**, in its general sense, is any piece of data, hardware, software or other component of an SME that has value. For example, an employee's workstation, laptop or company smartphone would be considered an asset. Applications and software which runs on these devices also qualify as assets. The same is true for infrastructure (critical or not), such as servers, network infrastructure and support systems, including Cloud and SaaS-provided services.

However, SMEs' most common and often at-risk assets are *informational ones*. These include personal data (sensitive or not) which may reside in Cloud or on-premises databases as well as in physical (e.g., paper) files. For example, files on employees, customers, a newsletter subscription list, medical records, sales records, customer profiles kept in an online shop database etc.

We define a **threat** as an incident that may adversely affect an SME asset, compromising its confidentiality, integrity or availability.

In this context, we classify threats as:

- Internal or External; and
- Intentional or Unintentional.

**Internal threats** are confined within the organisation's "perimeter" while **external ones** have to "penetrate" it before causing damage. **Intentional threats** include criminal external hacking or a malicious insider stealing information, whereas **unintentional threats** generally involve human error (usually but not always linked to employee action), a technical malfunction or a physical event such as a natural disaster.

It's worth mentioning that, although we opt for this simplified classification [Jouini, L. Ben Arfa Rabaia et al., 2014], to make understanding and managing threats more attainable to SMEs, there exist different established threat classification models, e.g., per threat category (as in Microsoft's STRIDE model, which we'll utilise in subsection 2.4.3), per threat agent/actor, per level of consequence, etc.

#### 2.3.2.1 Internal threats

Internal threats (also known as *insider threats*) are potentially more damaging to an SME, since an insider, malicious or not, possesses internal knowledge, access privileges and direct access to key resources and infrastructure. Below, we present a non-exhaustive listing of the most prominent types of internal threats:

- **Negligent actors:** Employee negligence or error is the most common source for security incidents. While, in most cases, such incidents cost comparatively less to mitigate, their effects can still be harmful to the SME. Examples of human error are:
  - sending sensitive data to the wrong recipient (data leak)
  - misconfiguring an infrastructure, network or software
  - using unsafe workplace practices (e.g., clicking through a phishing email / catching malware)
  - accidental deletion or alteration of data.

- **Malicious actors:** These agents can be extremely harmful to the SME, since they possess internal knowledge about CS measures the organization uses and the sensitive information it processes. Leveraging this knowledge, they may steal or leak data, sabotage production, or provide hackers (third parties) with access to a company's resources. For example:
  - **insider data breach:** The data, of the users, that are kept by the system can be compromised by a malicious insider (e.g., disgruntled employee) e.g., with financial, personal or other incentives.
  - **insider intentional alteration or deletion of sensitive data and/or software:** Malicious insiders could alter or delete sensitive data and/or software.
  - **insider network or application attack** (DoS, code injection, intentional misconfiguration, installation of back-doors etc): A potential direct attack to the SME's network and application resources leveraging its own infrastructure.
- The generic **misuse or abuse of access privileges:** this threat can be an "ingredient" to most attacks described and entails the **abuse of privileges associated with a particular user account**, used inappropriately or fraudulently, either maliciously, negligently or accidentally or even through wilful ignorance of policies. This threat also includes SME IT staff misconfiguring access privileges.
- Other generic technical malfunctions and physical events or disasters.

#### 2.3.2.2 External threats

**External threats** exemplify the risk of attackers from the outside of the SME's "perimeter" attempting to exploit vulnerabilities through the use of malicious software, hacking, sabotage, social engineering and other means. These malicious actors can be individual hackers, hacker or criminal groups, organisations (e.g., competitors) or even, although unlikely for small enterprises, hostile countries. It might even include "benevolent" actors such as hacktivists, white-hat hackers and "script kiddies". For example, malicious competitors might aim to attack the reliability and the proper operation of an enterprise, or gain access to sensitive personal information, in order to steal trade secrets or boost their margin / market part. Hacktivists, on the other hand, could attack a specific SME if they decide it serves a cause which they oppose.

Below, we present a non-exhaustive listing of the most common types and categories of external threats:

- **Malware attacks:** This includes any type of malicious software such as viruses, worms, trojans, spyware, ransomware, rootkits, crypto-miners etc, and is the **most common type of external cyber threat**. Malware will usually infiltrate an SME's infrastructure via a link (e.g., phishing) on an untrusted website or email or an unwanted software download which a careless or cyber-unaware employee would click-through. The malware then installs itself and propagates in the SME's infrastructure, collects sensitive data, manipulates and blocks access to network components, and may even destroy data or shut down entire operations altogether.
- **Social engineering attacks:** As mentioned before, social engineering attempts to trick SME employees into either providing an entry point for malware or directly compromising access credentials or other personal data or sensitive information. The victim provides sensitive information or unwittingly installs malware on their device, because the attacker

usually poses as a legitimate actor. The most common techniques in social engineering attacks are:

- *Baiting*, where the attacker lures the victim with a promise of something attractive like a gift card. The victim provides sensitive information such as credentials to the attacker.
- *Pretexting*, where the attacker pressures the victim into giving up information under false pretences; typically, by impersonating someone with authority, e.g., a government, police, bank or tax officer, whose position would compel the victim to comply. In the example of “voice phishing”, the impersonator uses a simple phone call to trick the victim into disclosing sensitive data or access credentials.
- *Phishing*, by far the most common penetration method, where the attacker sends emails, SMSs or other types of messages pretending to come from a trusted source. These fraudulent emails are usually sent to many potential victims but can also be more targeted and crafted to lure specific victims within the SME. For example, the “spear phishing” attack targets a specific employee, while a “whaling” attack takes this concept a step further by targeting high-value individuals such as CFOs, CEOs etc.
- *Piggybacking*, where an authorized user / victim provides physical access to the attacker who “piggybacks” off the victim’s credentials. For example, an employee may grant access to someone posing as a new employee who misplaced their credential card.
- *Tailgating*, where an unauthorized individual physically follows an authorized user into a location, e.g., by quickly slipping in through a protected door after the authorized user has opened it. In this attack, unlike piggybacking, the victim is completely unaware that they are being used by the attacker.
- **Denial of service (DoS) attacks:** These attacks overload the company’s infrastructure with a large volume of traffic, preventing its normal function. An attack involving multiple attacking devices is known as a **distributed denial-of-service (DDoS)** attack. The most common techniques employed are: (a) *HTTP flood DDoS*, where the attacker uses HTTP requests that appear legitimate to overwhelm an application or web server; (b) *SYN flood DDoS* where the attacker floods the SME with SYN-ACK challenges – acknowledgements; (c) *UDP flood DDoS* where the victim host is flooded with User Datagram Protocol (UDP) packets sent to random ports; (d) *ICMP flood* where a barrage of ICMP Echo Request packets overwhelms the victim host(s), consuming both inbound and outgoing bandwidth, and (e) *NTP amplification*, which exploits the Network Time Protocol.
- **Injection attacks:** These common attacks exploit security vulnerabilities to directly insert malicious code into a system (usually an Internet-facing web application). Successful attacks may expose data, execute a DoS attack or compromise entire systems. The most common attack vectors include:
  - *SQL injection*, where an attacker enters SQL code into an end user input channel, e.g., a web form field or comment field.
  - *Code injection*, where an attacker directly injects code into an application if it is vulnerable (e.g., does not check for user input, sanity, etc). The web server then executes the malicious code as if it were part of the application.

- *OS command injection*, where an attacker exploits a vulnerability to input commands for the operating system to execute. This severe attack can exploit information at the OS level or completely take over the system.
  - *LDAP injection*, where the attacker tries to alter Lightweight Directory Access Protocol (LDAP) queries; also, very severe, since LDAP servers can store user accounts and credentials for an entire organization.
  - *Cross-Site Scripting (XSS)*, where an attacker injects malicious JavaScript. The end user (web app visitor)'s browser then executes the code, enabling the attacker to redirect the victims to a malicious website or steal session cookies to hijack sessions.
- **Man-in-the-middle attacks:** These attacks which can be diverse and complex in their nature, involves eavesdropping and/or altering the data exchange between two systems or users, e.g., between a user and a web app. The attackers can listen in on the communication, expose personal data, and even impersonate each party participating in the communication. Examples of such attacks include:
  - *Wi-Fi eavesdropping*, where an attacker poses as a legitimate actor, such as a Wi-Fi hotspot where end users will connect. The attacker then monitors the activity of connected users and intercepts critical data such as payment card details and login credentials.
  - *Email hijacking*, where an attacker impersonates (spoofs) the email address of a legitimate organization, such as a bank, and tricks users into giving up sensitive information or transferring money to the attacker.
  - *DNS spoofing*, where the attackers impersonate a DNS server, directing a user to a malicious website posing as legitimate. They may then divert traffic from the legitimate site or steal credentials.
  - *IP spoofing*, where an attacker impersonates an IP address to pose as a website and deceive users into thinking they are interacting with that website.
  - *HTTPS spoofing*, where various HTTPS impersonation techniques are leveraged to deceive the browser into thinking that a malicious website is safe (e.g., “HTTPS” or the lock seal employed in the URL to conceal the malicious nature of the website).
- **Supply chain attacks:** These are sophisticated and severe cyberattacks, where the attackers target software vendors or IT services companies, aiming to infect their customers, often with ransomware (e.g., by “slipping” malware into the “supply chain” of software updates which the IT company installs on its customers’ computers). SMEs may have additional reasons to worry take measures, since a rising trend is observed by supply-chain cybercriminals moving on from large organisations and public infrastructure and seeking to extract ransom from smaller businesses might otherwise not appear as promising extortion targets.
- **Physical attacks:** A potential physical attack to a specific sensitive location of the SME infrastructure or other physical assets of the SME is always a threat.

## 2.4 Cybersecurity in the Cloud

European SMEs are migrating operations to the Cloud, in dramatically increasing numbers. This is due to a number of reasons.

On the one hand, there are significant financial benefits to be gained, both for infrastructure and for software & services. Relocating IT operations from an on-premises model to the Cloud translates into a direct shift of IT costs from *capital* to *operational* expenses. In this model, cash flow-conscious SMEs only stand to benefit from both smaller upfront investments and from the financial certainty which comes with subscription models with recurring billing.

On the other hand, SMEs now stand to benefit from simplified scalability, a previously unattainable feature. Instead of buying and installing new on-premises servers, storage and infrastructure, as the SME scales, it can just pay for Cloud resources and services at just the right amount required and release them if/when they are no longer necessary, which both eases the burden of having to predict growth and prevents overprovisioning. For seasonal businesses with resource needs that change throughout the year, this kind of simple provisioning can be extremely valuable.

However, this does not imply that the Cloud only has benefits in store for SMEs. Adopting Cloud (e.g., SaaS) solutions, from simple invoicing software to a complete e-commerce suite, or even building new ones in the Cloud, can be a complex process. SMEs have to make informed choices related to required services and deployment models as well as adjust their operational procedures into a unified Cloud scheme, supported by a risk-based CS approach for protecting personal data, based on their individual requirements. In doing so, it is especially important for SME management to have a clear understanding of the associated critical areas with respect to the CS and personal data protection associated with the Cloud.

### 2.4.1 Cloud focus areas

The Cloud Security Alliance recommends 13 Cloud Computing **critical areas** (Cloud Security Alliance (CSA), 2017) related to security and privacy. These are focused on both **governance** (strategic and policy) and **operations** (architecture, tactical security and implementation) issues from both the provider and end-user perspectives. The following subsections present these critical areas, which address both the strategic and tactical Cloud security issues and can be applied to any combination of cloud service and deployment model.

We use the CSA guidance as a source throughout this section but have selected and adapted the recommendations to better fit SMEs' strategic and operational requirements.

## GOVERNANCE

### 2.4.1.1 Governance and Enterprise Risk Management

Governance is related to the organization and entails the control and supervision over the operational and procedural activities of the cloud services. Cloud migration requires examining policies and legal issues extensively with the new type of dependencies and business models. Threats relating to agreement breaches, cloud providers transparency, sensitive data protection need adequate attention. SMEs should have the ability to govern and measure the enterprise risks considering the strategic and operational activities.



#### *2.4.1.2 Legal Issues: Contracts and Electronic Discovery*

Cloud architectures can pose complex legal challenges which SMEs may find quite resource-intensive to address. Both providers and end users need to comply with a) existing regulatory requirements and b) Service Level Agreements (SLAs) between user and Cloud provider. Such issues may concern **SLA/contractual obligations, CS policies, security/data breach disclosure laws, regulatory requirements, privacy requirements, international laws**, etc. It's noteworthy that before the SME migrates or launches critical business processes into the Cloud, it should perform basic due diligence by evaluating its existing practice, organizational needs, and constraints to identify requirements. Periodic monitoring, testing and evaluating of Cloud assets are also necessary. Finally, the area considers the **electronic document identification**, which is critical for **data retention, record keeping** and audits.

#### *2.4.1.3 Compliance and Audit Management*

SMEs should obtain -and maintain- compliance when leveraging the Cloud. This can prove challenging due to the interdependent and overlapping prescriptions of internal security and other policies and external regulatory, legislative and other compliance requirements. Due to the fact that Cloud providers are usually servicing their clients at a global scale and in a decentralised, distributed and virtual manner, the largest challenge can be **delivering, measuring, and communicating compliance requirements across different jurisdictions**. This focus area therefore provides guidance on becoming compliant and proving compliance during audits.

#### *2.4.1.4 Information Governance*

Data, the key asset in every SME operation, is central in Cloud computing. SME end users process (e.g., store, read, edit etc) data in the Cloud. However, the CS responsibility this data, as well as the supporting infrastructure, platforms and applications, are usually not managed by the SME (e.g., in the SaaS model) or the Cloud infrastructure provider, but by the SaaS app provider. Of course, these coincide in the cases of file sharing services such as Dropbox or Microsoft OneDrive. This prioritises the need for **identification, control, governance and protection of data** in the Cloud. In any case, information governance should at all times guarantee that the information which the SME stores in the Cloud and uses, is aligned with its organizational policies, standards and overall strategies, including regulatory, contractual, and business objectives. The most prominent aspects and requirements to be tackled here are: (a) multitenancy (the SME's data being collocated at the same infrastructure as other organisations which are not necessarily trusted); and (b) defining how the security responsibility should be shared, e.g., by defining data ownership and custodianship and by addressing the jurisdictional, compliance and other issues associated with the CSPs. This focus area also covers assigning responsibility for the generic CS and personal data protection requirements within the SME, such as data confidentiality, integrity, and availability.

### **OPERATIONS**

#### *2.4.1.5 Management Plane and Business Continuity*

The Cloud's dynamic configuration potential can bring previously-unattainable scalability to SMEs. It does that by providing virtualisation and centralisation for the administrative management of IT resources, such as computation, storage, networking, and even databases, configurations and applications. However, "with great power comes great responsibility"; from a

CS standpoint, a centralised Cloud administration console (also referred to as the **management plane**) consolidates these assets and makes them publicly accessible with just a set of authentication credentials, thus severely impacting how we need to evaluate and manage security compared to traditional models. This focus area provides recommendations on who is responsible for what when managing Cloud assets. Overall, (a) the provider is responsible for ensuring the management plane's integrity and availability while exposing the necessary access control and security features are exposed to the end user (e.g., granular access control), while (b) the end user is responsible for properly configuring the management plane, as well as for securing and managing their access credentials. The same is true for the other focus of this area: **business continuity and disaster recovery**. This area also brings some shared management responsibility for security, where the provider has to manage their part of the infrastructure, but the Cloud customer is also ultimately responsible for how they use and manage their service. This is especially true when planning for outages. Such disaster planning can be manifested as "Business Continuity Within the Cloud Provider", "Business Continuity for Loss of the Cloud Provider" and "Business Continuity for the Private Cloud".

#### *2.4.1.6 Infrastructure Security*

This critical area deals with traditional **Cloud infrastructure** CS concerns such as networking, workload security, hybrid cloud considerations and some security fundamentals for private clouds. It provides guidance encompassing a wide range, from the physical layer of the stack, through to end users' configuration and implementation of infrastructure components. It specifically addresses CS configurations not for the physical infrastructure (which is managed by the provider) but for the virtual/abstracted infrastructure managed by the SME engineers, e.g., the compute, network, and storage assets which they use from the Cloud resource pools to build and run their virtualised infrastructure or apps.

#### *2.4.1.7 Virtualization and Containers*

Virtualization is the core technology used to convert and effectively "subdivide" physical infrastructure into the pooled resources on which the Cloud is fundamentally based. It does this by enabling the **abstraction** required for resource pools, which are then managed using orchestration. Virtualization severely impacts many security aspects and is fundamental to implementing Cloud security. Cloud assets provisioned from a pool of virtual resources may appear similar to the physical assets they replace (e.g., when remotely logging on to a virtual server), but in reality, virtual assets work differently from the physical resources from which they are abstracted. This focus area deals with **virtualisation-specific security concerns, measures and responsibilities**. These can be identified as: (a) compute virtualisation, including containers; (b) network virtualisation, including SDN, and (c) storage virtualisation.

#### *2.4.1.8 Incident Response, Notification and Remediation*

Incident response (IR) is a critical component of any secure system and Cloud setups are no exception. We know that there is no system can be configured to be 100% secure and breaches are bound to happen. Therefore, Cloud setups should provide an effective means for incident handling. This domain seeks to address the **incident response-related issues** specifically related to Cloud setups, that should be in place at both the provider and end user levels to enable proper handling and forensics of potential security or data breaches. In more detail, it studies the incident response lifecycle suggesting Cloud-focused best practices at each phase, from



preparation, to detection & analysis, to containment, eradication & recovery, to post-mortem. It should be noted that SLAs play a special role in IR, since any incident using a public cloud or hosted provider would require both an understanding of the relevant SLAs by the SME as well as close coordination with the cloud provider.

#### *2.4.1.9 Application Security*

This focus domain is primarily addressed to software development and IT teams, designing and deploying applications in the Cloud (and specifically in Platform- and Infrastructure-as-a-Service models), and deals with **security issues pertaining to the lifecycles of software applications designed for, and deployed in, specifically in Cloud environments**. Application security has always been a very broad and complex domain, ranging from the early design and threat modelling, to maintaining and securing production applications. The external and internal threats that an application is going to be exposed to in the Cloud are more in number and severity, compared to applications traditionally deployed on-premises. Cloud deployments present significant opportunities such as (a) a higher baseline security; (b) responsiveness via APIs and automation; (c) isolated environments and application stacks; (d) independent VMs enabling microservice architectures; (e) elasticity, e.g., automatic provisioning and deprovisioning or resources using auto-scale groups; (f) potential for DevOps methodologies, enabling CI/CD pipelines; and (g) a unified management interface. These are balanced by a number of challenges; namely: (a) limited visibility, e.g., into monitoring and logging data; (b) Increased application scope, with infrastructure configurations directly affecting deployed apps, as well as the potential for creating unnecessarily super-privileged users, such as developer or operations accounts with access to the management plane – a major threat for data breaches; (c) evolving threat models, and (d) reduced transparency, especially in integration with external services. This area recommends a series of security activities during all phases of application development, deployment, and operations in the Cloud, including **Secure Design and Development, Secure Deployment, Secure Operations, Cloud-specific designs, DevOps**, and many more.

#### *2.4.1.10 Data Security and Encryption*

Data security and encryption is a crucial domain for SMEs for building customer trust and, eventually, for growth. Companies should be trained and equipped to identify personal data at rest or in transit which need additional protection and controls. This identification usually takes places with information audits. Personal data and information stored in the Cloud which is identified as highly sensitive, encryption at the storage or database level can be considered, and safeguarded with robust access control. The CSA recommends, for this focus area, that security controls applied to data stored in the Cloud should be **risk based** (an approach also adopted by ENISA), so it can be more efficient and cost-effective for SMEs while, at the same time, allowing them to securely entrust more data to third parties (Cloud providers). Going into additional details, the recommendations deal with (a) controlling what data goes (and where) in the Cloud; (b) managing and protecting data in the Cloud (access control, encryption, architecture, monitoring/logging/alerting, etc) and (c) adopting and enforcing an information lifecycle management security policy (e.g., managing data location/residency across jurisdictions, ensuring compliance, backups and continuity etc). Additional issues addressed by the domain, and related to encryption are: volume storage encryption, object storage encryption, application- and database-layer encryption, as well as higher-layer encryption by the provider as is sometimes the case in SaaS models. Key management, another very key consideration, deals with who

manages and stores encryption and access keys, and where. For example, Cloud-provided key management services tend to be the most convenient but least secure option, and users who adopt it need to understand in depth the SLA and security model offered by the provider before making the choice.

#### *2.4.1.11 Identity, Entitlement and Access Management*

End-users in the Cloud need to establish a trust relationship with the provide in order to be able to manage IAM. This required a great deal of managing responsibilities and roles as well as complex technical implementations to effectively manage, especially in the case where a company needs centrally managed IAM for several cloud providers or implementations, which is usually address with federated IAM. This focus domain addresses **IAM between the provider and the end user** in the broader domains of authentication, authorisation and access control within this relationship; for example, how end-users (e.g., application developers or DevOps engineers) would be able to securely access the SME's Cloud resources in order to do their work. Compared to traditional on-premises deployment models, identity and access management (IAM) in the Cloud adds the notion of entitlement. This can be seen as the “permissions” (assigned to specific persons, roles, etc) system that make the granular control of access possible. Cloud providers support different IAM standards, such as SAML, OAuth and OpenID, aiming to support centralised identity provision and management as well as single sign-on (SSO), using secure authentication (including MFA) while mapping entitlements and handling the entire process of defining, propagating, and enforcing authorizations.

#### *2.4.1.12 Security-as-a-Service*

Most of CSA's guidance reflects on secure infrastructure, software or services implementations *for* the Cloud. However, this area examines paradigms of security services delivered *from* the Cloud. These services, usually delivered in a SaaS model, can be used to defend Cloud or other IT assets and can be a very attractive proposition for SMEs, offering very targeted CS value at a cost level they can control. Examples could range from single-purpose Cloud SaaS services offering monitoring and alerting for IT infrastructure with continuous real-time metrics, visualizations, health alarms etc. to complete security, privacy and compliance stacks delivered from the Cloud. Security-as-a-Service (commonly abbreviated as **SecaaS**) offerings may be categorised as: (a) Identity, Entitlement, and Access Management solutions; (b) Cloud Access, Security Brokers and Cloud Security Gateways; (c) Web Security, e.g., web ACLs and security enforcements for web apps; (d) Email Security; (e) Security Assessment, e.g., vulnerability scanners, static and dynamic application security testers, cloud provider security assessment tools, etc; (f) Web application firewalls; (g) Intrusion detection/prevention systems; (h) Security Information & Event Management; (i) Encryption and Key Management solutions; (j) Business Continuity and Disaster Recovery, e.g., Cloud backup and archival solutions; (k) Security Management, e.g., solutions offering integrated endpoint protection, agent management, network security, mobile device management etc, and (l) DDoS protection offerings, which are, by nature, Cloud-based.

#### *2.4.1.13 Cloud related technologies*

Instead of dealing with recommendations for directly securing Cloud assets, the last critical focus area examines recommendations for other key technologies which are interrelated and interact with the Cloud. These technologies may either rely exclusively on Cloud computing to deploy and

operate (such as SDN) or may not require Cloud, but are commonly encountered in Cloud deployments. The specific areas covered are (a) **Big Data**. In this domain, the Cloud is commonly leveraged in IaaS or PaaS, due to its elasticity and massive storage capabilities. The Cloud specifically simplifies Big Data's distributed data collection, storage and processing requirements; (b) the **Internet of Things**, where many IoT apps, sensors, devices etc connect to the Cloud for back-end processing and storage. Key Cloud IoT *security* considerations include data collection and sanitisation, device registration, authentication, and authorization, API security, communications encryption and the security patching/updating of software and devices; (c) **Mobile devices**. Mobile apps, similar to IoT, connect to the Cloud for back-end processing and storage but are more prone to security issues due to the fact that smartphones, contrary, to most IoT devices, are also general-purpose computers and can be compromised in more ways to do more malicious activities. Mobile developers should examine device registration, authentication, and authorization, as well as mobile app APIs for security weaknesses. The final area is (d) **Serverless computing**, which can be loosely defined as the use of PaaS and SaaS cloud offerings to such a degree that all or some application stacks run in the Cloud, without customer-managed operating systems, or even containers. In this context, the end-user (e.g., the SME software engineer) only manages *settings* for the services, not the underlying hardware and software stacks. Examples include object storage, Cloud load balancers, Cloud databases (DBaaS), machine learning, message queues, notification services, Cloud code execution environments (restricted containers where a consumer runs application code), API gateways and, of course, web servers. These serverless setups place the security burden on the Cloud, so SMEs should pick their provider carefully and understand how the security SLAs and related capabilities would affect them and their processed personal data.

## 2.4.2 Cloud threats

CSA's Top Threats Working Group, in their 2019 instalment of the "egregious eleven" report (Cloud Security Alliance (CSA), 2019), have updated their identification and description of the salient threats, challenges, risk and vulnerabilities of assets residing in the Cloud. SMEs, and especially management, stand to benefit from studying them, in their efforts to raise CS awareness and reinforce the protection of personal data.

### 2.4.2.1 Data breaches

A data breach is a CS (and privacy) incident where personal and/or confidential information is compromised by an unauthorised party. Data breaches occur increasingly often and can be the result of many of the threats detailed in Section 2.3.2 of this report. In fact, they are less often the result of malicious external hacking than of negligent actors, such as SME staff misconfiguring access (or granted unnecessarily privileged access) or even inadvertently sending data to the wrong recipient. Sometimes, data breaches can remain undetected for months but their business impact always tends to be very severe, including, but not limited to (a) violation of the data subjects' fundamental rights; (b) impact to the SME's reputation and customers trust; (c) misappropriation of intellectual property, e.g., by competitors; (d) regulatory implications that may result in fines, sanctions etc; (e) non-monetary legal and contractual liabilities and, of course (f) incurred expenses for incident response and forensics.

#### *2.4.2.2 Misconfiguration and inadequate change control*

Misconfiguration of cloud resources, aside from a leading cause of data breaches, can severely impact the SME by violating basic integrity and confidentiality requirements, thus allowing for the deletion or modification of Cloud resources, information leakage and/or service interruption. Common examples of this security issue would include (a) incorrectly configured data storage elements or containers; (b) excessive permissions; (c) default credentials and configuration settings left unchanged and (d) standard security controls being disabled. The most common cause for such misconfiguration is the lack of appropriate change control. In order to support rapid change, the Cloud requires automation, and the expansion of roles and access within the SME. Management (both within IT and top-level) should be able to utilise Cloud dashboards to audit (a) what changed; (b) whether compliance requirements are met and (c) support their decisions with key Cloud metrics. The impact of Cloud misconfigurations can be severe, depending on their nature and how quickly they are discovered/handled. The most commonly reported aftereffect is data breaches in cloud repositories.

#### *2.4.2.3 Lack of Cloud security architecture*

SMEs have shifted enthusiastically towards adopting the Cloud. However, for reasons we have already mentioned, SMEs either often lack the drive and/or resources for truly secure Cloud architectures and implementations or adopt SaaS-delivered apps without understanding in depth the implications of shared security responsibility (among SME and provider) during the processing of personal data. Unfortunately, this risk remains high as SMEs tend to migrate to the Cloud adopting a “lift-and-shift” approach, directly porting existing IT stacks and configurations, often as-fast-as-possible, thus exposing sensitive information to a plethora of threats. We believe that adopting a robust Cloud security strategy will provide SMEs with a strong foundation to do business, going forward. Additionally, leveraging cloud-native tools, such as SecaaS offerings, to increase protections and transparency will also minimize risk and cost.

#### *2.4.2.4 Insufficient identity, credential, access and key management*

The far-reaching impact of IAM is explored by the relevant critical focus area in Section 2.4.1.11. The Cloud introduces new challenges in the already complex environment of IAM and both providers and end users need to understand implications and manage it without compromising security and privacy. To name a few causes, IAM-related CS events and privacy breaches in an SME may occur due to: (a) insecure credentials; (b) lack, or negligent implementation of policy mandating the regular and automated rotation of cryptographic keys, passwords and certificates; (c) storing sensitive credentials or cryptographic keys in public repositories; (d) inability of present identity, credential and access management systems to scale; (e) lack of multifactor authentication (MFA)-authenticated access control for sensitive personal data, and, of course, (f) insufficient, or laxly enforced, password policy.

#### *2.4.2.5 Account hijacking*

Account hijacking occurs when a malicious actor, internal or external, gains control of a user account which either has high or administrative-level permissions (i.e. allowing the attacker to compromise critical SME assets) or is sensitive in nature (i.e. allowing the attacker to impersonate the victim). Such accounts may even include cloud service accounts or subscriptions, which often provide complete administrative control over the company’s Cloud assets. Such attacks often

employ phishing, exploitation Cloud vulnerabilities, or directly stealing credentials, and, needless to say, can cause very severe disruption to SME operations as well as infringement of fundamental rights in the case of privacy breaches. Fallout from hijacking can be extremely severe; in recent cases, there have been significant operational and business disruptions, including purging organizational assets, data and capabilities. SMEs should promote cyber awareness of such threats and consider strategies to contain breach damage stemming from the compromise of sensitive or privileged user or system accounts in the Cloud.

#### *2.4.2.6 Insider threats*

Insider threats are explored in detail, including their subtypes in Section 2.3.2.1. However, CSA identifies attributes and specific facets of these threats that are either influenced or exacerbated by Cloud architectures and deployment models. The most common Cloud scenarios reference (a) misconfigured cloud servers, virtual networks, storage objects etc, (b) SME staff storing sensitive Cloud data on personal devices and systems and (c) employees or other insiders (staff or contractors) falling prey to phishing emails or social engineering leading up to malicious attacks. Malicious or negligent insiders can be an even more dangerous threat due to the existence of privileged accounts which include “root” cloud service and management plane accounts which can provide complete administrative control over the company’s Cloud assets.

#### *2.4.2.7 Insecure Interfaces and APIs*

Cloud service providers (CSPs) make a variety of software interfaces and APIs available to end users in order for the cloud services to be efficiently managed and applications delivered. Several actions like, management, provisioning, orchestration and monitoring are carried out through these APIs. Vulnerabilities and security breaches in the Cloud are all too often attributed to improperly designed, unprotected, broken, exposed or hacked APIs. SMEs either integrating with -and managing- Cloud assets over APIs, or offering their products and services through apps delivered to end users over APIs should study the security requirements of implementing and exposing these interfaces and adapt.

#### *2.4.2.8 Weak management plane*

A weak management plane (also referred to as the Cloud control plane) is the situation when a CSP does not offer adequate or sufficient security options (e.g., in the cloud management console) for Cloud assets to meet the end user (e.g., SME)’s security requirements. An example of a weak management plane is the lack of providing an MFA or 2FA authentication option for accessing assets along with the capabilities to enforce it. Unfortunately, similar to other Cloud threats, a weak control plane is something which SMEs’ IT security staff might notice only after they have migrated to the cloud. The SME will not be fully in control of the security configuration, the relevant data flows and where architectural weak points might manifest; eventually leading up to a potential breach, unavailability, or similar. Potential CSP should always be thoroughly researched by prospecting SMEs for the Cloud, to provide as full a set of security controls as possible so companies can fulfil both their internal (e.g., security and personal data protection policy) and their legal / statutory obligations.

#### *2.4.2.9 Metastructure and applistructure failures*

A newly introduced top threat “metastructure and applistructure failures” (Cloud Security Alliance (CSA), 2021) refers to failures at the edge of the responsibility area between Cloud provider and



user. A basic understanding of the logical models and how they are described, especially by the CSA, is necessary for differentiating the security responsibility demarcation points between CSPs and the SME. For example, in the infrastructure-as-a-service (IaaS) delivery model, both the provider and the end user share responsibility. The former is responsible for the physical and logical infrastructure on which the Cloud offering is built, while the user is responsible for the purely virtual infrastructure which they abstract.

In this logical model, the ‘metastructure’ is a differentiating Cloud characteristic, described by CSA as “the protocols and mechanisms which provide the interface between the infrastructure layer and the other layers. The glue that ties the technologies and enables management and configuration.”

Examples of failures at this level include a poor API implementation by the CSP, offering attackers an opportunity to disrupt the confidentiality, integrity, or availability of the SME’s Cloud assets.

Above this demarcation, e.g., in the ‘applistructure’, it is increasingly end users who have the responsibility of understanding in depth how to properly implement secure cloud applications. For example, applications that are not designed for cloud environments will not be able to fully leverage cloud resources and capabilities. In this respect, CSPs should conduct transparent penetration testing for ‘metastructure’ flaws, and provide findings to customers, while SME end users should implement appropriate features and controls in cloud-native app designs.

#### *2.4.2.10 Limited cloud usage visibility*

This is also a newcomer in the list as defined in (Cloud Security Alliance (CSA), 2019), and it is manifested as threat when an organisation is unable to efficiently determine (by visualisation and analytics) whether the utilisation of their Cloud resources is safe or malicious. According to the CSA, this can be divided into two key challenges: (a) Unsanctioned app use: This occurs when SME staff are utilising cloud resources without explicit permission (e.g., from IT), which can result in a self-support model called ‘Shadow IT’. When cloud resource utilisation does not meet company security policy, this tactic is very risky, especially when associated with processing personal data. (b) Sanctioned app misuse: Analysis and in-depth understanding of how approved applications are being used can be quite a challenge. Often, these apps, although sanctioned, are used in nefarious ways by insiders, or by external malicious actors who target the app/service using credential theft, SQL injection, DNS attacks etc. CSA recommends a series of activities and guidance to mitigate this risk.

#### *2.4.2.11 Abuse and nefarious use of cloud computing*

An unpleasantly common threat is when attackers hijack, or spin their own, Cloud resources in order host malware or perform a series of other malicious activities, including, but not limited to, (a) DDoS attacks, (b) phishing and email spamming, (c) mining cryptocurrencies leveraging the SME’s computing resources, (d) large-scale and distributed click fraud (e.g., by serving / clicking on digital ads), (e) brute-forcing stolen credential databases or other locked/encrypted sensitive material leveraging the SME’s Cloud computing resources, (f) hosting illegal/pirated content, e.g., copyrighted content or software etc. One way to detect such abuses are by looking for anomalies in billing, since provisioning the necessary resources will incur additional charges from the CSP. Providers should also provide a complete incident reporting and handling framework for SMEs to

report resources abuse. On the other hand, SME IT departments should implement or rent security controls to monitor assets, API calls and anomalous Cloud resource usage.

### 2.4.3 Matching Cloud concepts and architectures with threats

An appropriate association between the top threats identified in the previous subsection and the associated Cloud concepts, models and architectures are deemed necessary before security and privacy controls can be designed to efficiently address them. This section attempts to provide this visual linking, also considering the identified critical focus areas of Section 2.4.1.

In Table 1 below, we present a visual association between each threat and the respective a) security responsibility (sharing model); (b) Cloud logical model architecture; (c) Cloud service delivery model; (d) related CSA critical focus areas and (e) threat categories (Microsoft, 2005).

Table 1. Matching threats with Cloud concepts and architectures

Threat (Cloud Security Alliance (CSA), 2019)	Responsibility	Architecture	Service models	Areas	Categories
1. Data breaches	Both	All	All	GERM LICED CAM IG MPBC IR DSE IEAM RCT	Information Disclosure
2. Misconfiguration and inadequate change control	User	All	All	CAM IG MPBC IS VC AS DSE IEAM	Tampering with Data Repudiation Information Disclosure Denial of Service
3. Lack of Cloud security architecture	User	Infra	PaaS, IaaS	CCA MPBC IS	All
4. Insufficient identity, credential, access and key management	User	Infra	PaaS, IaaS	DSE IEAM	All
5. Account hijacking	Both	Appli, Meta	All	GERM MPBC IR IEAM	All
6. Insider threats	User	Infra	All	GERM IG DSE IEAM	Spoofing Identity Tampering with Data Information Disclosure Elevation of Privilege
7. Insecure Interfaces and APIs	Both	Appli, Meta, Infra	All	IG MPBC IR DSE AS IEAM	Tampering with Data Repudiation Information Disclosure Elevation of Privilege
8. Weak management plane	User	Infra	All	CCA IG IS VC IEAM	Tampering with Data Information Disclosure Elevation of Privilege
9. Metastructure and applistructure failures	Both	Appli, Meta	All	CCA GERM CAM IG PBC IS VC IR AS DSE IEAM	All
10. Limited cloud usage visibility	Both	All	All	IG DSE SecaaS	All
11. Abuse and nefarious use of cloud computing	Both	All	All	MPBC IS IR AS	All

Legend (critical areas)	
CCA: Cloud Concepts and Architectures	VC: Virtualization and Containers
GERM: Governance and Enterprise Risk Management;	IR: Incident Response
LICED: Legal Issues, Contracts and Electronic Discovery	AS: Application Security
CAM: Compliance and Audit Management	DSE: Data Security and Encryption
IG: Information Governance	IEAM: Identity Entitlement and Access Management
MPBC: Management Plane and Business Continuity	SecaaS: Security as a Service
IS: Infrastructure Security	RCT: Related Cloud Technologies

This matching is important for two reasons.

- (a) **Reason one:** it enables requirements and model developers to understand what critical areas their work should focus on in order to satisfy the requirements for covering specific threats. To provide an example: when, during SENTINEL's modelling we are developing tools and

methods to satisfy requirements of e.g., the ‘**account hijacking**’ threat, we would need to make sure that:

1. Our work supports, and is supported by, at least CSA's Cloud focus areas of (i) Governance and Enterprise Risk Management; (ii) Management Plane and Business Continuity; (iii) Incident Response and (iv) Identity-Entitlement-Access Management.
2. We clarify that security responsibility is shared among both provider and the SME end user.
3. Our work is focused in the ‘applistructure’ and ‘metastructure’ layer of the Cloud’s logical architecture.
4. Make sure that during self-assessment, we identify the correct gap to be filled during their tailored requirements analysis, when they declare utilisation of all three Cloud service delivery models: Software as a service (SaaS), Platform as a service (PaaS) and Infrastructure as a service (IaaS).

This will be utilised to address SENTINEL’s tailored analyses, which will be derived from SME self-assessment, to be developed in WP2 and WP4.

- (b) **Reason two:** During both security implementations and incident response, it provides software and IT security engineers with a solid understanding and a foundation for threat analysis for specific threats and attack vectors, based on the relevant properties and security policies of the SME assets which they support.

## 2.5 Legal Considerations

This section attempts to provide a concise introduction to data protection law, with an emphasis on the European Union’s Regulation (EU) 2016/679 (GDPR), narrowing down focus, where possible, in the area of small and medium enterprises. It thus aims to provide an all-around and appropriate legal background to the reader so they can better address issues in the domain.

Taking the necessary steps to ensure a data privacy-oriented work ethic is vital for SMEs. Companies should be aware of their duties that have been set out in the GDPR. Compliance with the GDPR does not only protect SMEs from the imposition of high fines, but it can also function as a key influence on the public standing of their brand. In fact, research has shown that businesses who show a significant amount of transparency to consumers are rewarded with a significant amount of customer trust.

### 2.5.1 The concept of personal data

Personal data is any information relating to a specific natural person that can lead to his or her identification. Personal data are, for example, belonging to a group, being prosecuted for an offence, having a certain sexual preference, having a certain political, philosophical or religious belief, and so on. Personal data refer only to living natural persons and not to deceased persons. The deceased are not protected by the data protection legislation, but this does not mean that they are not subject to medical confidentiality. It is simply that the processing of data of deceased persons is not covered by the provisions of the data protection legislation. In principle, legal persons do not have personal data. Exceptionally, legal persons are subject to data protection



legislation when the name of a commercial company refers to the name of the main partner and when an institution or even a commercial enterprise is commonly identified with the person who runs it.

Statistics that do not lead to the identification of a specific natural person do not constitute personal data. For example, a statistical survey does not constitute personal data. But if the statistic can lead to identification, then we have personal data.

Personal data are in principle distinguished from value judgements. Exceptionally, value judgments may also constitute personal data. A typical example is the assessment of service or creditworthiness, which constitutes both a value judgment and personal data.

Personal data can be divided into simple and sensitive (special categories). Most of them are simple. Sensitive data are, exclusively, racial or ethnic origin (e.g., that a person is an ethnic gypsy), political opinions, religious or philosophical beliefs or trade union membership, genetic data, biometric data for the purpose of unambiguous identification of a person (e.g., fingerprints, iris), health, sexual life or sexual orientation. Anything that is not sensitive is simple. The reason we are interested in this distinction is because when we come across sensitive personal data, they need enhanced protection.

## 2.5.2 Basic principles of data processing for SMEs

The processing of personal data must be based on one of the lawful bases for processing set out in Articles 5 and 6 GDPR. These principles are summarised in the principles of **lawfulness** (personal data must be obtained in a lawful and fair manner), **transparency** (the data subject must know whether and which personal data are being held about him or her), **data minimisation** (personal data must be adequate, relevant and no more than is necessary for the purpose justifying their processing, e.g., in the case of school certificates it is not necessary that they indicate the student's religion or in the case of identity cards it is not necessary that they indicate the cardholder's religion), **time limitation** (personal data cannot be kept longer than necessary), **accuracy** (personal data must be accurate and regularly updated), and **integrity** (taking appropriate technical and organisational security measures in order to avoid unauthorised access, changes, leaks of personal data and accidental loss, destruction, damage).

It is noteworthy that GDPR's provisions are horizontal, in the sense that as there are **no exemptions** or "lightweight approaches" based on the organization size, availability of recourses and capabilities. **SMEs are therefore bound by these principles**, and they need to incorporate them in their day-to-day business. For example, all SMEs, similar to larger organisations, need to be clear on the lawful basis of their data processing (principle of lawfulness), they need to provide information notices to their employees and customers (principle of transparency), they need to have a defined retention time for their personal data records (principle of time limitation) etc.

The GDPR does, however, have a few provisions for smaller enterprises, i.e. those with fewer than 250 employees. Therefore, SMEs:

- Are exempt from having to keep records of their processing activities, **unless** the processing of personal data is a regular activity, or in case it poses a potential threat to individuals' rights and freedoms, or includes sensitive personal data or criminal records.

- Are required to appoint a Data Protection Officer **only if** processing is their main business *and* if it poses threats to individuals' rights and freedoms. An example could be monitoring individuals or processing sensitive data or criminal records in particular as it is done on a large scale.
- Are entitled, under GDPR to consider the **cost of implementations** of privacy-by-design architectures and other data security controls as part of assessing the technical and organizational measures which are put in place to offer data protection.
- **DPIAs:** GDPR Article 35 on data protection impact assessment (DPIA) identifies the "scope" and the "context" of processing as areas to consider when determining whether a DPIA is required. As a result of this language, the size of the processing could be one factor in determining whether there is likely a high risk to the rights and freedoms of natural persons. Nevertheless, despite the size of the business, organizations which have any doubt as to whether a DPIA is required should engage in the impact assessment.

## 2.5.3 Innovations of the General Data Protection Regulation

### 2.5.3.1 *Strengthening citizens' rights*

The most important added value of the Regulation lies in the enhancement of citizens' rights. Consequently, the obligations of data controllers are also strengthened. A key feature is the strengthening of citizens' rights. In this context, the GDPR recognises new rights, affirms but also updates and renews existing rights for citizens and embraces new mechanisms for the protection of the rights concerned, by strengthening the obligations of data controllers, establishing a new body, the data protection officer, and imposing severe sanctions in cases of violations.

#### **a. Right to information (principle of transparency)**

The general list of data subject's rights is based on the general principle of transparency in the processing of personal data or, more correctly, on a transparent information policy which aims to facilitate the exercise of rights by the data subject, but also to provide consent. This principle is referred to, firstly, in Article 5(1)(a) of the GDPR and specified in recital 39, according to which any information and communication relating to the processing of the personal data in question must be easily accessible and comprehensible, in clear and plain language, free from misinterpretation.

#### **b. Right to erasure (right to be forgotten)**

The Regulation positively introduces in Article 17 a pre-existing right to erasure, the so-called right to be forgotten. This right is a corollary of the more general freedom to develop one's personality. It is the right of the individual to be able to erase from the internet information that he or she does not want and that is not useful for informing the public. In essence, it is a right to shape the digital presentation, which is created by consulting relevant search engines. The right hitherto established consists in the deletion of results from search engines. An individual right of deletion has also been recognised for online newspaper archives.

#### **c. Right to portability**

The relevant right consists, in accordance with Article 20 of the GDPR, in the possibility for the data subject to obtain personal data concerning him or her which he or she has provided to a

controller in a structured, commonly used and machine-readable interoperable format and to transmit them to another controller, where the processing of personal data is carried out by automated means. Data controllers should be encouraged to develop interoperable formats that allow data portability.

#### **d. Right to human intervention**

In accordance with paragraph 71 of the Preamble and Article 22 of the GDPR, the data subject should have the right not to be subject to a decision which evaluates personal aspects relating to him or her and which produces legal effects concerning that person or significantly affects him or her in a similar way, taken solely on the basis of automated processing, such as the automatic refusal of an online credit application or e-recruitment practices without human intervention.

#### **e. Strengthening child protection**

An important achievement of the Regulation in the field of rights is the strengthening of the protection of children in the new environment of technological risk. The added value of the Regulation in the area of child protection consists in the requirement in Article 8 to obtain the consent of the holder of parental responsibility for the processing of personal data of children up to the age of sixteen. The Regulation leaves Member States the possibility to provide by law for a lower age, but not lower than thirteen years. For example, the Greek legislator has chosen the age of fifteen. What is noteworthy is the recognition of the responsibility for obtaining consent from the parental authority to the controller, who must make reasonable efforts to verify that consent is given or approved by the person having parental responsibility for the child, considering the available technology.

The idea of protecting childhood is also reflected in the case law of the ECtHR (*Marper v. United Kingdom*). According to the Court, the retention of data of un-convicted persons could be particularly harmful in the case of minors, given their particular situation and the importance of their development and integration into society. The Court considers that particular attention should be paid to the protection of minors from any harm that might result from the retention by the authorities of their personal data after they have been acquitted of a criminal offence.

SMEs need to be aware of the rights of the data subjects and to have policies that enable them to fulfil these rights in accordance with the GDPR provisions.

##### *2.5.3.2 Enhanced obligations towards the controller*

The enhancement of citizens' rights is achieved by imposing enhanced obligations on data controllers. The enhanced liability of the controller is an innovation of the Regulation, as Article 23(2)(a) of the Regulation exempts him/her if he/she proves that he/she is not liable (Article 23 Law 2472/97), while the Regulation requires the controller to implement appropriate technical and organisational measures (TOMs) to ensure and be able to demonstrate that the processing is carried out in accordance with the Regulation [Article 24§1].

The obligations of the controller are summarised below:

- a. Appropriate **technical and organisational measures**: The controller must implement appropriate technical and organisational measures to ensure and be able to demonstrate that processing is carried out in accordance with the Regulation.

- b. The controller must **by design and by default** establish an appropriate structure (privacy by design) and procedures to meet the requirements of the Regulation.
- c. **Obligation to inform** the supervisory authority and the data subject: the controllers must inform the supervisory authority and the data subject without delay once they have been informed of the data breach. Any complaint of a breach shall also constitute notification of the breach.
- d. Preparation of an **impact assessment**: the controller must prepare an impact assessment for processing of data presenting a high risk and relating to the assessment of personal aspects, large-scale data or public area monitoring (DPIA).
- e. Establish a **security policy** and codes of conduct: The controller must establish data security policies and codes of conduct.
- f. **Keeping activity records**: the controller and processor shall keep a written or electronic record of their processing activities where the undertaking or organisation employs more than 250 persons, the processing poses risks to data, is not occasional or involves special categories of data. That record shall be made available to the supervisory authority at its request for the exercise of its powers.
- g. Appointment of a data protection officer. In case of large-scale data processing, the controller is required to appoint a **Data protection Officer (DPO)**.

It is important to note that the *application of the data protection regulation and the obligations this provides for controllers does not ultimately depend on the size of a company, but on the type and nature of its activities*. Activities that present high risks for the individuals' rights and freedoms, whether they are carried out by an SME or by a large company, trigger the application of more stringent rules. However, some of the obligations of the GDPR may not apply to all SMEs. For instance, as stated above, companies with *less than 250 employees don't need to keep records* of their processing activities unless processing of personal data is a regular activity, poses a threat to individuals' rights and freedoms, or concerns sensitive data or criminal records. Similarly, SMEs will only have to appoint a *DPO* if they undertake large scale processing of personal data and it poses specific threats to the individuals' rights and freedoms (such as monitoring of individuals or processing of sensitive data or criminal records).

#### 2.5.3.3 Accountability principle

A key innovation of the Regulation is the adoption of the **accountability principle**. This means that the controllers (i.e., the person who determines for what purpose the data are processed) must demonstrate that they have taken the necessary technical and organisational measures to protect the data. Under the former regime of the Directive and Law No. 2472/1997, the conduct of scientific research with sensitive data required authorisation from the Hellenic DPA. Under the current regime, this authorisation has been replaced by an obligation for the researcher to ensure technical and organisational security measures in a quasi-self-regulatory regime. This is always in conjunction with the need to carry out an impact assessment study on the rights of the citizen in the case of high-risk processing, which is provided for in Articles 35 et seq. GDPR.

The accountability principle applies to all controllers, including SMEs. This means that the SMEs need to make provisions for their GDPR compliance documentation.

#### 2.5.3.4 Extraterritorial application

According to Article 3 of the GDPR, the scope of the Regulation extends to the activities of an establishment of a controller or processor that takes place within the EU, but also to the activities of an establishment of a controller or processor outside the EU when the processing concerns data subjects located in the EU (e.g., in cases of e-commerce and profiling). In accordance with Article 3(3), the GDPR applies to the activities of an establishment of a controller or processor within the EU, i.e., the criterion of the place of establishment of the controller is adopted in order to determine the scope of the Regulation. The CJEU has given a broader interpretation to the concept of establishment, moving away from a purely formalistic approach. Para. 2 of Article 3 extends the scope of the GDPR to activities of a controller or processor with an establishment outside the EU, where processing of data of subjects located in the EU is carried out which relates to (a) provision of services or goods to subjects, independently of whether a payment is requested (e.g., in cases of e-commerce) (b) The monitoring of the behaviour of data subjects within the EU.

The extraterritorial application of the GDPR is not in any way associated with the size of an organization. It affects all controllers, including SMEs which are not established in the EU as long as their goods/services are addressed to EU citizens.

## 2.6 Summary: Generic and technical requirements

In Section 2 we studied the CS challenges faced by SMEs today, in their quest towards protecting personal data. We presented several organisational challenges and barriers to adoption; we mentioned the generic and high-level security requirements (such as the all-permeating CIA triad) and identified the major threats to CS and privacy which SMEs face in their operating environment, both internal and external. We also dedicated a subsection to the challenges introduced by the adoption of the Cloud, as well as the threats which arise and the critical focus areas in the domain. Lastly, we did an overview of the legal landscape for protecting personal data, focusing on the basic principles and requirements of the GDPR, including special provisions and exemptions for SMEs.

From this environment of challenges, threats and CS needs, we are distilling the major generic and specific requirements, which we present in a concise manner, in the form of simple grouped terms, in the table below. Table 2 will be used, (in conjunction with the Cloud threat mapping presented in Section 2.4.3) for associating SENTINEL components with system requirements and for informing the ontology for the overall RE methodology.

*Table 2. Generic and technical requirements for cybersecurity and personal data protection*

CIA triad	PDP & compliance	PETs
Confidentiality	Data collection & flow mapping	Encryption
Integrity	Record keeping & audit management	Anonymisation
Availability	Data sovereignty & portability	Pseudonymisation
<b>CS generic</b>	DPIA	Obfuscation
Policy drafting	Data transfers, vendor & 3 <sup>rd</sup> party management	Data minimisation
Policy enforcing	DPO management	Disclosure control
Non-repudiation	Notices, consent management	Access control

AAA – Authentication, Authorisation, Accounting	Compliance & accountability	Differential privacy
Incident reporting & handling	<b>CS technical</b>	
Cyber awareness	Endpoint security - computers	Cloud security (SecaaS)
Education & training	Endpoint security – mobile	SW lifecycle security
Unlinkability	Pentesting & vuln.assessment	Monitoring - alerting
Unobservability	Email security	Logging
Self-assessment	Network security	Analytics, visualisation
Business continuity	IAM (identity/access mgmt.)	Forensics

In Appendix IV, we attempt a more detailed expansion of both functional and non-functional high-level requirements of Table 2.

## 3 Cybersecurity for privacy: Managing risk

### 3.1 Introduction

SMEs dominate the European business landscape and constitute the backbone of the EU economy, promoting competitiveness and investments of the Digital Single Market (European Commission, 2021)<sup>1</sup>.

SMEs, always looking for the best value in delivering their products and services, are increasingly depending on distributed and Cloud IT assets, while many have an online presence integrated with complete e-commerce solutions for selling products or services online. However, as it has been sufficiently demonstrated in Section 2, these assets, along with traditional on-premises IT assets, information and infrastructure, are subject to a wide range of threats against which it is not easy for an SME to dedicate the resources and effort required to establish a robust CS policy and defences. The risk level (based on severity) of these threats increases proportionally to the nature of the informational assets at stake. In the case of sensitive and personally identifiable data or information this risk is usually high or very high.

This risk, combined with the high volume of data which European SMEs process, calls for a broader raising of awareness towards the EU (GDPR)<sup>2</sup>, which defines such data in the way described in subsection 2.5.1. SMEs assume the role of the data controller e.g., the entity determining both the purpose and the means for processing personal data. When they process this data internally, they do also take up the role of data processor.

#### 3.1.1 Common misconceptions

As we have mentioned in Section 2.2, CS awareness or, more accurately, lack thereof, has persistently been a key SME challenge. This lack of awareness by both SME management and

<sup>1</sup> It is estimated that more than 95% of enterprises globally are SMEs while, in the EU, they represent a 99% of the total.

<sup>2</sup> Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR).



employees includes not only a lack of perception of the threats at a technical level, but also misconceptions at various levels, such as the myths that:

- their company is small, therefore an unlikely victim of a cyberattack;
- cyberattacks are only related to external / malicious hacking;
- CS is a costly investment, reserved for large corporations and that SMEs don't necessarily need security policies as long as they can assign some additional tasks on top of IT staff's existing duties;
- malicious actors are only interested in large enterprises;
- cyber incidents, even if they would happen, would be of minor consequence to the SME, financially or in terms of brand image;
- purchasing antivirus and doing software updates now and then suffices for CS.

Similar misconceptions are evident when we turn our focus towards understanding -and complying with- the GDPR<sup>3</sup>:

- “GDPR only applies to big business”
- “We don't handle any sensitive personal data / we're not a hospital”
- “It's unlikely we would ever be seriously fined”
- “GDPR compliance is just a box-ticking exercise”
- etc.

It is not enough however, to point out these realities, along with the rest of the challenges and barriers to adoption which SMEs face. We need to offer practical guidance and recommendations which are uncomplicated to follow and advertise their gains and benefits for SMEs. It is true that the experience from the field is still chaotic and that, although many companies of all sizes invest vast amounts of time and resources seeking recommendations and getting familiar with GDPR and generic CS concepts to eventually meet their requirements, the end result is often fragmented and difficult to manage; let alone judge as effective.

### 3.1.2 Recommendations for boosting cyber awareness

Raising awareness is, to put it simply, the first and foremost of the responses we are recommending. From top management to the last employee, SMEs need to become aware & active and take steps towards more and better knowledge towards CS, privacy and personal data protection. In SENTINEL we believe that any gains for SMEs in these domains, even small ones, are gains absolutely worth having. For example, even SMEs with extremely limited time and resources to dedicate, will find out that regularly checking an internationally accepted cyber hygiene checklist such as that advocated by ENISA and the National Cybersecurity Alliance

---

<sup>3</sup> Star II EU Project. <https://star-project-2.eu/>

checklist (ENISA, 2020) can have an immediate positive effect on both their awareness and overall security stance.

In a more general approach, we recommend that SMEs do prioritize cybersecurity at every domain within the company, including getting management actively involved. Regular CS training that is accessible and free, but also mandatory, for everyone is also a major step. These should be followed by simple but regular cyber exercises and drills, both planned and unplanned. All of these activities should sponsor cyber best practices based on established security checklists and action points and support the overall SME security policy, as we are going to outline in the rest of Section 3.

## 3.2 Assessing risk

### 3.2.1 SMEs and information security risk

In Section 2.3.1 we referred to the most basic and overarching CS concepts which drive requirements such as **confidentiality**, **integrity** and **availability**. However, we know that security cannot just be “implemented” and expected to provide 100% protection. In practice, when implementing CS measures, it is necessary to evaluate each of these basic requirements and prioritise them depending on the specific operation of the company and, of course, on the type and sensitive nature of the data being processed. This implementation should therefore follow a “risk management approach”; in other words, a process of identifying, quantifying, and managing the risk associated with each asset, aiming to achieve a balance, e.g., not over-dedicate resources to protect assets whose impact if compromised would be minimal, while at the same time improving the security stance and minimizing overall weaknesses.

There exist several international standards and frameworks both for assessing risk associated with information systems and for recommending the necessary controls and measures. The most widely employed is the ISO/IEC 27000 family, but we should also note the BSI PAS 555:2013, the CSA Cloud Controls Matrix (CCM), the PCI Data Security Standard and many more (ENISA, 2015). ISO 27000 allows for a rigorous and structured approach for establishing, implementing, maintaining and continually improving an “information security management system (ISMS)” within a company. It consists of a multitude of interacting standards covering the whole ISMS lifecycle, to guide the company in a) identifying assets and associated security requirements, b) assessing risk, c) identifying and adopting controls to mitigate risk and d) monitoring, maintaining and improving these controls. However, this family of standards can be extremely burdensome and costly for an SME to implement, to the extent of being completely out of SMEs’ scope and capabilities, especially in the case of small and micro enterprises.

### 3.2.2 ENISA’s methodology for the security of personal data processing

ENISA, the European Union Agency for Cybersecurity, has produced extremely valuable methodologies, best practices and toolkits specifically tailored and targeted to SMEs. Specifically ameliorating the situation described above, ENISA has produced its **Guidelines** and a practical **Handbook** for SMEs processing personal data (ENISA, 2016; ENISA, 2017b). In their work, a simplified framework is proposed which provides guidelines for SMEs (acting as data controllers or processors) through each specific data processing operation and supports them in identifying and evaluating the relevant security risks and implementing the appropriate controls.



In SENTINEL, we propose the full adoption of ENISA's approach for three key reasons: (a) It provides an integrated and all-round effective methodology for assessing risk and adopting mitigative measures; (b) It is one of very few frameworks globally specifically designed and addressed to small businesses, and (c) it is an extremely well-researched approach, based on a solid body of work both by ENISA and other internationally recognised and acclaimed standards and bodies in CS.

Defining SME's requirements for CS should start with identifying their assets and associated threats and assessing risk or, more specifically, the risk these assets face at the current point in time. We shall define risk, within this context, as the **likelihood** that a threat could materialise, multiplied by the severity of its **impact**, both of which should be considered in the appropriate balance among them. Of course, calculating likelihood and impact for SMEs may introduce some room for subjectivity. For example, when estimating impact, the ad-hoc nature and different types, sensitivity etc. of personal data which the SME might be processing, calls for a thorough understanding of every facet of both the nature of the data and details of processing activities, before qualitative assessments can be made, i.e. ranking the impact of a potential data breach for the specific data and processing operation (to the SME and, more importantly, to the rights and freedoms of individuals - data subjects), as low, medium or high.

In the next subsection, we shall present ENISA's risk assessment approach for SMEs in more detail, aiming to inform SENTINEL's baseline and provide a solid foundation and better alignment for SMES for the project's technological and methodological tools.

**Five structured phases** are proposed: (a) defining the processing operation and its context (see Section 3.2.2.1); (b) understanding and evaluating impact (see Section 3.2.2.2); (c) defining the likelihood of threats (see Section 3.2.2.3); (d) assessing risk (see Section 3.2.2.4) and (e) mitigating risk by implementing organisational and technical measures (see Section 3.3).

#### *3.2.2.1 Defining the context of the processing operation*

This phase is crucial for SMEs (or for their data processors, in case they have outsourced operations) to define the boundaries of the processing which they perform and place in within a set context. This should begin with identifying each step and operation performed for data processing (collecting, saving, using, sending, deleting etc) along with relevant entities and operations, e.g., data recipients, IT assets used for processing etc.

ENISA recommends a minimum set of questions to be asked to aid the processor toward understanding the data and related operations:

- **What is the personal data processing operation?** Each processing operation, as a matter of principle, needs its own dedicated risk assessment, even if the IT assets employed at the same. For instance, a company manages HR data (e.g., data on salaries, leaves, etc.) and purchase order data, on the same infrastructure. A different risk assessment process should be followed for the two operations as in the first case the personal data involved are more critical and would result in a higher risk level, also leading to the recommendation of different security measures.
- **What are the types of personal data processed?** When special categories of data ('sensitive data') are involved, the risk is by default higher. Special categories of data

include (Article 9 GDPR): (a) data revealing racial or ethnic origin, (b) political opinions, (c) religious or philosophical beliefs, (d) trade union membership, (e) genetic data, (f) biometric data, (g) data concerning health and (h) data concerning a natural person's sex life or sexual orientation.

- **What is the purpose of the processing?** Supposing an SME processes customers' name, postal and/or email address in the context of its e-commerce platform, the same data may be processed by the SME for marketing (offers, newsletters). Still, the two processing operations, due to their distinct purposes, may present different types of risks that need to be specifically addressed.
- **What are the means used for the processing?** This may include automated or non-automated or semi-automated means, including specific IT assets. We have already mentioned (Section 2.4), SMEs increasingly rely on third-party processors for technology, such as Cloud service providers. It therefore becomes critical to acquire a deep understanding of the technologies employed, which will also aid in identifying associated vulnerabilities and threats and recommending the right measures. Examples include HR applications as well as CRM, ERP and e-commerce solutions provided either via Cloud-SaaS or via traditional on-premises architectures.
- **Where does the processing of personal data take place?** E.g., In the case where a company has delegated, to achieve more value, management of part of its IT assets (used for the processing of personal data) to a cloud provider with servers all over the world, it should specify with the cloud provider the physical location (jurisdiction) where personal data reside and adopt the necessary GDPR controls.
- **Who are the data subjects?** Specific data subjects' categories could dictate a high-risk assignment, even at this stage, as is the case of processing the personal data of children and vulnerable populations. In SENTINEL, this is starkly illustrated in the requirements of the pilot case TIG, as detailed in Section 6.2.1 of the present report.
- **Who are the recipients?** Identifying the intended recipients of personal data helps the SME understand the associated transfers and the conditions and risks beard by them, as early as possible. To illustrate examples of such transfers, consider an Internet dating app, publicising members' profiles to other registered members (as part of their core service offering). This is one type of transfer. However, the company may also have a statutory requirement to provide access to subscription and payments-related data to Revenue, financial audit services etc, as has been the recent case of Airbnb and tax services worldwide. This is another type of recipient and transfer.

### *3.2.2.2 Understanding and evaluating impact*

We mentioned early on in this report the differences in importance of impact of potential security and data breaches. We explained that, in the case of privacy and personal data protection, it is not just the company's image, brand reputation, customer loyalty, service disruption and potential financial losses that are at stake but, above all, it is the violation of the fundamental rights of individuals. This, going beyond measuring volume, can dictate high impact even in a breach involving leaking one individual's sensitive personal data. We also highlighted that there can be

a subjective element to the qualitative assessment of this impact, which is addressed by going into as much depth as possible during the process as discussed in Section 3.2.2.1.

We define the level of impact as the assessed severity of the consequences a data breach might have to the specific individual(s).

- **Low:** Individuals may encounter a few minor inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations, etc.).
- **Medium:** Individuals may encounter significant inconveniences, which they will be able to overcome despite a few difficulties (extra costs, denial of access to business services, fear, lack of understanding, stress, minor physical ailments, etc.).
- **High:** Individuals may encounter significant consequences, which they should be able to overcome albeit with serious difficulties (misappropriation of funds, blacklisting by financial institutions, property damage, loss of employment, subpoena, worsening of health, etc.).
- **Very high:** Individuals which may encounter significant, or even irreversible consequences, which they may not overcome (inability to work, long-term psychological or physical ailments, death, etc.).

We should stress again that since this impact assessment is qualitative and subjective in nature, SMEs need to consider and evaluate together, not in isolation, all of the below:

- A. The questions asked in Section 3.2.2.1.
- B. (i) The type of personal data, (ii) the criticality of the processing operation(s), (iii) the volume and timespan of data processed, (iv) the specific business of the controller/processor (e.g., data breach in a hospital is of higher impact compared to one in an auto service shop), (v) special data subject categories (e.g., children, vulnerable groups, public figures etc).
- C. The identifiability of data. In the cases where either the data is not personally, directly or indirectly, identifiable or in the case where strong pseudonymisation, anonymisation or encryption techniques (privacy-enhancing technologies or privacy-by-design architectures) are employed.

Considering all of the above, ENISA recommends that the SME is asked to evaluate the impact of the loss of each of the basic security requirements (*confidentiality, integrity, availability*) in the case of a breach, and assign an impact level assuming the worst-case scenario.

An example interview question could be: “What would be the impact of an unauthorized disclosure (**loss of confidentiality**) of personal data - in the context of your specific data processing- could have on the individual? Please assign a rating (low/med/high/v. high). Similar questions are asked (or ratings elicited via an online for or web app) for integrity and availability.

**Sample scenarios of loss of confidentiality:** (a) a laptop or company smartphone containing personal data is lost during transit; (b) equipment has been disposed without destruction of the personal data; (c) personal data are inadvertently sent to a number of unauthorised recipients; (d) some customers could access other customers’ accounts in an online service; (e) personal

data are published on an online forum; (f) a USB drive with customer data has been stolen; (g) your misconfigured or out-of-date online shop makes customer data available publicly.

**Sample scenarios of loss of integrity:** (a) a digital record that is necessary for the provision of an online social service has been changed. Your company has no way of knowing who changed it or when; (b) a digital record that is important for the accuracy of an individual's file in your online medical service has been changed; (c) you online shop is defaced and hacked and you lose your entire customer database and sales data.

**Sample scenarios of loss of availability:** (a) your online shop has gone offline due to a software error and some processing is required to bring it online again; (b) A digital personnel record is lost from the HR system and the individual needs to provide again information to the SME "from scratch"; (c) a critical service (e.g., online medical lookup database or financial service) is down and cannot be immediately fixed; (d) your ERP system is hacked and goes offline, including your ability to process or invoice customers.

This entire process will result in three (3) impact levels, one for each aspect. The highest of these is selected and assigned as the result of the impact assessment for each specific pair of data and processing operation.

### 3.2.2.3 *Defining the likelihood of threats*

#### 3.2.2.3.1 *Introduction*

We described that the risk is assessed as a measure of the impact level of a potential breach and the probability of occurrence of the associated threat. SMEs should study the threats which pertain to their specific assets and processing operations to evaluate their probability of occurring. We should be careful not to consider the severity of personal data types, subjects etc since these have already been considered in the previous phases. A threat is defined in this context as any potential event negatively affecting personal data security, such as: (a) a malicious hacker gaining access to the customer database of your online shop; (b) a malicious hacker intercepting your electronic communications; (c) a disgruntled employee stealing personal data from your CRM/ERP and selling them to a competitor; (d) a member of hospital staff inadvertently altering a critical parameter in the medical file of a patient; (e) the entire Cloud ERP going down due to a massive software malfunction of your SaaS provider; (f) a drive with an offline backup of your entire company data, including personal data, is lost in transit by a third party contractor.

To assist in understanding threats and assessing their likelihood, ENISA defines support questions to make SMEs more aware of the overall assets' environment for processing personal data and its associated threats. These are assigned between four main domains:

#### 3.2.2.3.2 *IT assets (hardware, software, network etc)*

- Is any part of your processing of personal data performed through the internet?
- Is it possible to provide access to your internal personal data processing system through the internet for specific users?
- Is your personal data processing system interconnected to another external or internal (to your organization) IT system or service?

- Can unauthorized individuals easily access your data processing environment?
- Is your personal data processing system designed, implemented or maintained without following relevant documented best practices?

#### 3.2.2.3.3 Processes and procedures

- Are roles & responsibilities with regard to personal data processing vague or not clearly defined in your SME?
- Is the acceptable use of the network, system and physical resources within your SME ambiguous or not clearly defined?
- Are employees allowed to bring and use their own devices to connect to your personal data processing system?
- Are employees allowed to transfer, store or otherwise process personal data outside the premises of the company?
- Have you neglected implementing monitoring and logging (with immutability) for personal data processing operations?

#### 3.2.2.3.4 People and parties involved in the processing

- Do you have any personal data processing operations in place which are accessible by an unlimited number of staff?
- Is any part of your data processing operation performed by a contractors/third parties (data processors)?
- Can you describe the obligations of the parties or persons involved in personal data processing as ambiguous or not clearly stated?
- Are personnel involved in the processing of personal data unfamiliar with CS?
- Is there opportunity for persons/parties involved in the data processing operations to neglect to securely store and/or destroy personal data?

#### 3.2.2.3.5 Type of business and processing volume/scale

- Do you consider your business sector as prone to cyberattacks?
- Has your company suffered a cyberattack or other type of security or data breach over the last two years?
- Have you received any notifications and/or complaints with regard to the security of the IT system (used for the processing of personal data) over the last year?
- Do you process data for a large volume of individuals?
- Are you aware of any CS best practices specific to your business sector that may have not been adequately followed?

### 3.2.2.3.6 Evaluation of threat likelihood

Answering questions like the above<sup>4</sup> will help the SME evaluate the likelihood of the associated threats. In each question a *yes* indicates a high threat probability while a *no* a lower probability. The assessment of threat occurrence probability can then be performed, qualitatively, considering the entirety of the personal data processing context(s). The likelihood may be graded as (a) **low**, where the threat is unlikely to materialize; (b) **medium**, where it is possible that the threat will materialise and (c) **high**, where the threat will likely materialise.

The likelihood level is assigned to each of the four areas (IT assets, Processes and procedures, People and parties involved in the processing and Type of business and processing volume/scale) following this basic set of rules:

- Low, when all replies in an assessment area are negative
- Medium, in the case of two or three positive replies in an assessment area
- High, when all replies in an assessment area are positive

Table 3. Threat likelihood per area

Area	Probability	
	Level	Score
IT assets	Low	1
	Med	2
	High	3
Processes and procedures	Low	1
	Med	2
	High	3
People and parties involved in the processing	Low	1
	Med	2
	High	3
Type of business and processing volume/scale	Low	1
	Med	2
	High	3

Table 4. Threat probability level

Probability scale	Probability level
4-5	Low
6-8	Med
9-12	High

Finally, to evaluate the likelihood of each threat, we first assess its occurrence probability per assessment area and then we sum up the results, as per the mappings of Table 3 and Table 4.

### 3.2.2.4 Evaluating the level of risk

Risk is determined, per threat, as the product of the multiplication of the level of the probability of the threat and its assessed impact level (as per subsection 3.2.2.2). As we have mentioned before, the risk referenced on the matrix presented on Table 5, is assigned assuming the worst possible impact on the individual for each threat. Impact level evaluations are therefore weighted towards threat occurrence probability. High and Very High Impact levels have all been assigned

<sup>4</sup> The list is by no means exhaustive and it is part of SENTINEL's self-assessment approach (WP4) to enrich and extend ENISA's suggestions.



to high risk levels and have been merged to assist with selecting and recommending mitigative measures, as detailed in Section 3.3.

*Table 5. Risk level evaluation, per threat*

		Impact level		
		Low	Med.	High
Threat occurrence probability level	Low			
	Med.			
	High			

### 3.3 Mitigating risk

#### 3.3.1 Introduction

We can assert from our study that, in today's ever-evolving threat landscape where SMEs rush to the Cloud, trying to achieve more for less, the need for identifying and recommending appropriate cyber countermeasures is more astute than ever. In the previous two subsections we both highlighted the need to drive cyber awareness for SMEs at the core/management level in order to foster a positive security culture and presented ENISA's structured framework for assessing information security requirements for protecting privacy and personal data using a risk-based approach. Following the evaluation of the level of risk, the SME (or its sub-processors if it has any) should proceed with the selection and implementation of the appropriate CS mitigations for the protection of personal data.

These activities are discussed in Section 3.3.2 with respect to organisational measures and in Section 3.3.3 with respect to technical measures. We attempt a non-exhaustive listing of measures which can be used at the middle and lower grades of the ontologies in the RE process for SENTINEL. The terms may represent desired a) organizational and technical measures, b) best practices, c) CS functions or d) change goals or capabilities pertaining to the specific domain and requirements of the participant SME.

In SENTINEL, we wish to avoid complicated formal policy and procedures and simplify our approach as much as possible, to make it approachable, understandable, affordable and practical for smaller enterprises. We do however selectively adopt the best that these procedures and standards have to offer. Following a) the hierarchy of the ISO/IEC 27001:2013 standard (ISO/IEC, 2013) and b) ENISA's risk-based approach to protecting personal data (ENISA, 2016; ENISA, 2017b), we group these measures i) by category and ii) by associated risk level (low/medium/high), below.

### 3.3.2 Organisational measures for personal data protection

#### 3.3.2.1 *Defining and enforcing a policy*

- i. Create a unified company policy for CS and personal data protection. Review and revise this policy annually (LOW).
- ii. Create separate policy regarding privacy and PDP and communicate to all personnel and relevant third parties (data processors). This policy should, at a minimum, address: roles and responsibilities of personnel, baseline measures for PDP, data processors, third parties etc. Build and maintain a detailed inventory of specific policies/procedures for PDP. (MEDIUM).
- iii. Review and revise policy per semester (HIGH).

#### 3.3.2.2 *Assigning roles and responsibilities*

- i. Define and allocate roles and responsibilities for CS and PDP per the company policy. Clearly define hand over procedures during re-organizations, changes / terminations of employment, rights revocation etc. (LOW).
- ii. Assign persons exclusively in charge of specific tasks for CS & PDP and appoint an information security officer (MEDIUM).
- iii. Formally appoint the information security officer -in writing-, clearly identifying their tasks and responsibilities. Segregate conflicting areas of responsibility (e.g., in the roles of security officer, security auditor, DPO etc.) to limit unauthorized or unintentional misuse of personal data (HIGH).

#### 3.3.2.3 *Enforcing an access control policy*

- i. Grant each person involved with personal data processing specific access control rights on a need-to-know basis (LOW).
- ii. Create a detailed access control policy document. Determine the SME's access control rules, access rights and restrictions for specific user roles for PDP. Define and document the segregation of access control roles, e.g., access request, access authorization, access administration (MEDIUM).
- iii. Identify roles with "excessive" access rights. Only assign these roles to limited / specific staff members (HIGH).

#### 3.3.2.4 *Securely managing assets*

- i. Create a register of the SME's assets, hardware, software, and network, used for personal data processing. At a minimum, include: IT resource, type (e.g., server, workstation, tablet etc.), location (on-premises, Cloud etc.). Assign a specific member of staff, e.g., IT officer, to maintaining and updating the register, on a regular basis (LOW).
- ii. Clearly define and document roles with access to certain assets (MEDIUM).

- iii. Review and revise registry -and access to assets- annually or more often as changes happen (HIGH).

#### 3.3.2.5 *Managing change*

- i. The assignee for managing assets is to ensure that all changes to IT assets of the SME are registered and monitored regularly. Software development should be performed in a separate environment that is *not* connected to the production infrastructure used for doing business or for processing personal data. When testing is required, “dummy” data should be used, not actual data. Specific procedures should be in place at all times, for the protection of personal data when testing assets (LOW).
- ii. Create and regularly maintain a detailed change policy document, which should include: a process (including timelines) for introducing changes and the roles/users that have change rights (MEDIUM).

#### 3.3.2.6 *Managing data processors for the GDPR*

- i. Define, document and agree *formal procedures, including requirements and obligations, for processing personal data*, between the SME and any third parties who process personal data on its behalf (e.g., Cloud service providers), prior to any processing activities. These should establish, as a minimum, the same level of security as mandated in the organization’s security policy. Upon discovering a data breach, the data processor shall notify the controller (SME) without undue delay. The data processor should provide sufficient documented evidence of compliance (LOW).
- ii. The SME should regularly audit the compliance of this outsourced or contracted third parties (data processors) to the agreed level of requirements and obligations (MEDIUM).
- iii. The personnel of the outsourced or contracted third parties (data processors) who are processing personal data should be subject to specific documented confidentiality/non-disclosure agreements (HIGH).

#### 3.3.2.7 *Handling incidents*

- i. Define an incident response plan with procedures to ensure an effective and orderly response to incidents involving personal data. Personal data breaches should be reported immediately to management, or, if discovered by outsourced data processors, reported to the data controller (SME). Immediate notification procedures for the reporting of the breaches to competent authorities and affected data subjects should also be in place, following art. 33 and 34 GDPR (LOW).
- ii. Document the incident response plan formally, in writing with detailed procedures, including a list of possible mitigation actions and clear assignment of roles (MEDIUM).
- iii. Perform detailed tracking and detailed event logging to record incidents and data breaches along with event details and subsequent reporting and mitigation actions performed, to enable non-repudiation auditing (HIGH).

#### 3.3.2.8 *Managing business continuity*

- i. Establish specific procedures and controls to be followed to ensure the required level of continuity and availability of the IT assets for processing personal data, in the event of an incident/data breach (LOW).
- ii. Create and document a detailed *business continuity plan (BCP)*, attached to the SME security policy, which should include clear actions and assignment of roles in case of an incident. The BCP should also define an acceptable guaranteed service quality for core business processes which provide CS and personal data protection (MEDIUM).
- iii. Specific personnel –with the necessary responsibility, authority and competence– to be tasked with managing business continuity in the event of an incident or data breach. Also, an alternative IT facility (e.g., a ‘disaster site’, with sync to a Cloud provider or co-located in a datacentre) should be considered, depending on the acceptable downtime of the related IT assets (HIGH).

#### 3.3.2.9 *Managing human resources*

- i. Ensure that employees understand their responsibilities and obligations related to PDP. Roles and responsibilities should be clearly communicated during the pre-employment and/or induction processes (LOW).
- ii. Employees should be asked, to review and consent with the SME security policy in place and sign respective confidentiality and non-disclosure agreements, before taking up duties (MEDIUM).
- iii. Employees involved in high-risk personal data processing should be bound to specific confidentiality clauses, under employment contract, NDA or other legal act (HIGH).

#### 3.3.2.10 *Cybersecurity awareness, education and training*

- i. Inform staff about the CS controls of the IT assets relating to their work. Employees involved in personal data processing should additionally be informed about relevant GDPR requirements and legal obligations through regular awareness activities (LOW).
- ii. Perform regular CS training programmes for staff, including specific programmes for the induction of new employees to GDPR obligations and activities (MEDIUM).
- iii. Document a training plan with clearly defined goals and objectives to be executed annually (HIGH).

### 3.3.3 Technical measures for personal data protection

#### 3.3.3.1 *Authentication and Access control*

- i. Implement a strict access control system for all users accessing SME IT assets, which should allow creating, approving, reviewing and deleting user accounts and their roles and permissions. User accounts should be personal and not shared (common) amongst users. In cases where this can’t be implemented, ensure that people using the same account have the same roles and responsibilities. This system should also

support robust authentication, based on the access control policy, requiring as a minimum a username/password combination. Passwords should respect a certain (configurable) minimum level of complexity and not be acceptable by the system unless their strength criteria are met. Finally, passwords must always be stored in a hashed/encrypted form in the database (LOW).

- ii. Define and document a company-wide password policy, to include at least password length, complexity, validity period, as well as number of acceptable unsuccessful login attempts. (MEDIUM).
- iii. IT assets used for processing personal data should only be accessible using two-factor authentication (2FA). The authentication factors could be passwords, security tokens, USB tokens, biometrics etc. Device authentication and access control should also be performed (HIGH).

#### 3.3.3.2 *Logging and monitoring*

- i. Implement and enable detailed logging and monitoring for every IT asset used in the processing of personal data. Every type of data processing (view, modification, deletion) should be logged. Log files should be timestamped and adequately protected against tampering and unauthorized access. Clocks should be synchronised to a single reference time source (LOW).
- ii. Enable logging of system administrator actions and events, including addition/deletion/change of user rights or access/viewing of log files. Modifying or deleting of log files should not be possible, irrespective of the access privileges of the user. Implement and enable log file health monitoring, including alerting and reporting if unusual activity or problems are detected (MEDIUM).

#### 3.3.3.3 *Server and database security*

- i. Configure database and applications servers to run on a separate account, and the minimum OS privileges necessary to function correctly. Only the personal data which is absolutely necessary for each task should be accessed and processed (LOW).
- ii. Implement encryption for data at-rest either by software or hardware means. Consider drives with built-in encryption. Apply pseudonymization techniques through separation of data from direct identifiers linking this data with the data subject (MEDIUM).
- iii. Consider privacy-by-design techniques at the database layer. E.g., authorized queries, privacy-preserving querying, searchable encryption, etc (HIGH).

#### 3.3.3.4 *Endpoint security (workstations and mobile devices)*

- i. (a) Users should not be able to deactivate or bypass security settings; (b) Install and configure anti-virus software for every device. Update on a weekly basis; (c) Disable the privileges for users to install or activate unauthorized software applications; (d) Implement screen-lock and session time-outs when the user has been inactive for a certain time period and (e) Critical security updates released by the operating system developer should be installed regularly (LOW).

- ii. Update anti-virus software with new signatures on a daily basis (MEDIUM).
- iii. Prevent transferring data from company workstations to external storage devices (e.g., USB, DVD, external hard drives etc). Workstations used for the processing of personal data should not be directly accessible via the Internet unless security measures are in place to prevent unauthorised personal data processing. Finally, full disk encryption should be enforced on all workstation drives (HIGH).

#### 3.3.3.5 *Endpoint security (mobile devices)*

- i. Define and document mobile device management procedures for security. Devices allowed to access SME IT assets should be pre-registered and authorized. Mobile devices should be subject to the same levels of access control as other terminal equipment (LOW).
- ii. Identify and assign specific roles and responsibilities for mobile devices. Enable functionality to remotely erase data (related to the SME's processing) on mobile devices that may have been compromised. Mobile devices should support separation of private and business use of the device through secure containers. Finally, mobile devices should be physically protected against theft when not in use (MEDIUM).
- iii. Implement two factor authentication (2FA) for accessing mobile devices for work. Personal data stored at the mobile device (related to the SME's processing operations) should be encrypted (HIGH).

#### 3.3.3.6 *Network security*

- i. Enforce encryption of all communication and data transfers over the Internet, e.g., through TLS/SSL (LOW).
- ii. (a) Only allow wireless access to the SME's IT assets for specific users and processes when absolutely necessary and enforce strong encryption and Wi-Fi security; (b) Prevent remote access to IT assets unless absolutely necessary, under the control and monitoring of the IT security officer, through pre-registered and approved devices; (c) Monitor network traffic to and from IT assets through tightly configured ACLs, firewalls and intrusion detection systems (IDS); (d) Segregate the network of the IT assets processing personal data from the rest of the networks of the SME, and (e) only allow access to IT assets to pre-authorized devices and terminal equipment, e.g., via MAC filtering or Network Access Control (MEDIUM).

#### 3.3.3.7 *Backup policy*

- i. Define and document company-wide data backup and restore procedures and clearly link them to specific staff roles and responsibilities. Backups should be given an appropriate level of physical and environmental protection, at least as robust as the standards applied to the data being backed up. Backups should be monitored and verified for integrity. Full backups should be carried out regularly (LOW).
- ii. Backup media should be regularly tested for reliability. Incremental, automatic (scheduled) backups should be carried out on a daily basis. Redundant copies of the backups should be securely stored in different locations. In case a third party is used,



e.g., a Cloud provider, the data must be strongly encrypted before being transmitted out of the SME (MEDIUM).

- iii. Copies of all backups should be encrypted and stored offline securely (HIGH).

#### 3.3.3.8 *Application lifecycle security*

- i. (a) Follow and adhere to best practices, state of the art and well-acknowledged secure development practices, frameworks or standards during software development lifecycles; (b) Define and implement specific security requirements during early stages of development; (c) Adopt specific techniques for supporting privacy, e.g., state-of-the-art privacy-enhancing technologies / PETs, in analogy to the defined security requirements; (d) Follow secure coding standards and practices, and (e) Perform rigorous testing and validation against the implementation of the initial security requirements, during development.
- ii. (a) Perform vulnerability assessment as well as application and infrastructure penetration testing by a trusted third party before deploying to production; (b) Schedule and carry out penetration testing regularly afterwards; (c) Obtain deep insight into security vulnerabilities of the SME's IT assets, both hardware and software, and (d) Evaluate software patches in a testing environment before deploying to a production environment.

#### 3.3.3.9 *Data disposal*

- i. Perform software-based overwriting on media prior to disposal. When this isn't possible, e.g., DVDs, etc., perform physical destruction. Shred / destroy paper or similar print media used to store personal data (LOW).
- ii. Perform multiple passes of software-based overwriting on media prior to disposal. If a third party's services are used to securely dispose of media or of paper-based records, a service agreement should be in place and a record of destruction of records should be produced as appropriate (MEDIUM).
- iii. Perform rigorous hardware-based measures, e.g., degaussing, following software erasure. Depending on the case, also consider physical destruction. If a third-party data processor is outsourced for data disposal, the process should only take place at the physical premises of the data controller SME, to avoid off-site transfer of personal data (HIGH).

#### 3.3.3.10 *Physical security*

- ii. Ensure the physical perimeter of the SME's IT assets is inaccessible by non-authorized personnel (LOW).
- iii. (a) Require identification, through appropriate means, e.g., ID cards, for personnel and visitors, accessing the company premises; (b) Identify and enforce *secure zones* by appropriate entry controls. Maintain a physical log book or electronic audit trail of all such access; (c) Install and operate intrusion detection systems in every security zone, and (d) Install / build physical barriers to prevent unauthorized physical access; (e) Physically lock and regularly monitor vacant secure areas; (f) Install and operate

automatic fire suppression systems, closed control dedicated air conditioning systems and uninterruptible power supply (UPS) at the server room and at the physical location of other critical IT assets, and (g) grant service personnel of third parties and subcontractors restricted access to secure areas (MEDIUM).

### **3.4 Summary: Responding to the challenges**

SMEs are faced with unique challenges, such as limited recourses, lack of dedicated qualified IT security experts and high regulatory pressure, including specific sectorial regulatory provisions. It is within SENTINEL's mission to support and guide SMEs, in the most approachable and easy manner possible, through a risk management approach which is practical to both understand and implement.

ENISA's methodology, designed with the SME in mind, as laid out in Sections 3.2 and 3.3, provides the baseline for the design and implementation SENTINEL's self-assessment portal, with the added value of a) GDPR-specific self-assessment framework for accountability, b) feedback from testing in cyber ranges, c) AI-enabling features which will assist SMEs in concluding more informed qualitative assessments (e.g., for threats probability and security incidents' impact levels) and providing the necessary flow of data into SENTINEL's digital core for smart recommendations as well as drafting and monitoring enforcement of CS policies and managing incident response and handling, and d) the intelligent selection and recommendation of awareness, education and training resources, tailored to each SME's requirements.

## 4 The SENTINEL digital platform

### 4.1 Introduction

For SENTINEL to achieve its mission a novel approach is key, in which consortium partners contribute either technologies/methodologies which they own, or extend existing (e.g., open source) CS and personal data protection frameworks and technologies for accessible CS, privacy, personal data protection and compliance for SMEs, in a ‘one stop shop’ approach.

In this section we shall (a) present an overview of the proposed / initial system architecture, (b) attempt an initial discussion of components interaction and how the platform may be utilised by participant SMEs, (c) examine the seven (7) technological and methodological assets contributed by consortium partners to the project and how these map onto high-level CS & PDP requirements and (d) define the project’s technological innovation.

### 4.2 The SENTINEL architecture

#### 4.2.1 An overview of the framework’s structure and functionality

A systemic view of the proposed SENTINEL conceptual architecture is shown in Figure 1.

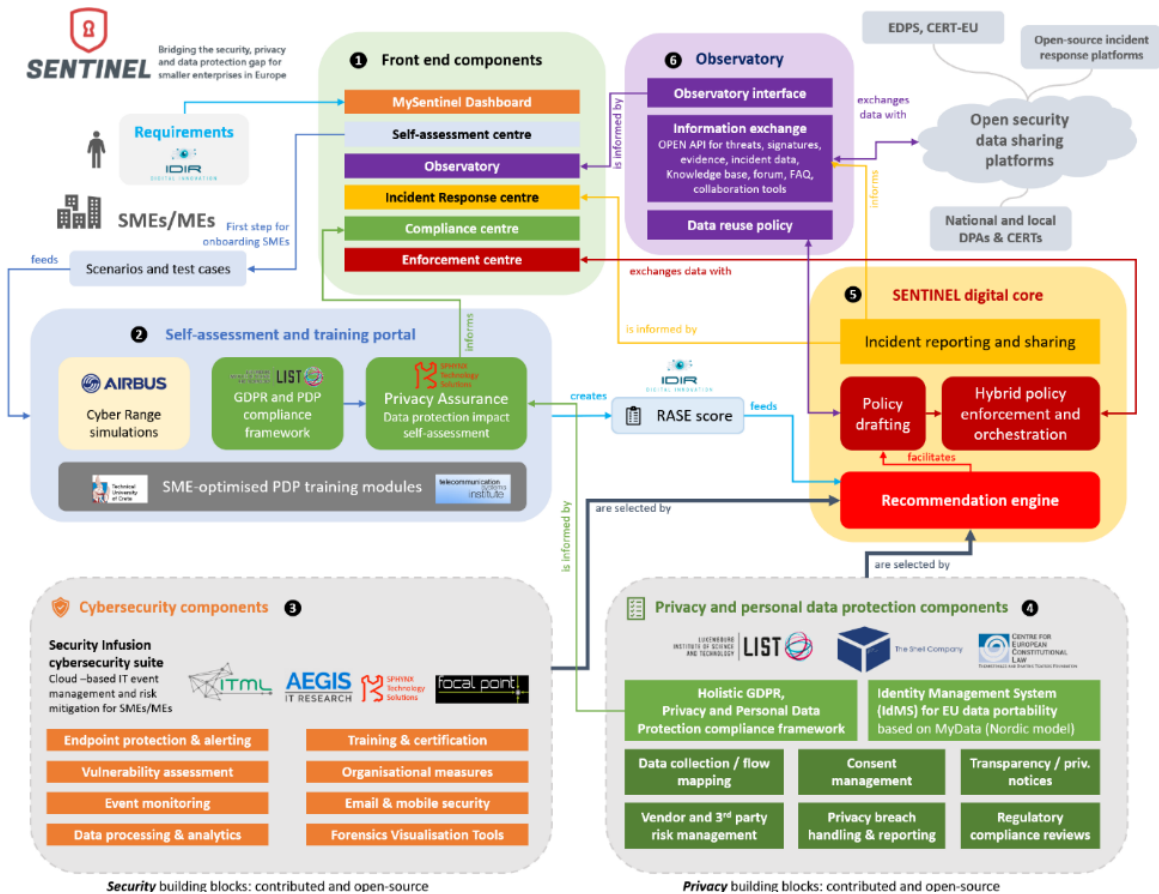


Figure 1. The envisioned SENTINEL conceptual architecture

It is important to stress early on that this initial, proposed, and high-level design, including the data exchange and interactions between components and building blocks, will be considered technically in detail, and refined, during Task 1.2, and reported in deliverable D1.2.

Task 1.2 will establish convergence with the following set of guidelines which, in turn, derive from the stated project propositions:

- a. the CS and PDP technological or methodological components to be selected and integrated **should map to generic or specific capabilities** and requirements identified for the participant SMEs, as identified by SENTINEL's RE methodology, examined herein;
- b. the **refined architecture** should be **robust, technologically feasible and easily usable by SMEs**;
- c. the architecture should assist SMEs end users with a methodology (to utilise the framework and maximise its benefits) which is **detailed, theoretically relevant and approachable**; and
- d. the architecture should provide specific technological and methodological facilitators to **help achieve the ambitious experimentation and dissemination KPIs** of the project.

In the remainder of section 4.2 we provide a high-level discussion of the proposed architecture, interactions and envisioned usage.

In Figure 1, we identify six distinct supersets of components which are henceforth referred to as the **building blocks** of SENTINEL. We are going to briefly discuss these below, including references to their interdependencies and data exchange as these were presented in the DoA. However, as planned in the DoA, the detailed technical functional and non-functional requirements, as well as those of their constituent components and modules, are the subject of T1.2, which will establish the updated architecture of the framework.

#### 4.2.2 Front-end components

Group (1): This building block represents a grouping of front-end components and public-facing web apps, all of which aggregate data to SENTINEL's primary dashboard, labelled MySentinel. This forms the platform's hub which welcomes new and existing end users and provides quick visual insight into SMEs' current progress and score, by presenting every connected service and KPI concisely with an emphasis on consistency and user experience. From the dashboard, users can easily navigate to: (a) the *self-assessment portal*, usually the first stop in their journey to increased cyber awareness, which combines SENTINEL's self-assessment tools (detailed in 4.1.2.2); (b) the *observatory*, a comprehensive knowledge base for cybersecurity, privacy and personal data protection, exchanging data in real-time among open security data platforms globally and enable a continuous feedback loop with the platform's *digital core*, to (i) optimise the reuse of policy and technology components and (ii) make data readily available for AI/ML optimisations; (c) the *incident response centre*, a SENTINEL component exchanging information with (i) the digital core's incident reporting module and (ii) the observatory's information exchange APIs to capture and share information about incidents such as data breaches to open security platforms; (d) the *compliance centre*, where the SMEs can access reports, request documentation and stay up to date with the latest developments and urgent notices as well as validate specific policy points for regulatory compliance and (e) the *enforcement centre*, where SMEs monitor the implementation of the proposed internal CS and PDP policy and get critical notifications, bubbling

up all the way to the Dashboard, assisted by the agent-based automation provided by the core's *policy orchestration* module.

#### 4.2.3 Self-assessment and training portal

Group (2): This building block is envisioned as a web app incorporating SENTINEL's simulation, self-assessment and training technologies and methodologies. The goal here is to gather data and indicators from every module, which will form the basis for calculating each participant SME's RASE score, a grouping of evaluated indicators, to be communicated to the *digital core's recommendation engine* which, in turn identify the gaps which need to be filled to achieve the identified desired CS and PDP capabilities for each SME. It remains to be defined during T1.2 whether SME assessment will be implemented in a unified 'customer journey' or in multiple distinct assessment processes, as well as what data input and output points need to be considered. Users may elect to utilise some or all the assessment options here, although specific assessments may be marked as mandatory, since a minimum set up data needs to be made available for the RASE score to be defined, to enable self-assessment. These assessments can be identified as (a) the **CyberRange** – enabled simulations and cyber scenarios, presented in Sec.4.4.6; (b) a self-assessment web tool to both evaluate the risk level associated with each data processing activity the SME preforms and assess its **current standing towards GDPR compliance**, presented in Sec.4.4.3; (c) a self-assessment module for **DPIA and holistic PDP and privacy assurance** for SMEs handling personal data, presented in Sec.4.4.5; (d) a self-assessment module combining (i) **risk evaluation for personal data protection and OTMs recommendation**, based on the ENISA PDP framework for SMEs with (ii) **tailored requirements analyses and RASE** (Risk Assessment for Small Enterprises) **score calculation**; and (e) a module for **selecting and recommending appropriate external training courses**, either free, or at an attainable cost, tailored to the SME's resources, for boosting staff cyber awareness and education.

The self-assessment portal essentially enables a central point where participant SMEs can self-profile to both a) evaluate necessary metrics for scoring and b) boost their own understanding through awareness, especially where qualitative or subjective evaluations are necessary when assessing risk. This portal will be designed with usability in mind, so end users are effortlessly guided through all the necessary iterations until the minimum data required to calculate the SME RASE score is gathered and exchanged with the digital core.

#### 4.2.4 Digital core

Group (5): The digital core, lying at the heart of the platform, delivers SENTINEL's overarching promise of "Intelligence for Compliance" and effectively allows enterprise-grade and but also attainable cybersecurity and personal data protection for SMEs. The digital core comprises three critical components: (a) the **intelligent recommendation engine**, which identifies and recommend the most suitable combinations among available internal or external modules, based on advanced AI/ML techniques with multi-criteria optimizations, including cost-effectiveness and usability, tailored to the requirements of each SME/ME; (b) A **policy drafting** module which combines technology recommendations with the necessary organisational measures, offering a human-readable, unified and enforceable data protection management policy. This module also includes a hybrid **enforcement and orchestration component** which helps SMEs track their progress enforcing the selected policies; (c) an **incident handling, reporting and sharing**

**module** which interfaces with open sharing data platforms for security to facilitate data openness and interchange while helping enrich the SENTINEL knowledge base.

#### 4.2.5 Observatory

Group (6): The SENTINEL observatory is a knowledge hub, comprising three key functions: (a) a centralised threat intelligence **knowledge base**, aggregating information about recently identified data and privacy breaches, attack vectors, forensic intelligence and cyberthreats signatures and related data as well as anonymised RASE scoring information by SMEs ecosystems, complete with a searchable KB, FAQ and collaboration tools; (b) an **open API platform** to exchange threat intelligence with SME associations, as well as open source incident response platforms, CERTs and DPAs, in coordination with the core's incident handling capabilities; and (c) an intelligent **module to coordinate policy reuse** elements when drafting new security and privacy policies for participants, exchanging data with the core's policy drafting module. The observatory incorporates global benchmarks identified for participant SMEs as well as the means to report recommendations and best practices in a concise, human-readable way at the MySentinel dashboard.

#### 4.2.6 SENTINEL cybersecurity and personal data protection components

SENTINEL achieving its objectives depends, in the final analysis, on the availability of several **internal or external components**. These components are visible in the conceptual architecture (see Figure 1) as groups (3) and (4). They are to be selected by the *recommendation engine*, drafted into proposed internal policy by the *policy drafting module*, monitored by the *policy enforcement module* and the results communicated to the *dashboard*, *incident response centre*, *compliance centre* and the *observatory*.

However, to better clarify each module's role in the envisioned integrated framework, we are presenting a more detailed mapping of all components, both internal or external to their assigned SENTINEL building blocks, and clarifying their relationships, in Table 6 below. The first seven (7) rows represent **components contributed internally by consortium partners**, based on existing technologies, and are referred to as SENTINEL's background technological assets – these are examined in detail in Section 4.4 of this deliverable. The next eight (8) rows represent components which form the necessary facilitators for core SENTINEL functionality and **will be developed from the ground up**. These components are the technical constituent parts of the platform's four building blocks (groups 1, 2, 5, 6 in Figure 1) and will be developed & integrated both during individual tasks and during the integration phase (WP5) of the project. The rest of the rows attempt a provisional mapping of modules which will need to be offered to SMEs **externally** either as freeware/open-source/open-data or commercially. This listing is of course non-exhaustive and subject to updates from tasks T1.2 and T2.4 as well as WP5.

Table 6. SENTINEL proposed components and modules mapping

Component	Assigned to group or building block	Interacts with (components or tasks)
Security Infusion	(3) Core CS	Digital Core, Integration tasks
IdMS	(4) Core PDP	Digital Core, Integration tasks
PDP/GDPR compliance framework	(2) Self-assessment, (4) Core PDP	Self-assessment, Integration tasks
MITIGATE	(2) Self-assessment,	Self-assessment, Integration tasks,



Component	Assigned to group or building block	Interacts with (components or tasks)
	(3) Core CS	Digital Core
Security and Privacy Assurance	(1) MySentinel (2) Self-assessment, (3) Core PDP	Self-assessment, Integration tasks, Digital Core
CyberRange	(2) Self-assessment	Self-assessment, Integration tasks
FVT (visualisations)	(1) MySentinel (3) Core CS	Integration tasks, Final solution integration, Self-assessment, Security and Privacy Assurance, Observatory
Intelligent requirements analyses, PDP risk assessment, RASE scoring and recommendations, including for training	(2) Self-assessment	PDP/GDPR compliance framework, CyberRange, Security and Privacy Assurance, Digital Core
Compliance monitoring	(1) MySentinel	Policy drafting & enforcement module, Observatory, Front-end components
Incident reporting and sharing module	(1) MySentinel (6) Observatory (5) Digital core	Front-end components, Policy drafting & enforcement module
Policy drafting & enforcement	(1) MySentinel (5) Digital core	Digital Core, Legal input, Front-end components, Observatory, Self- assessment
Recommendation engine	(5) Digital core	Contributed CS and PDP components, Self-assessment, External CS and PDP components, Legal input, Policy drafting & enforcement module
Observatory components, KB and security data exchange	(6) Observatory	Incident reporting and sharing module, Front-end components, External CS and PDP components, Legal input, Integration tasks
Education and training content	(2) Self-assessment	Observatory, Front-end components
Other MySentinel and web components. To be defined in T1.2	(1) MySentinel, (2) Self-assessment, (6) Observatory	Front-end components, Integration tasks plus all technical tasks
Endpoint protection*	(3) Core CS	Digital Core
Email and mobile security*	(3) Core CS	Digital Core
Software lifecycle security management*	(3) Core CS	Digital Core
Backup and business continuity management*	(3) Core CS	Digital Core
Privacy enhancing technologies for PDP: data minimisation, anonymisation, pseudonymisation, encryption *	(4) Core PDP	Digital Core
Transparency, privacy notices and consent management *	(4) Core PDP	Digital Core
Vendor and 3 <sup>rd</sup> party / subprocessors GDPR risk management*	(4) Core PDP	Digital Core
Logging, record keeping and audit management*	(4) Core PDP	Digital Core
{others / to be defined}*	(3) Core CS or (4) Core PDP	Digital Core

\* (open source or commercial),

### 4.3 Using SENTINEL: a sample scenario

In this subsection, we shall consider a generic case of how the platform might be utilised by participant SMEs, to assist in understanding the envisioned usage of the proposed architecture. Two additional specific example scenarios are presented in the DoA.

In such a typical scenario, first-time users get on board the platform dashboard to access the SME self-assessment centre. After completing the initial digital survey about the participants' company details, architecture and structure, proposed resource and budget allocation and goal-setting, the first two steps available to them are (i) a set of rigorous digital GDPR compliance, privacy assurance and DPIA self-assessment processes to identify and analyse privacy and data protection risks; and (ii) Participation in cyber ranges and infrastructure for simulating data breaches and conducting vulnerability assessments. This testing is automated, self-contained and performed with regularity for dynamic monitoring and updating their compliance score, as a RASE scoring component. The cyber range infrastructure for simulations and assessment is continually updated with pre-set scenarios and test cases by SENTINEL partners and administrators as needed. Completed assessment processes will sum up SME's RASE score (risk assessment for small enterprises), a critical component whose constituents for different security and privacy aspects inform the digital core's intelligent recommendation engine which, in turn, coordinates automated policy drafting.

SMEs, having completed assessment phases (i) and/or (ii) above, may then access a set of optional SME-optimised external PDP training modules (for implementing security and privacy organisational and technical measures), and, of course, their MySentinel dashboard which includes (a) their latest SENTINEL notifications, their up-to-date RASE score and a detailed analysis of the relevant impact factors identified; (b) the enforcement centre, where they can monitor and direct the implementation of the proposed measures; (c) the incident response centre, where data and privacy breaches are tracked and reported in real-time to the competent entities and authorities as well as open security data aggregators via open security data sharing platforms; (d) the compliance centre where the SMEs/MEs but also third parties may interact with each other to get or save reports, request documentation, stay up to date with the latest developments and urgent notices, and validate specific policy points for regulatory compliance with their assigned partner entities; and (e) the observatory, where the central knowledge base of the platform lies, along with collaboration tools and modules to orchestrate policy reuse and exchange data with open platforms.

The recommendation engine, in order to draft specific policy points, takes into account, leveraging advanced AI/ML technology with multi-criteria optimisations: (i) The participant's specific RASE score point constituents and the policy points they correspond to, based on the DPIA and other assessments performed; (ii) The requirements mapping of available security modules; (iii) their compatibility with the participant's setup; (iv) The features and compatibility of available DP-Data Protection/privacy enhancement modules; (v) Additional optimisation factors such as the Resilience / Privacy / Security achieved, including mean time-to-recovery from breaches; (vi) a cost-effectiveness match based on individual SME requirements and declarations; and (vii) the evaluated impact of data breaches of various gravity, as estimated in the ENISA-based risk assessment PDP approach during self-assessment, and other socioeconomic factors. Based on all these factors, a recommended policy is digitally drafted and offered to the company administrator(s) for review and implementation.

Following the finalization of the proposed policy, SENTINEL's hybrid agent-based orchestration and enforcement engine operates in a semi-automated way to help the SME user get the required technical and operational measures on-board with minimal human intervention, including for education, training, the implementation and validation of checklists and every other necessary measure to achieve the prescribed data protection resilience and GDPR compliance. The progress on every single policy point is digitally recorded, leveraging a workflow-based approach, and made available at the front-end, for monitoring in the SENTINEL dashboard's (1) enforcement and (2) compliance centres.

Data gathered from incident response, as well as anonymised policy points and other SENTINEL data streams will enrich the Knowledge Base in SENTINEL's observatory. This internal data is integrated with external open data sources to offer the participant an integrated informational portal and an exchange centre with external entities as described in 4.2.5.

## 4.4 SENTINEL contributed components

In the context of the objectives of T1.1, and in order to better map background technological assets onto the desired functionalities of the SENTINEL framework, in this subsection we focus on the specific technological and methodological components which, contributed by the project consortium's partners, form an integral part of the SENTINEL baseline. These components can be referenced as the first seven rows in [Table 6](#). For each one of these components, we attempt (a) a more in-depth description of the underlying technology or methodology, (b) an exploration of its usefulness and targeting for SMEs and (c) a mapping to SME requirements in the form of generic and specific CS and PDP aspects, as they have been referenced in [Table 2](#), at the end of the description of each component.

### 4.4.1 Security Infusion

Security Infusion (SI) is contributed by ITML. It is a complete agent-based software solution which collects, analyses, visualises, and presents real-time and historical data on the operation and security status of an organisation's IT assets. SI enables the retrospective forensic analysis by storing data related to past events, so they can be retrieved when necessary. Additionally, it offers regular or on-demand scans on the managed infrastructure, namely port scanning, and vulnerability assessment, thus providing reports, alerts and recommendations for the mitigation of the detected issues.

The principal SENTINEL requirements which SI addresses are monitoring, auditing, and mitigation.

Regarding CS **monitoring**, SI offers the technical infrastructure through which an SME's devices (hosts) and network are monitored using lightweight, agent-based software that runs on those assets. The agents collect relevant information including file integrity monitoring, log monitoring, rootcheck, and process monitoring. SI's monitoring capabilities provide operational awareness and early warning for detected events and CS vulnerabilities.

**Auditing** is achieved through aggregation of the security related information collected by SI's agents and visualization of the aggregated data in a Dashboard form. Additionally, data analytics services are provided for the SME's environment under protection, making use of previously identified and managed threats, security expert actions and monitored devices and services.

Sophisticated ML algorithms assist in providing business-critical, meaningful insights based on operational data.

Finally, SI provides services to end users to support **mitigation** actions on the collected, aggregated and analysed data and events, mainly through rule-based alerts that enable active response where needed and reporting on high-level events that can assist a human operator in their efforts to take actions against detected threats or vulnerabilities.

In addition to the above generic requirements, SI partially addresses a) **integrity**, by identifying filesystem changes and unauthorized / non-approved software installations, b) **availability** of hosts and services, by detecting possible threats, attacks and vulnerabilities that may hinder the availability of a service or product offered by an SME, and c) **compliance**, as SI constitutes a basis upon which the policy of an organization can be designed and implemented for compliance, as well as providing an additional service layer for compliance risks and security events identification.

SI at its current maturity state is a good fit for small companies in terms of cost and infrastructure. SI supports both on-premises Cloud implementations. This flexibility allows SMEs to pick the optimal approach to their own requirements, depending on their existing infrastructure and data sharing policy. As SI captures and handles data produced within the perimeter of the company, it is the company's decision to either perform these protective monitoring actions exclusively within these boundaries or to leverage SI's cloud infrastructure.

Although SI ideally fits the average-sized SME profile, it can easily be adapted to micro and even single-person enterprises by offering an even more targeted, relevant and desired subset of services to the end user.

Currently, SI's main target users are either IT security experts that investigate the alarms and events and make deductions on the appropriate responses and actions to be followed, or security savvy operators that can monitor the aggregated information, detect possible anomalies and possibly consult with security experts on the mitigation actions. One of SI's future aspirations is to provide semi-automatic or automatic mitigation actions, realized using AI/ML techniques on existing data, in order to include end users that are not security experts, such as ordinary SME IT staff or SME owners.

Table 7 shows the mapping of the generic requirements of Table 2, to the SI functionalities described above.

*Table 7. Mapping generic requirements to SI component*

CIA triad	PDP & compliance	PETs
<input checked="" type="checkbox"/> Confidentiality	<input type="checkbox"/> Data collection & flow mapping	<input type="checkbox"/> Encryption
<input checked="" type="checkbox"/> Integrity	<input checked="" type="checkbox"/> Record keeping & audit mgmt	<input type="checkbox"/> Anonymisation
<input checked="" type="checkbox"/> Availability	<input type="checkbox"/> Data sovereignty & portability	<input type="checkbox"/> Pseudonymisation
<b>CS generic</b>	<input type="checkbox"/> DPIA	<input type="checkbox"/> Obfuscation
<input checked="" type="checkbox"/> Policy drafting	<input type="checkbox"/> Transfers, vendors & 3 <sup>rd</sup> party mgmt	<input type="checkbox"/> Data minimisation
<input type="checkbox"/> Policy enforcing	<input type="checkbox"/> DPO management	<input type="checkbox"/> Disclosure control
<input type="checkbox"/> Non-repudiation	<input type="checkbox"/> Notices, consent management	<input type="checkbox"/> Access control
<input type="checkbox"/> AAA-Authentication, Authorisation, Accounting	<input checked="" type="checkbox"/> Compliance & accountability	<input type="checkbox"/> Differential privacy
<input checked="" type="checkbox"/> Incident reporting & handling	<b>CS technical</b>	

<input checked="" type="checkbox"/> Cyber awareness	<input type="checkbox"/> Endpoint security - computers	<input checked="" type="checkbox"/> Cloud security (SecaaS)
<input type="checkbox"/> Education & training	<input type="checkbox"/> Endpoint security – mobile	<input type="checkbox"/> SW lifecycle security
<input type="checkbox"/> Unlinkability	<input type="checkbox"/> Pentesting & vuln.assessment	<input checked="" type="checkbox"/> Monitoring - alerting
<input type="checkbox"/> Unobservability	<input type="checkbox"/> Email security	<input type="checkbox"/> Logging
<input type="checkbox"/> Self-assessment	<input type="checkbox"/> Network security	<input checked="" type="checkbox"/> Analytics, visualisation
<input type="checkbox"/> Business continuity	<input type="checkbox"/> IAM (identity/access mgmt.)	<input checked="" type="checkbox"/> Forensics

#### 4.4.2 Identity management system

The identity management system (IdMS) is to be developed by The Shell Company. We have already mentioned that the greatest GDPR-related risk for an SME is the exposure of end-users' (e.g., customers') personal data (data breach). A plausible mitigation, offering direct privacy-by-design benefits, is the transferring of the responsibility for managing personal data, in a GDPR-compliant manner, to a third party. The SENTINEL IdMS aspires to provide just this role. In such a scenario, the participant SME would have data controller responsibilities anymore, and only retain part of its role as data processor, effectively allowing the company to bear a smaller GDPR burden.

To place it “in laymen’s terms”, the identity management system functions in a similar way to a single sign-on (SSO) mechanism, such as the European digital ID or a Google Account, where SME customers (and data subjects in general) are invited to enrol (a.k.a. create their account where all personal data is collected, stored, managed etc). Operating at an infrastructure level, these accounts enable a unified EU-wide hub for personal data management which, from the position of the data controller, satisfies all related GDPR obligations, but also takes care of data sovereignty and guarantees individuals’ fundamental rights and freedoms. These are:

- **Transparency:** All data gathered by the IdMS shall have a legal basis, stated by the data processor (SME) and be easily accessible and comprehensible, in clear and plain language, avoiding risks of misinterpretation. For each specific data field/point, the IdMS has to be able to record and manage consent. Of course, users (data subjects) are able to clearly view and manage/revoke records of consent.
- **Right to erasure / object / rectification:** The end-user must be able to change/remove/revoke his data or consents at any time. If part of the data must be kept for reasons of compliance / security / business continuity, this data will be anonymised.
- **Right to portability:** At any time, users are able to extract a complete record of the data stored in the IdMS, related to their person. This data will be extracted in a common readable format (csv, json, xml, etc.).
- **Keeping activity records:** There will be full auditability (who, what, where, when) of all events (logins, changes to consents, changes to data, read data, write data) related to the IdMS for users and SME’s. Security alerts, monitoring and response handling also need to be implemented.
- **Confidentiality:** Data should be store in the most secure encrypted format possible, to ensure it is only accessible by the intended and authorized end-users, and not e.g., the IdMS systems administrators or SME partners.

- **Integrity:** Data may only be changed or removed by authorized end-users.
- **Authentication:** End users will need to authenticate (SSO) in a secure way using for example MFA or adaptive authentication based on a risk score.
- **Availability:** The IdMS should have a minimal accepted downtime value. Delivering an uninterrupted and dependable service is of paramount importance since disruption will impact the business delivery of participating SMEs. Secure, reliable and encrypted backups, highly available and redundant elastic Cloud deployments and robust Cloud DDoS protections and among the secure architectures which need to be implemented.

From the SMEs (processor's) side, the following requirements need to be in place for a GDPR compliant adoption of the IdMS for their customers or data subjects:

- **Compliant data processing principles:** A participant SME should, at all times, document and electronically evidence a legal basis for which the data will be processed, as well as how they will be processed.
- **Time limitation:** A participant SME should, at all times, document whether they will store the personal data locally; and if so, how and for how long.
- **Data access:** A participant SME should, at all times, document who will have access to the data (internally/third parties/...) and provide the associated legal reason.

Besides the GDPR requirements, the IdMS will also comply with SENTINEL's overarching requirements for SMEs:

- **Cost-effectiveness:** The implementation of the IdMS has to be cost effective for an SME. The IdMS shouldn't consume more human and financial resources compared to implementing a local IdP system or a comparable Cloud solution.
- **Usability** is related to cost effectiveness. A majority of the envisioned IdMS users would be online merchants of products or services. The IdMS should lower the bar for them to implement GDPR compliance. Integration with existing software should be straightforward, which will be also a cost minimisation factor. Example: the availability of an easy-to-install module for WordPress, Drupal etc.

Table 8 shows the mapping of the generic requirements of Table 2, to the IdMS functionalities described above.

*Table 8. Mapping generic requirements to IdMS component*

CIA triad	PDP & compliance	PETs
<input checked="" type="checkbox"/> Confidentiality	<input type="checkbox"/> Data collection & flow mapping	<input checked="" type="checkbox"/> Encryption
<input checked="" type="checkbox"/> Integrity	<input checked="" type="checkbox"/> Record keeping & audit mgmt	<input type="checkbox"/> Anonymisation
<input checked="" type="checkbox"/> Availability	<input checked="" type="checkbox"/> Data sovereignty & portability	<input type="checkbox"/> Pseudonymisation
<b>CS generic</b>	<input type="checkbox"/> DPIA	<input type="checkbox"/> Obfuscation
<input type="checkbox"/> Policy drafting	<input type="checkbox"/> Transfers, vendors & 3 <sup>rd</sup> party mgmt	<input checked="" type="checkbox"/> Data minimisation
<input type="checkbox"/> Policy enforcing	<input type="checkbox"/> DPO management	<input checked="" type="checkbox"/> Disclosure control
<input checked="" type="checkbox"/> Non-repudiation	<input checked="" type="checkbox"/> Notices, consent management	<input checked="" type="checkbox"/> Access control
<input checked="" type="checkbox"/> AAA-Authentication, Authorisation, Accounting	<input checked="" type="checkbox"/> Compliance & accountability	<input type="checkbox"/> Differential privacy
<input type="checkbox"/> Incident reporting & handling	<b>CS technical</b>	



<input type="checkbox"/> Cyber awareness	<input type="checkbox"/> Endpoint security - computers	<input type="checkbox"/> Cloud security (SecaaS)
<input type="checkbox"/> Education & training	<input type="checkbox"/> Endpoint security – mobile	<input type="checkbox"/> SW lifecycle security
<input type="checkbox"/> Unlinkability	<input type="checkbox"/> Pentesting & vuln.assessment	<input type="checkbox"/> Monitoring - alerting
<input type="checkbox"/> Unobservability	<input type="checkbox"/> Email security	<input checked="" type="checkbox"/> Logging
<input type="checkbox"/> Self-assessment	<input type="checkbox"/> Network security	<input type="checkbox"/> Analytics, visualisation
<input type="checkbox"/> Business continuity	<input checked="" type="checkbox"/> IAM (identity/access mgmt.)	<input type="checkbox"/> Forensics

#### 4.4.3 GDPR self-assessment methodology

The GDPR self-assessment methodology is to be developed, to be integrated with SENTINEL's self-assessment portal for SMEs, by LIST.

GDPR introduces a responsibility shift between regulators and regulated entities (the SMEs). The latter are now responsible for implementing appropriate and effective technical and organisational measures for protecting personal data, as well as the ability to evidence / demonstrate their implementation. Complying with the GDPR thus presupposes demonstrating accountability [GDPR Art. 5(2)]. Delving into more detail SMEs processing personal data should be able to demonstrate their capabilities to:

- Protect the privacy of their data subjects (customer, employees, beneficiaries etc) when processing personal data (**appropriateness**)
- Ensure the effectiveness of the adopted organisational and technical measures over time (**effectiveness**)

In the GDPR self-assessment approach developed for SENTINEL, each capability cited above is based on three processes. Each process covers a well-defined set of requirements which must be satisfied for compliance. Below, these three processes are presented in more detail.

##### 4.4.3.1 Data Collection

The first process deals with gathering the data and requirements which will enable the recommendation of the appropriate technical and organisational measures for compliance, following a risk-based approach.

GDPR compliance is associated, among other provisions with keeping records of personal data processing activities [GDPR Art. 30]. This methodology enables SMEs to centrally manage their processing records for GDPR (**Req#1.1**).

The aforementioned risk-based approach requires determining the level of risk (to the privacy and the rights and freedoms of the data subject) associated with the SME performing said processing activity. In other words, if this processing activity is judged as low-risk, fewer evidence may be required to demonstrate accountability, e.g., keeping records of processing activities suffices when the risk is low. Conversely, when risk is evaluated as high, during a data protection impact assessment (DPIA), additional evidence is expected for the SME to demonstrate accountability. Our GDPR self-assessment approach will consider specific types of evidence and their assumed risk level, as can be seen in Table 9.

Activities associated with higher risk levels, presuppose the implementations of all activities associated with lower risk levels; e.g., an SME processing high-risk (e.g., sensitive) personal data

should keep detailed records, implement AND evidence effectiveness of the appropriate technical and organisational measures.

*Table 9. Associating SME activities with risk level for compliance*

Risk level	DPIA criteria	How to demonstrate accountability / How to comply with GDPR?
Low	0	Demonstrate that the SME maintains detailed records of processing activities
Medium	1	Demonstrate that appropriate measures are implemented
High	2	Demonstrate that the implemented measure are effective

To make online self-assessment more usable for end users, by reducing the volume of input required, once a processing activity is sufficiently described to make an assessment, the self-assessment portal should automatically evaluate the associated risk level (**Req#1.2**). As detailed in ENISA's risk-based approach (subsection 3.2.2.2), this assessment includes subjective and qualitative characteristics, which necessitate the simplification of the self-assessment process with automatically evaluable sets of questions which will inform the self-assessment's model-driven approach.

The data collection process should also be as usable by end users as possible, putting all the necessary user interface and user experience best practices into application during the design and the implementation of the appropriate web forms enabling the “user journey” in the self-assessment portal (**Req#1.3**). In doing so, and similar to Req#1.2, the requested user input shall follow a predefined data template (e.g., multiple choice / evaluable); the SME end user will only have to pick the scenario context best describing their actual context from a predetermined number of choices. (**Req#1.4**).

The (a) scenarios for personal data processing activities, (b) scenarios for evaluating the associated and (c) the complete list of either implemented or recommended technical and organisational measures (which may later form part of the recommended CS and PDP policy) should be drawn from SENTINEL's common knowledge base and be interlinked with the appropriate attributes to enable intelligent association and selection (**Req#1.5**).

#### 4.4.3.2 Assessment

The second process deals with measuring the appropriateness and effectiveness of technical and organisational measures, which forms the core activity for assessing GDPR compliance.

In more details, the assessment consists of analysing each set of technical and organisational measures, which the SME self-declares to have implemented, against predefined and rated categories of “data protection measures”. This model will be developed in R and integrated with the SENTINEL self-assessment portal (**Req#2.1**). The data will then be made exportable (e.g., CSV/XLSX) and/or communicated over a web services API, to better interface with SMEs who might have in place software for keeping records of personal data processing activities for GDPR (**Req#2.2**).

#### 4.4.3.3 Assessment results

The third process is dedicated to demonstrating accountability. The results of the GDPR compliance self-assessment provide two distinct groups of feedback:

1. Feedback with regard to the **assessed capability level** of the SME's current processes.
2. Feedback with regard to **recommended organisational and technical measures**, which is further broken down into
  - a. Mandatory recommendations
  - b. Optional recommendations

This feedback will be aided with visual aids and charts, wherever possible, and exportable to download and print (**Req#3.1**). The results will also be communicated to / integrated with the MySentinel Dashboard (**Req#3.2**).

Table 10. Requirements overview for the GDPR self-assessment methodology

Functional requirement	Id.	Individual requirements
Data Collection	Req#1.1	The platform should allow record keeping management.
	Req#1.2	The platform should auto-determine the risk level associated with personal data processing activities.
	Req#1.3	The platform should make data collection easy.
	Req#1.4	The platform should present users with pre-defined choices, limiting the subjectivity of qualitative assessments.
	Req#1.5	The platform should interface with SENTINEL's common knowledge base for informational objects (e.g., processing activity and risks/threat scenarios, organisational & technical measures etc).
Assessment	Req#2.1	The platform should be able to integrate software components developed in R.
	Req#2.2	Data processing record-keeping software must be connected to the self-assessment component.
Assessment results	Req#3.1	The platform should provide visual aids and cues and be able to export results.
	Req#3.2	The platform should be integrated with the MySentinel Dashboard.

Data-driven and B2C SMEs are more affected by the GDPR. Usually, these SMEs lack the resources to hire a dedicated DPO. SENTINEL could help alleviate this by providing parts of an e-DPO service, even for the companies which may be exempt from this requirement. This e-DPO should help them to tackle CS for personal data protection issues. The GDPR self-assessment, coupled with ENISA's approach, as shown in Table 11, can be leveraged to demonstrate compliance, manage compliance and/or elicit actionable CS and PDP recommendations.

Table 11. Mapping generic requirements to GDPR assessment methodology component

CIA triad	PDP & compliance	PETs
<input type="checkbox"/> Confidentiality	<input checked="" type="checkbox"/> Data collection & flow mapping	<input type="checkbox"/> Encryption
<input type="checkbox"/> Integrity	<input checked="" type="checkbox"/> Record keeping & audit mgmt	<input type="checkbox"/> Anonymisation
<input type="checkbox"/> Availability	<input type="checkbox"/> Data sovereignty & portability	<input type="checkbox"/> Pseudonymisation
<b>CS generic</b>	<input checked="" type="checkbox"/> DPIA	<input type="checkbox"/> Obfuscation
<input checked="" type="checkbox"/> Policy drafting	<input type="checkbox"/> Transfers, vendors & 3 <sup>rd</sup> party mgmt	<input type="checkbox"/> Data minimisation
<input type="checkbox"/> Policy enforcing	<input type="checkbox"/> DPO management	<input type="checkbox"/> Disclosure control
<input type="checkbox"/> Non-repudiation	<input type="checkbox"/> Notices, consent management	<input type="checkbox"/> Access control
<input type="checkbox"/> AAA-Authentication, Authorisation, Accounting	<input checked="" type="checkbox"/> Compliance & accountability	<input type="checkbox"/> Differential privacy
<input type="checkbox"/> Incident reporting & handling	<b>CS technical</b>	

<input checked="" type="checkbox"/> Cyber awareness	<input type="checkbox"/> Endpoint security - computers	<input type="checkbox"/> Cloud security (SecaaS)
<input type="checkbox"/> Education & training	<input type="checkbox"/> Endpoint security – mobile	<input type="checkbox"/> SW lifecycle security
<input type="checkbox"/> Unlinkability	<input type="checkbox"/> Pentesting & vuln.assessment	<input type="checkbox"/> Monitoring - alerting
<input type="checkbox"/> Unobservability	<input type="checkbox"/> Email security	<input type="checkbox"/> Logging
<input checked="" type="checkbox"/> Self-assessment	<input type="checkbox"/> Network security	<input type="checkbox"/> Analytics, visualisation
<input type="checkbox"/> Business continuity	<input type="checkbox"/> IAM (identity/access mgmt.)	<input type="checkbox"/> Forensics

#### 4.4.4 MITIGATE: evidence-driven risk assessment

MITIGATE is a methodology and software, contributed by Focal Point (Papastergiou and Polemi, 2017; Kalogeraki, Apostolou et al., 2018; Kalogeraki, Polemi et al., 2018; Schauer, Polemi et al., 2019). The software is simulation-based and enables the identification, analysis and mitigation of company-wide cyber threats.

In the literature, the analysis of cyber risks is based on a straightforward approach which combines a set of parameters such as the likelihood and consequences of a security event, the exploitation level of a vulnerability etc. MITIGATE supports this approach with rational decision making. MITIGATE obtains security-related information from online repositories and promotes a rigorous, rational approach that gathers and critically appraises quality information gleaned by simulations or available online. In MITIGATE, the evaluation and mitigation of the cyber threats is neither objective nor neutral; it is an inherently rational process which relies on well-defined and acceptable security data, not on the experience and judgment of individuals.

##### 4.4.4.1 Key Features

MITIGATE integrates a collaborative and standards-based risk management system which considers threats arising from their interdependencies, including potential cascading effects. It enables operators to manage security in a holistic and cost-effective manner, while at the same time producing and sharing knowledge associated with the identification, assessment and quantification of company-wide cascading effects. In this way, operators are able to predict security risks, but also to mitigate and minimise the consequences of divergent security threats i.e., based on information associated with simulation scenarios and data acquired from online sources and repositories (e.g., National Institute of Standards and Technology (NIST) Repositories).

MITIGATE is supported by: (i) a range data analytics technique which leverages various data sources and data types, considering data that may be incomplete, uncertain, or probabilistic; (ii) pioneering mathematical techniques for predicting and analysing threat patterns; and (iii) innovative visualisation and simulation techniques. These instruments provide a basis for collaboration between the various agents to (a) identify and model assets, processes, risks, stakeholders' relationships/interactions and dependencies; (b) analyse threats, vulnerabilities and countermeasures accumulated in various online sources and repositories; (c) identify, evaluate and classify various ICT-based risks, while at the same time facilitating the risk resolution; (d) design, execute and analyse risks and threat simulations in order to discover viable attack vectors assets. These attack paths consist of vulnerability chains that can be exploited by attackers in order to accomplish their malicious goals; and (e) exploit the results towards formulating effective evidence-based mitigation plans.

#### 4.4.4.2 Incorporating the cybersecurity requirements of smaller enterprises

SMEs need more usable and cost-effective tools to address today's ever evolving threat landscape of increasing sophistication, where SMEs are increasingly targeted for data and privacy breaches. These tools should combine boosting cyber awareness and education with a better understanding of the company's cyber stance, threats and potential for improvement, including the business risks associated with potential security breaches (e.g., damage to individual rights and freedoms, service disruption, breach of statutory obligations, customer loss, and damage to reputation) and the extended risk to e-business as a whole.

MITIGATE contributes towards improving SMEs overall security and privacy level with the provision of an innovative, open, collaborative, integrated and comprehensive risk assessment framework. It can particularly help SMEs to continuously monitor and efficiently identify, assess and manage security and privacy risks associated with their IT-based business processes and IT assets, including those utilised in personal data processing activities.

#### 4.4.4.3 MITIGATE in SENTINEL

Within SENTINEL, MITIGATE will be used for risk assessment system, aiding SMEs in evaluating their overall security level at a cost effective (in terms of budget, human effort and time) and user-friendly manner, while specifically addressing their limited cyber expertise, budget and diversity of underlying on-premises or Cloud infrastructures.

MITIGATE responds to the requirements of a generic contemporary SME's business setup and CS requirements efficiently. In particular, the MITIGATE risk assessment approach will be further customized and simplified to provide much-needed guidance to SMEs in identify their requirements and risks, ensuring data protection and building a cyber awareness culture.

The MITIGATE risk assessment capabilities will be adapted and coupled with self-assessment and management capabilities, allowing the SMEs to (a) raise their IT security intelligence and culture; (b) lower IT security-related risks to defined acceptable levels, while keeping staff up to date with current and upcoming threats; (c) assist them on how to comply with regulatory frameworks; and (d) boost overall CS awareness. This is shown in Table 12.

Table 12. Mapping generic requirements to MITIGATE component

CIA triad	PDP & compliance	PETs
<input type="checkbox"/> Confidentiality	<input checked="" type="checkbox"/> Data collection & flow mapping	<input type="checkbox"/> Encryption
<input type="checkbox"/> Integrity	<input type="checkbox"/> Record keeping & audit mgmt	<input type="checkbox"/> Anonymisation
<input type="checkbox"/> Availability	<input type="checkbox"/> Data sovereignty & portability	<input type="checkbox"/> Pseudonymisation
CS generic	<input type="checkbox"/> DPIA	<input type="checkbox"/> Obfuscation
<input checked="" type="checkbox"/> Policy drafting	<input type="checkbox"/> Transfers, vendor & 3 <sup>rd</sup> party mgmt	<input type="checkbox"/> Data minimisation
<input type="checkbox"/> Policy enforcing	<input type="checkbox"/> DPO management	<input type="checkbox"/> Disclosure control
<input type="checkbox"/> Non-repudiation	<input type="checkbox"/> Notices, consent management	<input type="checkbox"/> Access control
<input type="checkbox"/> AAA Authentication Authorisation Accounting	<input checked="" type="checkbox"/> Compliance & accountability	<input type="checkbox"/> Differential privacy
<input type="checkbox"/> Incident reporting & handling	CS technical	
<input checked="" type="checkbox"/> Cyber awareness	<input type="checkbox"/> Endpoint security - computers	<input type="checkbox"/> Cloud security (SecaaS)
<input type="checkbox"/> Education & training	<input type="checkbox"/> Endpoint security – mobile	<input type="checkbox"/> SW lifecycle security
<input type="checkbox"/> Unlinkability	<input checked="" type="checkbox"/> Pentesting & vuln.assessment	<input checked="" type="checkbox"/> Monitoring - alerting
<input type="checkbox"/> Unobservability	<input type="checkbox"/> Email security	<input checked="" type="checkbox"/> Logging
<input checked="" type="checkbox"/> Self-assessment	<input type="checkbox"/> Network security	<input checked="" type="checkbox"/> Analytics, visualisation
<input type="checkbox"/> Business continuity	<input type="checkbox"/> IAM (identity/access mgmt.)	<input checked="" type="checkbox"/> Forensics

#### 4.4.5 Security and privacy assurance platform

The Security and Privacy Assurance Platform (SPAP) is contributed by Sphynx Technology Solutions. SPAP enables SMEs onboarding SENTINEL to perform complete security assessments based on international industrial standards, including Cloud and network standards. SPAP leverages a model-driven approach based on comprehensive security and privacy assurance models enabling an automated but systematic representation of the SMEs including relations between their assets. The analysis of this model is used in assessing SMEs' security posture by identifying and describing processes, personnel, IT assets, data assets (including classifications for personal data), threats corresponding to these assets and the sequence of events that can lead to the manifestation of threats. Additionally, SPAP allows identifying the security properties that must be maintained for each asset, the vulnerabilities which may compromise the security properties and the security controls that mitigate the exploitation of the vulnerabilities.

All organizations can be (and are) similarly attacked, no matter what their size. Criminals tend to target SMEs for various reasons such as they offer a good value to risk ratio and as many SMEs provide services to larger organizations, they can enable criminals attack those larger organizations through their supply chain. Moreover, although that the majority of SMEs (>80%) process critical information, the majority of SMEs use some basic security controls such as endpoint antivirus protection, backups, firewalls and perform systematic software updates whereas at the same time fewer SMEs utilise logging and alerting systems.

SPAP assesses the assurance of specific security principles. The most important *security requirements* that the SPAP addresses is the **CIA triad** (Confidentiality, Integrity, and Availability), which is an organisational model designed to guide information storing policies. SPAP is an easy-to-use tool, with which SMEs will create their own models and initiate assessments with which to identify security gaps and violations.

Furthermore, SPAP addresses **Authentication, Authorization and Accountability (AAA)** requirements which are also very important for SMEs. The AAA is a strong requirement especially in the case that we are dealing with **personal data**. Without any of them companies are keeping their data vulnerable to data breaches and unauthorized access. Studying those aspects, authentication determines whether users are who they claim to be and, authorization determines what users can and cannot access, and accountability practically monitors the resources a user consumes during network access (i.e., can include the amount of system time or the amount of data sent and received during a session). Today every organization is trying to use the best authentication/ authorization/ accounting practices to keep their data secure. Unfortunately, sometimes it is very difficult to recognize vulnerabilities in your system and to identify suspicious behaviour. Based on the SPAP, SME end users can build models which could identify authentication/ authorization issues early on. The platform also recognizes suspicious behaviour (e.g., repeated login failures or the suspicious use of a user account).

SPAP supports SMEs by providing an easy to use and, model driven tool that users could run tests both in a static and in a runtime fashion, to assess their assets security posture. In a static fashion SPAP will be able to perform evaluations such as penetration testing based on popular



tools (i.e., openVas<sup>5</sup>) and vulnerabilities assessments based on popular databases (i.e., MITRE<sup>6</sup>). In the run-time fashion, SPAS is able to deploy specific Event Captors that collect events (e.g., system events) that are digested by a monitor system. The monitor system is able to analyse and reason on these events in a model-driven way and assess the violation of specific security properties in real-time. Therefore, SPAP supports different static testing systems, able to determine the operational evidence to be captured and the assessment needed to assess the effectiveness of implemented system's security controls and runtime assessments of event patterns and rules.

Summarizing, the Security and Privacy Assurance Platform (SPAP) combines several features which can support SMEs/MEs offering them services in a cost-effective way. Within SENTINEL, SPAP will be further tailored to implement a digital data protection impact self-assessment (DPIA) functionality that will be offered to the SMEs offering them an accessible toolkit to identify and analyse privacy and data protection risks. The DPIA functionality will be able to inspect the organisational and technical measures that are put in place by the SMEs/MEs to ensure compliance with GDPR requirements. Moreover, it will be able to verify their effectiveness of those measures whereas it will be able to record all information related to the handling of personal data in line with the quality assurance approach, and to equip SMEs with a cost-efficient and simple to use tool to determine their accountability. Utilising DPIA, participating SMEs have a single provider for their security, privacy, and personal data protection self-assessment needs. This approach that SPAP follows can enable SMEs to identify and describe the processes within the targeted organisation, its personnel, the systems software, hardware, physical and data assets, the threats corresponding to these assets and the sequence of events that leads to the manifestation of these threats, the security properties that must be maintained for each asset, the vulnerabilities that compromise the security properties and the security controls that mitigate the exploitation of the vulnerabilities.

Table 13 shows the mapping of the generic requirements of Table 2, to the SPAP functionalities described above.

*Table 13. Mapping generic requirements to SPAP component*

CIA triad	PDP & compliance	PETs
<input checked="" type="checkbox"/> Confidentiality	<input checked="" type="checkbox"/> Data collection & flow mapping	<input type="checkbox"/> Encryption
<input checked="" type="checkbox"/> Integrity	<input checked="" type="checkbox"/> Record keeping & audit mgmt	<input type="checkbox"/> Anonymisation
<input checked="" type="checkbox"/> Availability	<input type="checkbox"/> Data sovereignty & portability	<input type="checkbox"/> Pseudonymisation
<b>CS generic</b>	<input checked="" type="checkbox"/> DPIA	<input type="checkbox"/> Obfuscation
<input checked="" type="checkbox"/> Policy drafting	<input type="checkbox"/> Transfers, vendors & 3 <sup>rd</sup> party mgmt	<input type="checkbox"/> Data minimisation
<input type="checkbox"/> Policy enforcing	<input type="checkbox"/> DPO management	<input type="checkbox"/> Disclosure control
<input checked="" type="checkbox"/> Non-repudiation	<input type="checkbox"/> Notices, consent management	<input type="checkbox"/> Access control
<input checked="" type="checkbox"/> AAA-Authentication, Authorisation, Accounting	<input checked="" type="checkbox"/> Compliance & accountability	<input type="checkbox"/> Differential privacy
<input type="checkbox"/> Incident reporting & handling	<b>CS technical</b>	
<input checked="" type="checkbox"/> Cyber awareness	<input type="checkbox"/> Endpoint security - computers	<input type="checkbox"/> Cloud security (SecaaS)
<input type="checkbox"/> Education & training	<input type="checkbox"/> Endpoint security – mobile	<input type="checkbox"/> SW lifecycle security
<input type="checkbox"/> Unlinkability	<input checked="" type="checkbox"/> Pentesting & vuln.assessment	<input checked="" type="checkbox"/> Monitoring - alerting
<input type="checkbox"/> Unobservability	<input type="checkbox"/> Email security	<input checked="" type="checkbox"/> Logging

<sup>5</sup><https://www.openvas.org/>

<sup>6</sup><https://www.mitre.org/>

<input checked="" type="checkbox"/> Self-assessment	<input type="checkbox"/> Network security	<input checked="" type="checkbox"/> Analytics, visualisation
<input type="checkbox"/> Business continuity	<input type="checkbox"/> IAM (identity/access mgmt.)	<input checked="" type="checkbox"/> Forensics

#### 4.4.6 Cyber Range

CyberRange, contributed by Airbus CyberSecurity, is a platform which is able to recreate realistic IT/OT infrastructures. Its purpose is to provide penetration testing and cyber training capabilities by automating the deployment of virtual infrastructures, simulating actual scenarios and enacting them with real cyber-attacks within a secured environment.

The platform offers an existing library of virtual machine and docker, to make it easier to start modelling SME's IT infrastructures to be simulated. There is also the possibility to integrate an external virtual machine or docker, and connect physical equipment to the virtual network.

Hardware-wise, the CyberRange is composed of a physical setup of servers and switches, which is either mobile or mountable in a server bay. The system hosts specialised software, designed by Airbus CyberSecurity, called LADE (Life and Death Engine). The LADE is able to automate deployment of virtualized infrastructure, composed of a virtual machine, virtual network and the associated containers, executing single actions and scenarios in the deployed architecture, and providing remote access to the VMs and containers from a web browser without additional plugins.

The CyberRange can be deployed for large infrastructures, but it can also be used by smaller enterprises without access to CS experts. Thanks to the user interface, it is easy, even for non-expert IT staff to replicate and deploy the SME's infrastructure in a simulation. With a drag and drop interface, the user is able to deploy predefined workstation and network templates. This offers the possibility for SMEs, to enable self-assessment and discover vulnerabilities.

The CyberRange is composed of work zones, a work zone is a set of resources (memory, CPU, network). Figure 2 shows an example of a work zone

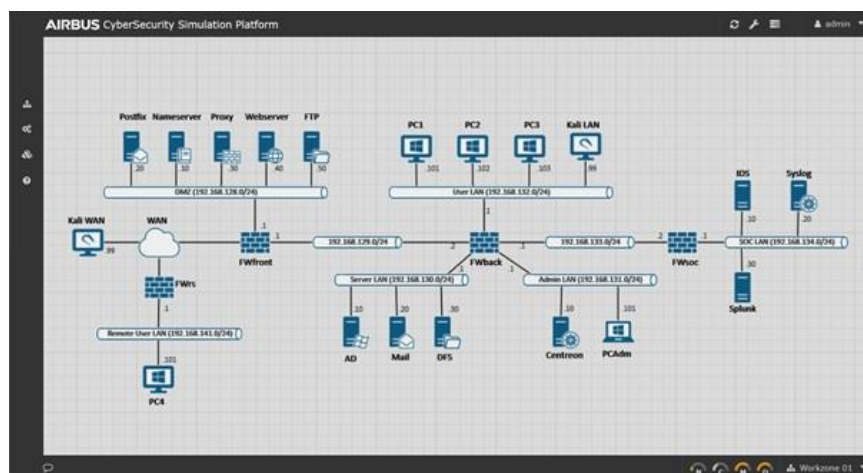


Figure 2. A CyberRange work zone

All work zones are isolated from each other and give the possibility to efficiently deploy networks and hosts. The CyberRange can also be accessed remotely. From the web interface, users can

access different work zones and open remote console to visualise the virtual machine and interact with it. For example, a trainer can launch and manage a cyber scenario for trainees in real-time.

Within SENTINEL, CyberRange, will be deployed for SMEs, and its effectiveness and adaptivity to their needs will be evaluated. The results from testing within the CyberRange, which is not a mandatory part of the SENTINEL’s self-assessment processes, will affect the participant SME’s RASE scoring and be used to identify CS, privacy and PDP gaps to be addressed. The experimentation results with SMEs will also be leveraged to enrich the CyberRange library of attacks, and further tailor cyber training designs and simulation scenarios specifically for SMEs.

Table 14 shows the mapping of the generic requirements of Table 2, to the CyberRange functionalities described above.

*Table 14. Mapping generic requirements to CyberRange component*

CIA triad	PDP & compliance	PETs
<input type="checkbox"/> Confidentiality	<input checked="" type="checkbox"/> Data collection & flow mapping	<input type="checkbox"/> Encryption
<input type="checkbox"/> Integrity	<input type="checkbox"/> Record keeping & audit mgmt	<input type="checkbox"/> Anonymisation
<input type="checkbox"/> Availability	<input type="checkbox"/> Data sovereignty & portability	<input type="checkbox"/> Pseudonymisation
CS generic	<input type="checkbox"/> DPIA	<input type="checkbox"/> Obfuscation
<input type="checkbox"/> Policy drafting	<input type="checkbox"/> Transfers, vendors & 3 <sup>rd</sup> party mgmt	<input type="checkbox"/> Data minimisation
<input type="checkbox"/> Policy enforcing	<input type="checkbox"/> DPO management	<input type="checkbox"/> Disclosure control
<input type="checkbox"/> Non-repudiation	<input type="checkbox"/> Notices, consent management	<input type="checkbox"/> Access control
<input type="checkbox"/> AAA-Authentication, Authorisation, Accounting	<input type="checkbox"/> Compliance & accountability	<input type="checkbox"/> Differential privacy
<input type="checkbox"/> Incident reporting & handling	CS technical	
<input checked="" type="checkbox"/> Cyber awareness	<input type="checkbox"/> Endpoint security - computers	<input type="checkbox"/> Cloud security (SecaaS)
<input type="checkbox"/> Education & training	<input type="checkbox"/> Endpoint security – mobile	<input type="checkbox"/> SW lifecycle security
<input type="checkbox"/> Unlinkability	<input checked="" type="checkbox"/> Pentesting & vuln.assessment	<input type="checkbox"/> Monitoring - alerting
<input type="checkbox"/> Unobservability	<input type="checkbox"/> Email security	<input type="checkbox"/> Logging
<input checked="" type="checkbox"/> Self-assessment	<input checked="" type="checkbox"/> Network security	<input checked="" type="checkbox"/> Analytics, visualisation
<input type="checkbox"/> Business continuity	<input type="checkbox"/> IAM (identity/access mgmt.)	<input type="checkbox"/> Forensics

#### 4.4.7 Forensics Visualisation Toolkit

Cyber risks are a major issue which all companies have to deal with. SMEs often are not in a position to effectively identify and address security breaches, due their well-analysed budget and resource restrictions as well as lack of awareness and expertise. It is sadly often the case that an SME security incident is discovered after a significant amount of time has passed, along with its severe consequences to personal rights, data integrity and compliance.

The Forensics Visualization Toolkit (FVT), contributed by AEGIS Research, realizes a security awareness “pyramid” for small enterprises, comprising user-centric visualization tools and services, deployed on top of traditional security solutions, to ease the “grey” area that lies between false negative and false positive incidents. It is evident that existing automated systems like e.g., antivirus systems, cannot provide the level of details a non-IT expert (e.g., lawyer) will need to act efficiently against an alert/alarm. Thus, either useful information is lost (the user decides to decrease the sensitivity level – false negative incident) or the system is overloaded (the user decides to increase the sensitivity level – false positive incident). FVT guides the user in the “grey” area between those two incidents and facilitates the identification of the pursued one, namely the true negative incident.

FVT acts as an additional layer to existing security solutions, for increasing the CS situational awareness of operators when dealing with security incidents. It provides custom implementations for the needs of forensics analysis in a specific Company Infrastructure (CI), analysing in depth the specific CI and defining a number of CI Performance Indicators (CIPIs) that are utilized to sufficiently monitor the deployment. It also provides intuitive and detailed visualizations to active digital forensics analysis, allowing multiple real-time views of the same data to be realized and speed up situational awareness. Other innovative forensics services of the FVT include the timeline analysis, preconfigured views, state comparisons and other means to quickly identify the root cause of a CS incident and minimise response time. These functionalities can also assist auditing procedures due to their complementarity to existing monitoring/logging solutions and efficient handling of large amounts of gathered digital evidence. Operators can track actions that led to specific events and quickly assess the required sources during an auditing process.

Within SENTINEL, FVT could facilitate small businesses' CS awareness by acting as remote cyber security service that is effective in identifying security threats, minimizing false positive alarms and finally help businesses limit potential risks. It can provide complementarity on top of other CS products by offering detailed and intuitive insights capable of guiding the human security operator. To support this SaaS approach, FVT would have to undergo some adaptations, mainly on the side of data management and resource handling since gathering security from many businesses involves privacy restrictions and larger amounts of data to be kept and handled simultaneously.

On the other hand, FVT is also capable of being deployed in an isolated environment and act as a user-centric visualization approach that can be offered to both IT and non-IT security experts of an SME that want an intuitive way of visualising their CS-related data. Based on its complete containerised version, FVT can be easily deployed in local networks, connect to existing data sources and offer its out-of-the-box visualisation capabilities.

Table 15 shows the mapping of the generic requirements of Table 2, to the CyberRange functionalities described above.

*Table 15. Mapping generic requirements to FVT component*

CIA triad	PDP & compliance	PETs
<input type="checkbox"/> Confidentiality	<input checked="" type="checkbox"/> Data collection & flow mapping	<input type="checkbox"/> Encryption
<input type="checkbox"/> Integrity	<input type="checkbox"/> Record keeping & audit mgmt	<input type="checkbox"/> Anonymisation
<input type="checkbox"/> Availability	<input type="checkbox"/> Data sovereignty & portability	<input type="checkbox"/> Pseudonymisation
<b>CS generic</b>	<input type="checkbox"/> DPIA	<input type="checkbox"/> Obfuscation
<input type="checkbox"/> Policy drafting	<input type="checkbox"/> Transfers, vendors & 3 <sup>rd</sup> party mgmt	<input type="checkbox"/> Data minimisation
<input type="checkbox"/> Policy enforcing	<input type="checkbox"/> DPO management	<input type="checkbox"/> Disclosure control
<input type="checkbox"/> Non-repudiation	<input type="checkbox"/> Notices, consent management	<input type="checkbox"/> Access control
<input type="checkbox"/> AAA-Authentication, Authorisation, Accounting	<input type="checkbox"/> Compliance & accountability	<input type="checkbox"/> Differential privacy
<input type="checkbox"/> Incident reporting & handling	<b>CS technical</b>	
<input checked="" type="checkbox"/> Cyber awareness	<input type="checkbox"/> Endpoint security - computers	<input checked="" type="checkbox"/> Cloud security (SecaaS)
<input type="checkbox"/> Education & training	<input type="checkbox"/> Endpoint security – mobile	<input type="checkbox"/> SW lifecycle security
<input type="checkbox"/> Unlinkability	<input type="checkbox"/> Pentesting & vuln.assessment	<input type="checkbox"/> Monitoring - alerting
<input type="checkbox"/> Unobservability	<input type="checkbox"/> Email security	<input checked="" type="checkbox"/> Logging
<input checked="" type="checkbox"/> Self-assessment	<input type="checkbox"/> Network security	<input checked="" type="checkbox"/> Analytics, visualisation
<input type="checkbox"/> Business continuity	<input type="checkbox"/> IAM (identity/access mgmt.)	<input checked="" type="checkbox"/> Forensics

## 4.5 Summary: SENTINEL's technological innovation

In subsection 4.4, we completed a study of the modules, in the form of methodologies and technology/software, which are contributed by consortium partners, to be further tailored for SMEs and integrated in SENTINEL. We also mapped their features to specific *functional requirements* (both generic and technical) identified earlier for CS, privacy and personal data protection.

The gaps *not directly covered* by partner-contributed technologies will be addressed by internal or external modules. The “ordering” of this selection will be the focus of the SENTINEL's RASE scoring and AI-enabled recommendation engine, so that SENTINEL's overarching non-functional requirements for *cost-effectiveness* and *usability* are satisfied. This selection would have to be managed in the following descending order (from higher to lower priority): (1) Internally developed and/or integrated modules, e.g., the SENTINEL self-assessment modules, staff education & trainings recommender, policy drafting module, incident response centre, etc.; (2) External free or open-source solutions and data-sharing platforms and (3) External commercial solutions.

Considering the above, we can summarise SENTINEL's technological innovation as:

- Democratising state-of-the-art CS and PDP services, usually only accessible to large enterprises, and delivering them to SMEs;
- Leveraging AI to ensure these recommendations optimally satisfy each SME's requirements for cost-effectiveness and usability;
- Complementing recommendations with intelligent policy drafting & management, incident response, CS knowledge base, open data sharing & reuse and compliance management;
- Venturing beyond the state-of-the-art
  - IdMS: positioning SMEs as key players in the merging personal data management/sovereignty ecosystem while effortlessly assuring compliance.
  - Self-assessment: digitalising existing theoretical frameworks for self-assessment (DPIA, GDPR compliance, etc.), with a focus on usability for SME end-users.
  - Cyber ranges: designing archetypal SME infrastructure templates and offering SMEs the unprecedented opportunity to train in such virtualised simulations.

## 5 SCORE: The SENTINEL RE methodology

### 5.1 Introduction

The field of Requirements Engineering is arguably one of the most sensitive areas in the development of not only software but more importantly in the development of systems and organisational structures and processes supported by such systems that provide added value to businesses. An early stakeholder understanding of the impact of different requirement choices on the enterprise is more likely to actively engage stakeholders, highlight strategic options and ultimately deliver useful and sustainable systems that are aligned to enterprise strategy and offer opportunities for influencing this strategy (Jarke, Loucopoulos et al., 2011).

The **purpose** of the SENTINEL RE methodology is to establish a way of working such that stakeholders of SMEs will be able to articulate their needs and aspirations for enhancing their CS for privacy environment. To this end, it is important for the project to establish a robust, generic and user-facing way of working that would facilitate the mapping from needs and aspirations to system functionalities offered by the SENTINEL innovative architecture. This is in alignment with one of the project's ambitions with respect to RE<sup>7</sup> which states that “...it (the RE methodology) will be used (a) to identify the challenges and needs for data privacy and compliance processes in SMEs thus ensuring that the SENTINEL framework meets these challenges and needs in a most effective and efficient manner, and (b) to inculcate a generic RE methodology specifically targeting SMEs to address their specific needs and capabilities in such a way so as to enable these companies to yield the benefits of using the SENTINEL framework”.

The SENTINEL RE methodology, referred to henceforth as “SCORE”<sup>8</sup>, has been developed specifically for the SENTINEL project, building upon earlier work, known as e-CORE (early Capability Oriented Requirements Engineering) (Loucopoulos, Kavakli et al., 2020) that has been applied on a variety of domains (Bravos, Loucopoulos et al., 2017; Loucopoulos and Kavakli, 2017; Loucopoulos, Kavakli et al., 2018; Dimitrakopoulos, Kavakli et al., 2019). SCORE focuses specifically on CS for privacy requirements in the context of other business and system requirements. It proposes a systematic process whose central focus is to answer the key question of “*what kind of capabilities are required for SMEs to obtain enterprise-grade security and personal data protection?*”.

A RE methodology attempts to facilitate the **transformation from an existing situation to a new desired one**. SCORE achieves this by developing user-centric models whereby SME stakeholders provide input about capabilities that a business possesses or exchanges to achieve a specific purpose or outcome. The models act as a repository of knowledge about business goals, people, process/procedures, technology, and information that form the essential building blocks of the SME business. Using these building blocks SCORE seeks to define the goals for change that need to be met by improved capabilities to ensure that requirements for CS for privacy are systematically identified.

---

<sup>7</sup> See DoA in the Grant Agreement, section 1.4.1.4.

<sup>8</sup> The name “SCORE” stands for “Security Capability Oriented Requirements Engineering”. It also signifies a relationship to the part of the SENTINEL project of ‘task 4.3: Tailor-made requirements analyses via self-assessment, trainings and RASE scoring’, that deals with scoring based on user requirements.



In order to provide a full account of SCORE we define its **ontological foundation** in terms of its **meta-model** (Section 5.2.1). The meta-model represents the semantic baseline for representing the essential elements required for eliciting requirements according to SCORE. We ensure that this baseline is consistent with the recommended ENISA methodology for the security of personal data (see Section 3.2.2) something that helps requirements stakeholders to respond to questions using the more formal modelling of the methodology (these questions are presented in Table 20). Based upon the aforementioned semantic baseline, we present four complementary views for modelling **capabilities**, **goals**, **actor dependencies** and **informational objects** (Section 5.2.2). These are intertwined views and they represent the necessary information to express a full set of requirements to be subjected to review and analysis. The models also can motivate stakeholders to answer the questions shown in Table 20, thus combining a theoretical with a practical way of specifying requirements. The overall framework of the SCORE way of working, the steps to be followed and the practical questions to be raised are detailed in Section 5.3.

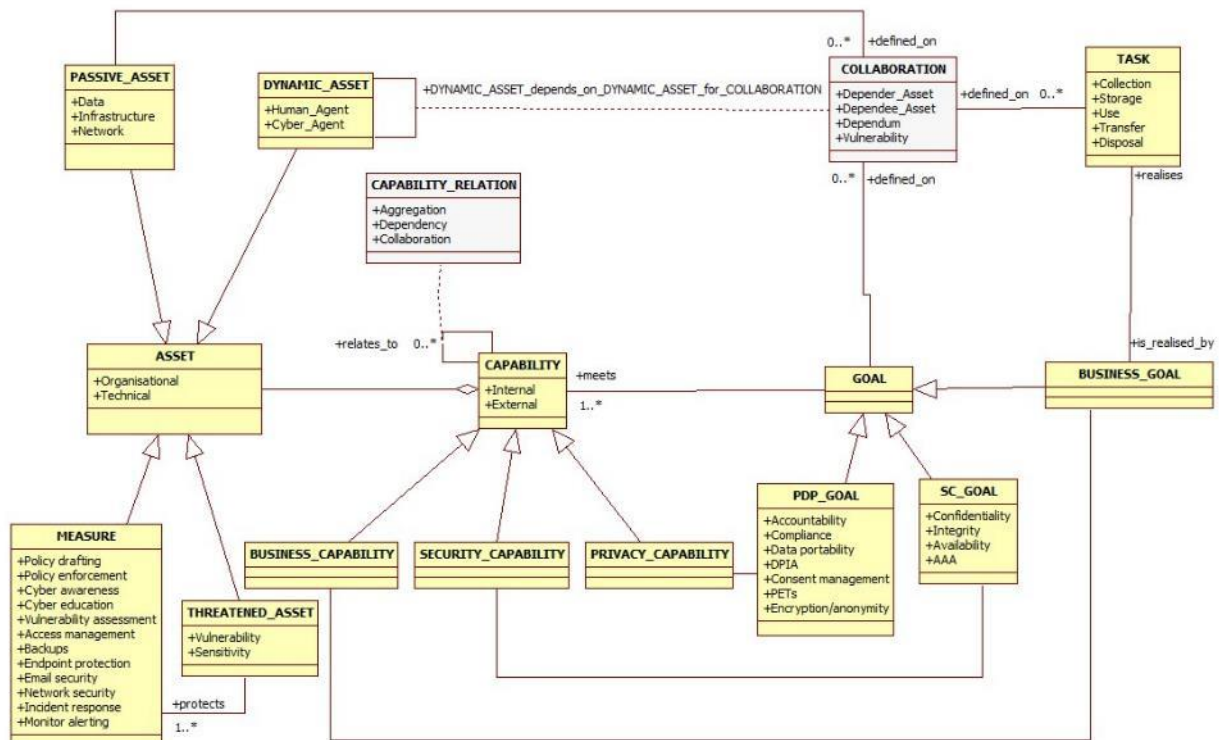
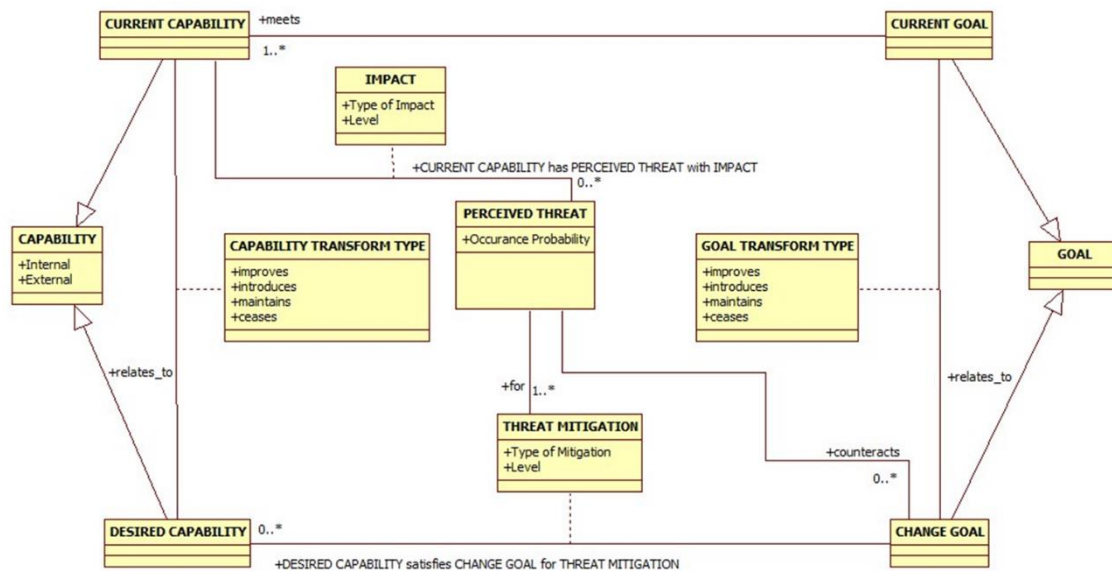
## 5.2 The SCORE meta-model and its modelling views

One of the main objectives of RE is the communication and sharing of enterprise knowledge between different stakeholders. An issue of concern therefore, is how to describe such knowledge so that this sharing can be effective. In practice this question can be answered in terms of two possible alternatives: using natural language (for example consultants' reports) or using **conceptual modelling**. The use of natural language has the advantage of ease of transferability but falls short on formality that in turn hinders any potential analysis that one might apply on such knowledge in order to inform decision makers on appropriate strategies. The use of conceptual modelling languages as defined by ISO (van Griethuysen, 1982; Jardine, 1984; ISO, 1987), overcomes these shortcomings. Furthermore, the use of conceptual modelling during the RE phase will greatly facilitate the mapping of requirements onto specific functionalities offered by the SENTINEL architecture.

The conceptual modelling framework applied in SENTINEL is based on our previous research and experience in the field of Requirements Engineering. The focus of the process is on enterprise *capabilities* and enterprise *goals*. This will offer SMEs the ability to focus on strategic issues pertaining to their needs for CS and personal data protection. The process follows attempts to first understand the current situation with respect to capabilities and goals, and the threats that are perceived as impacting those capabilities. This phase is then followed by analysing gaps and documenting the new stakeholder goals which should ultimately lead to a new set of capabilities ameliorating the threats.

### 5.2.1 The SCORE conceptual foundation

Central to SCORE is the notion of *capability*. We believe that capability represents a most suitable metaphor that provides the means of considering the intertwining of technical, organisational and social concerns in such a way, that it is possible to connect strategic objectives and high-level organizational requirements to technological artefacts in a unified manner. The use of capability for representing the status of a business and its needs (the what) rather than focusing on the technical implementation (the how) serves as a powerful communication tool among business users and information technologists.



In a capability-oriented paradigm we are interested in what has been identified in the strategic management field (Barney, 1991), as the possession of *valuable, rare, inimitable* and *non-substitutable* resources of enterprise as a source of sustainable advantage, whether these are existing capabilities or new ones that need to be introduced. Using capabilities as the starting

point one can begin investigating and analysing what lies behind these fundamental enterprise assets, what goals govern them, what actors are involved and how they collaborate to synergistically meet requirements for enterprise transformation.

The basic concepts upon which models of requirements can be built in shown in Figure 3. The Level 0 meta-model of Figure 3 is further detailed in the meta-model of Figure 4.

As shown in Figure 3 we are interested in both `CURRENT CAPABILITIES` and `DESIRED CAPABILITIES` in order to model the necessary transformations from the former to the latter. There is a symmetry between `CURRENT CAPABILITIES` and `DESIRED CAPABILITIES` in the sense that each set is related to enterprise goals, the former to `CURRENT GOALS` and the latter to `CHANGE GOALS`. Requirements are modelled and analysed in terms of the juxtaposition of `CHANGE GOALS` against `CURRENT GOALS` and their corresponding capabilities. In this sense we incorporate the concept of *capability transformation* at the same time as considering *goals transformation*.

In terms of CS and PDP requirements we are interested in identifying the `PERCEIVED THREATS` that are identified by business users as having an `IMPACT ON CURRENT CAPABILITIES`. Analysis of such threats and their potential impact will lead to the definition of new business goals (`CHANGE GOALS`) and their corresponding `DESIRED CAPABILITIES` leading to `THREAT MITIGATION`.

As shown in Figure 4, a `CAPABILITY` is a composition of `ASSETS` which may be organisational or technical in nature. Furthermore, `ASSETS` are distinguished between `PASSIVE` and `DYNAMIC`. `PASSIVE ASSETS` are enterprise resources that by themselves have no behaviour but rather they facilitate other assets that have a dynamic behaviour. `DYNAMIC ASSETS` represent the social dimension, focusing on the `COLLABORATION` between human, physical and cyber agents, defining dependencies between them. These dependencies may involve the exchange of `PASSIVE ASSETS`, or the execution of some `TASK`, or the achievement of a `GOAL`.

In the context of CS and personal data protection requirements, capabilities may involve technical measures (e.g., endpoint protection software, authentication, authorisation & access control technologies, PETs etc.), whilst organisational measures may include documenting and implementing a security / PDP policy, incident response protocols, etc. Similarly, analysis can be performed for other concepts as shown Figure 4.

The two meta-models shown in Figure 3 and Figure 4 represent an integrated view of the semantics used within the SCORE methodology. In practice, we partition this view into four modelling viewpoints, namely those of: *capability*, *goal*, *actor-dependency* and *informational*. This allows stakeholders to focus their attention on specific aspects pertaining to their requirements and to also manage the complexity and volume of information. These four modelling views are visually represented using standardised notation, explained in Section 5.2.2.

Given that these modelling viewpoints are semantic projections on the overall meta-models, it follows that the four individual viewpoints are **intrinsically interrelated** thus, presenting a holistic view of the situation being modelled.

There are anchor points in these models whose semantic relationships lead to ensuring completeness of all the different modelling views. This is demonstrated in the application of the methodology using the two pilot cases in Section 6. These interrelationships objectively provide answers to the following questions: “*why does the enterprise need these capabilities?*” (answered

by the *goal model*), “what socio-technical actors are involved, how do they co-operate in order to realise these capabilities and how vulnerable to CS threats is this cooperation?” (answered by the *actor dependency model*), “what kind of information is used in this co-operation?” (answered by the *informational object model*).

The advantage of this interrelation is twofold. First, it gives us the ability to validate all models for consistency and completeness in a visual manner. Second, it guides the identification of CS and PDP-related risks in the current situation, as well as the evaluation of the risk mitigation proposition(s) in the desired situation. This is demonstrated in Section 6.3 for the TIG pilot case and in Section 6.4 for the CG pilot case.

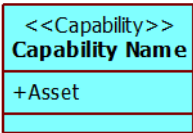
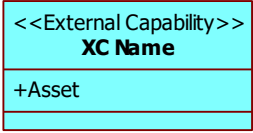
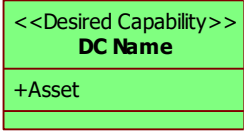

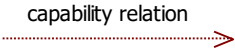
## 5.2.2 The SCORE modelling

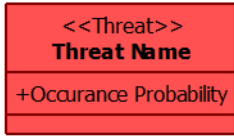
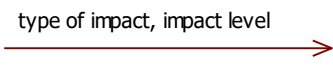
This section describes the way that SCORE modelling is applied using graphical notation for the modelling of capabilities, goals, actors and informational objects. The graphical notations adopted are used in order to ease communication between all requirements stakeholders and they all adhere to the SCORE underpinning semantics as shown in the meta-models of Figure 3 and Figure 4.

### 5.2.2.1 The capability model

The purpose of the capability model is to capture existing as well as desired (by the SME) capabilities, the assets that constitute each capability and the associated threats. The notation used is based on the Unified Modelling Language (UML) and is presented in Table 16. These terms are used here in the strict sense of RE practices and are consistent with the RE literature.

Table 16. Graphical notation used in capability modelling

Notation	Description	Example
	<b>Capability:</b> An aggregation of the assets necessary in order for the enterprise to meet its objectives <b>Asset:</b> The human (e.g., staff), physical (e.g., machines, land, etc.) or non-physical (e.g., software, funding etc.) assets encapsulated by the capability.	‘Data Sharing’ capability is the capacity for exchanging information using technical assets such as Microsoft OneDrive, Google Workspace, Dropbox, etc.
	<b>External Capability:</b> An aggregation of assets that belong to another enterprise whose collaboration is needed for some business objectives to be met	‘Online Training’ capability that some external company has with which the enterprise collaborates for providing training its staff.
	<b>Desired Capability:</b> a new or improved capability that meets a change goal.	“Risk Analysis” is a newly introduced capability aiming to satisfy the change goal ‘To protect sharing of service user personal data with social care agencies’.
	<b>Aggregation:</b> shows that a certain capability encapsulates a set of capabilities	“HR Managing” capability is the aggregation of ‘Responsibility Assigning’, ‘Staff Training’ and ‘Staff Accrediting’ capabilities.
	<b>Capability relation:</b> denotes inter or intra organization interaction of capabilities (collaboration, dependency)	The ‘Staff Accreditation’ capability depends on the ‘Staff Training’ capability in order to provide trusted

Notation	Description	Example
	towards the realization of a common end result.	services.
	<b>Threat:</b> any circumstance or event with the potential to adversely impact organizational capabilities.	Over dependency on the commercial Cloud for “Data Sharing” may adversely impact the capability of ‘Data protecting”.
	<b>Impact:</b> describes the type and severity of the impact of a threat to a capability (risk assessment)	‘Data breach’ threat has a high security impact on the ‘Data sharing’ capability.

As seen in Table 16, the notation used in SCORE allows for the visualisation of (a) existing capabilities (both internal and external) highlighted in colour blue, (b) desired capabilities, highlighted in colour green and (c) threats to existing capabilities, highlighted in colour red.


#### 5.2.2.2 The goal model

The purpose of the goal model is to define explicitly the SME intentions and causal relationships between these intentions and how these are met by SME capabilities. A goal model describes the ‘causal transformation’ of strategic goals into one or more sub-goals that constitute the means of achieving desired ends. Each step can result in the identification of new goals that are linked to the original one through causal relations thus forming a hierarchy of goals. Goals can be of different types (*Achieve, Maintain, Avoid*) depending on the kind of behaviour required for realising these goals. Soft goals are quality goals related to CS and PDP. The leaf goals in this hierarchy are operational goals that can be assigned to SME capabilities. Therefore, capabilities can be shown to be explicitly related the SME’s intentions. The diagrammatic notation of a goal model can show on one hand how a high-level strategic goal can be realised, through a systematic analysis of goals causality, to SME capabilities and on the other hand why a specific set of capabilities exist in the SME ecosystem.






Goals form the baseline information upon which any change will be sought to apply. Requirements for change are expressed through change goals. Change goals provide a way of identifying and reasoning about the needs for change (e.g., addressing certain threats) from an intentional perspective.

The notation used in this model is based on the KAOS (Dardenne, Lamsweerde et al., 1993; Matulevičius and Heymans, 2005) and *i\** (Yu and Mylopoulos, 1998) frameworks as implemented in the RE-Tools modelling toolset (Supakkul and Chung, 2009-2012). In SCORE we extend the notation to incorporate the notion of ‘change business goal’ Table 17, provides an overview of the notation used in goal modelling and their meaning. These terms are used here in the strict sense of RE practices and are consistent with the RE literature.

Table 17. Graphical notation used in goal modelling

Notation	Description	Example
	<b>Business Goal:</b> A high level intention that an enterprise wishes to achieve / avoid / cease. Strategic business goals are progressively refined to operational goals which are met by certain enterprise capabilities.	‘To provide safe and reliable services’ is a high level business goal common to most enterprises. This can be refined to operational goals such as ‘To process service user data’



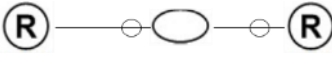
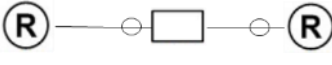
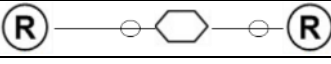


Notation	Description	Example
	<b>Soft Goal:</b> A quality goal related to cybersecurity or privacy	Security
	<b>AND Decomposition:</b> a way of refining high-level goals into more operational sub goals. If all sub goals are achieved, then the initial goal is also achieved. On the other hand, failing to achieve a sub goal means that initial goal cannot be achieved either.	The goal 'To provide trusted services' is AND decomposed in two sub goals 'To ensure staff accreditation' and 'To assess staff suitability'.
	<b>Assignment:</b> shows that a certain capability meets a business goal.	'To assess staff suitability' goal is met by the 'HR Managing' capability.
 [Change Business Goal Name (Transformation Type)]	<b>Change Goal:</b> A business goal aiming to address a perceived threat affecting some enterprise capability	'To increase cybersecurity and privacy awareness' is a new goal introduced in order to address the threat of data breach affecting the enterprise's 'Data sharing' capability.
 Change Sec/Priv Goal Name (Transformation Type)	<b>Change soft goal:</b> a quality goal related to cybersecurity or privacy aiming to address some perceived threat	'To strengthen secure processing of data' improves an existing security goal and aims to address the threat of data breach affecting the enterprise's 'Data sharing' capability.

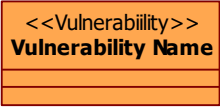
### 5.2.2.3 The actor dependency model

The purpose of the actor dependency model is to visually demonstrate the operational parts of SMEs through the collaboration between different organisational actors, where these actors are shown in the meta-model of Figure 4 as 'dynamic assets'. The notation used for actor-dependency modelling is shown in Table 18. These terms are used here in the strict sense of RE practices and are consistent with the RE literature.

Table 18. Graphical notation used in actor-dependency modelling

Notation	Description	Example
	<b>Automated agent:</b> A sub-type of a dynamic asset. It can be a software or physical system.	Cloud System, Online management system
	<b>Human agent:</b> A sub-type of a dynamic asset. It can refer to a person, team or organisation.	DPO, Staff
	<b>Goal Dependency:</b> describes the fact that one actor depends on the other achieving a goal so that the former may attain some other goal.	'TIG Staff' depends on the 'DPO' in order to monitor data processing'.
	<b>Resource Dependency:</b> describes the fact that one actor depends on the other actor for the availability of an entity (physical or informational).	The 'Leadership Team' depends on the 'Individual business manager' for knowing the 'incidents' regarding data breaches.
	<b>Task Dependency:</b> describes the fact that one actor depends on the other actor for	The 'Social Agency' depends on the 'Cloud

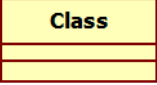






Notation	Description	Example
	carrying out an activity.	Service' for 'Accessing service user data'.
	<b>Vulnerability: a gap or weaknesses of an asset or of a collaboration between assets that undermine the security or privacy of the enterprise.</b>	The Staff 'Inadequate security awareness' undermines enterprise security.

#### 5.2.2.4 The informational object model

The purpose of the informational object model is to detail the types of data, the informational assets that are managed by the SME. It is important to identify these assets for which an SME is responsible, a point that has been discussed extensively in Section 2.5 in terms of the legal obligations of SMEs towards protecting personal data and in Section 3.1 which introduces the point that risk increases proportionally to the nature of the personal data at stake.

Table 19. Graphical notation used in informational object modelling

Notation	Description	Example
	<b>Class:</b> An entity type, described by a number of attributes.	Employee, Service User, Service
	<b>Association relationship:</b> specifies a logical connection between classes.	A 'Service' is provided to a 'Service User'
	<b>Aggregation relationship:</b> denotes that a class is a collection of other classes.	The 'Commissioning Authority' is an aggregation of a number of 'Commissioning Teams'
	<b>Composition relationship:</b> denotes that a class is composed of other classes.	The 'Genomic data' is composed of 'Genomic variant data' and 'Case related and technical data'
	<b>Generalisation relationship:</b> indicates that one of the two related classes (the subclass) is considered to be a specialised form of the other (the super type).	The 'Operational Manager' is a subclass of the 'Employee'

In order to model informational assets, we use the well-known terminology of the Unified Modelling Language (UML) for information-related concepts, known as Class Association Diagram (CAD) (see Table 19), to model the semantics of such objects that are found either as assets in the capability model or as resource dependencies between actors.

### 5.3 The SCORE way-of-working

The SENTINEL RE process and detailed activities are summarized in five phases, which can be applied as shown in Figure 5.

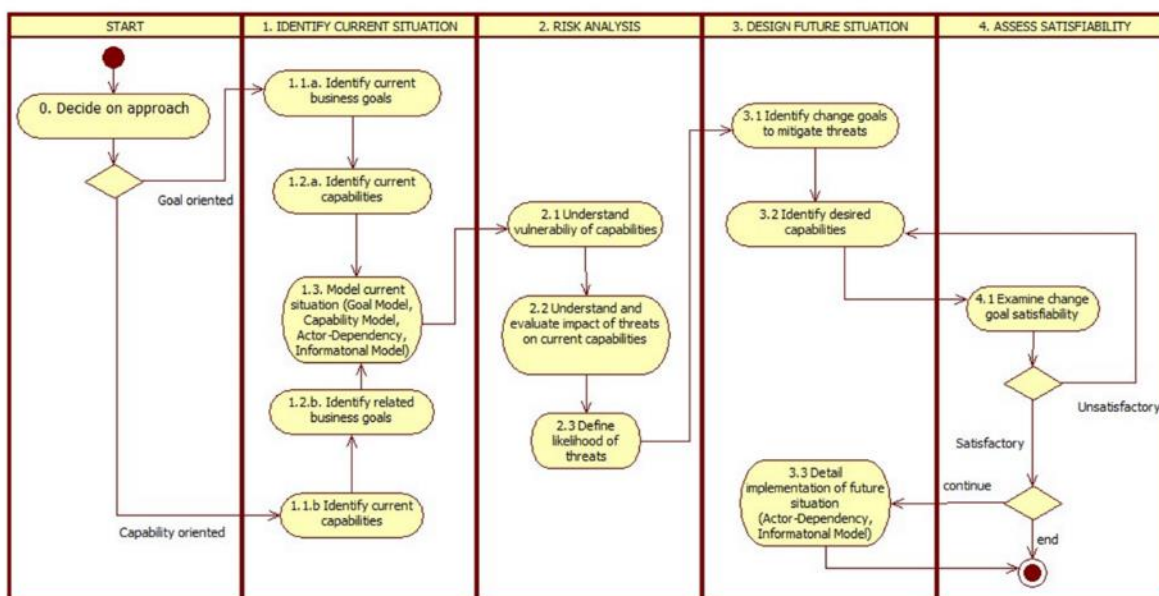


Figure 5. The SCORE way of working

In more detail, the requirements elicitation process in SENTINEL needs to be driven by a set of questions each of which would address specific ontologies that are to be found in the meta-model (see Figure 3 and Figure 4). The way that these questions will be phrased should result in a set of requirements statements with a formal underpinning and with the ability for downstream analysis to facilitate reasoning about the SME requirements.

Alternative ways for focusing the elicitation process are: Goal-oriented or Capability-oriented depending on the participants' knowledge and whether the analysis will focus on strategy first or on assets first. For example, in the TIG pilot case (see Section 6.3) the stakeholders were more interested in adopting strategic viewpoint and therefore a goal-oriented approach was chosen to demonstrate the SCORE way of working. In the case of CG the focus was mostly on assets and therefore a capability-oriented way of working was adopted (see Section 6.4).

Note that in both cases, as can be seen in Figure 5, the result of both is the modelling of the current situation (step 1.3).

To facilitate the process, a number of key questions could be asked as shown in Table 20. These questions correspond to the ENISA recommendations see Section 3.2.2). We link these recommendations to the SCORE meta-model concepts (see Figure 3 and Figure 4) and this is highlighted in bold in the questions presented in Table 20. The examples given for each question, are realistic examples taken from the TIG pilot case (see Section 6.3).

In the process outlined in Figure 5, phase 1 corresponds to the recommended ENISA step 1 'defining the processing operation and its context' (see Section 3.2.2.1); phase 2 corresponds to steps 2 and 3 of ENISA, 'understanding and evaluating impact' (see Section 3.2.2.2) and 'defining the likelihood of threats' (see Section 3.2.2.3). Evaluating risk, depends on multiple factors, self-assessed or otherwise evaluated, and will be an integral part of the SENTINEL digital framework implementation (as defined in work packages WP3, WP4 of the DoA). Phases 3 and 4 are about

designing a new situation. We specify a set of transformed capabilities incorporating appropriate technical and organisational measures in order to satisfy the change goals for mitigating risks identified in phase 2.

Table 20. SCORE process questionnaire

<b>1. IDENTIFY CURRENT SITUATION</b>
<p>1.1. What are the existing enterprise capabilities (<b>current capability</b>)? [e.g., data sharing]</p> <p>1.2. Which are the current goals that are met by these capabilities (<b>current business goal</b>)? [e.g., to ensure sharing of information between TIG and local agencies]</p> <p>1.3. What data processing <b>tasks</b> are done, identifying related <b>active and passive assets</b> and their dependencies (<b>asset</b> and <b>collaboration</b>)? [e.g., Staff uploads service user data using Microsoft OneDrive, Google Workspace, Dropbox]</p>
<b>2. ANALYSE RISK</b>
<p>2.1. Which <b>capability</b> is threatened? [e.g., data sharing]</p> <p>2.2. Which <b>asset(s)</b> (if any) of the above capability is <b>vulnerable</b>? [e.g., TIG Staff are unaware of privacy and therefore possibly vulnerable]</p> <p>2.2.1. Is the threatened asset <b>sensitive</b> with respect to PDP (Y/N)?</p> <p>2.2.2. What is the <b>perceived threat</b> (name)? [e.g., data breach]</p> <p>2.2.3. What is the <b>occurrence probability</b> for the threat (high/medium/low)?</p> <p>2.2.4. What is the <b>degree</b> of the likely <b>impact</b> (high/medium/low)?</p> <p>2.2.5. What is the <b>type</b> of the likely <b>impact</b> (security/privacy/both)?</p> <p>2.3. Which <b>asset collaboration</b> (if any) of the above capability is <b>vulnerable</b>? [e.g., uploading of service user data on External ICT Systems by TIG Staff has the vulnerability of connecting to unprotected network]</p> <p>2.3.1. What is the <b>perceived threat</b> (name)? [e.g., over dependency on the Cloud for service provision]</p> <p>2.3.2. What is the <b>occurrence probability</b> for the threat (high/medium/low)?</p> <p>2.3.3. What is the <b>degree</b> of the likely <b>impact</b> (high/medium/low)?</p> <p>2.3.4. What is the <b>type</b> of the likely <b>impact</b> (security/privacy/both)?</p>
<b>3. DESIGN FUTURE SITUATION</b>
<p>3.1. What are the new goals to ameliorate the threat (<b>change goal</b>)? [e.g., improve security of information sharing]</p> <p>3.2. What <b>protecting assets</b> are required in the transformed <b>desired capabilities</b> to satisfy the <b>change goals</b>? [e.g., policy enforcement]</p>
<b>4. ASSESS SATISFIABILITY OF CHANGE GOALS</b>
<p>4.1. What is the type and level of mitigation for the perceived threat of the desired capability to satisfy the change goal (<b>mitigation type, mitigation level</b>)? [e.g., the policy enforcement capability satisfying the change goal of improving security of information sharing, provides a high level of response against the threat of dependency on the cloud provider]</p> <p>4.2. Is the mitigation level satisfactory? If YES proceed to implementing the CS for privacy strategy.</p>

If NO return to phase 3.

- 4.3. Continue to the detailed specification of desired capabilities? If YES then implement the strategy by modelling actor dependency and informational objects that correspond to the desired capabilities which in turn meet the change goals.

To facilitate the process a number of key questions could be asked as shown in Table 20. These questions are aligned with ENISA's guidelines for SMEs see Section 3.2.2). We link these guidelines to the SCORE meta-model concepts (see Figure 3 and Figure 4) and this is highlighted in bold in the questions presented in Table 20. The examples given for each question, are realistic examples taken from the TIG pilot case (see Section 6.3).

It should be noted that in the final step (4) shown in Table 20, the requirements identified therein will be dealt with by the envisaged functionality of the SENTINEL framework which will be considered in deliverable D1.2 (The SENTINEL Technical Architecture).

## 5.4 Summary: SENTINEL RE methodology

Section 5 introduced the SENTINEL RE methodology, presenting its conceptual foundations and its way of working. The aim was to develop an innovative methodology dedicated to capturing and analysing requirements of SMEs for CS for privacy. To this end, it was considered vital that the methodology is not simply a set of questions that need to be answered by SME stakeholders, as found in the literature, but rather an innovative, systematic, stepwise way of working that is based on well-founded conceptual principles. The way of working is presented in Section 5.3 whereas the conceptual foundation is found in Section 5.2. These two represent an *orthogonal* way of considering SCORE where one dimension is that of 'the process' and the other 'the product'. The process dimension considers the steps that need to be followed and the product dimension considers the models that need to be used within each step.

Whilst it may be desirable to present the theoretical aspects of the methodology, it is also necessary to demonstrate the usability of the methodology and its relevance to real life cases. Therefore, we applied SCORE on the two pilot cases chosen for SENTINEL, to demonstrate both the 'process' and the 'product' dimensions. This work is presented in Section 6.

# 6 Demonstrating the use of SCORE on the pilot cases

## 6.1 Introduction

The following sections demonstrate the applicability of the SCORE methodology, described in Section 5, to the two pilot cases defined in the DoA. Please note that the analysis is not exhaustive at this stage. A detailed analysis of the requirements of the two pilot cases will be performed in WP6. Nevertheless, this section serves as the means of explaining, with modelling examples, the way that SCORE provides added value to SMEs in considering their CS and PDP requirements, as well as serving as a proof of concept for the methodology.

For each pilot case, there is a dedicated section on describing briefly the business setting as a way of providing an understanding of the context of the SCORE application. This is followed by a description of the step by step process defined in Section 5.3, using the graphical notation shown

in Section 5.2.2. The models produced were for both current and desired situations, clearly demonstrating the requirements for change.

## 6.2 The business cases

### 6.2.1 TIG pilot needs

#### 6.2.1.1 Company summary and business sector

Tristone Investment Group (TIG) is an independent investment company committed to the acquisition and growth of established, social care organisations that deliver positive social impact. Specifically, TIG is focused upon delivering exemplary standards of care, support and education to children, young people, and vulnerable adults. TIG has been founded upon the principles of Ethical Capitalism being passionate about the notion that sustainable commercial success can, and should, align with positive social impact.

All businesses within the group have a high degree of autonomy, covering a range of services and specialisms, all of which operate within specific conditions of important legislative and regulatory frameworks, as well as established models of service delivery. Each business is provided with support, guidance, recommendations, and insights into good practice conditions of operation, creativity, and innovation. For the needs of the SENTINEL project, one of the businesses in TIG which is used for the purpose of demonstrating the SCORE methodology is that of “Juventas”.

#### 6.2.1.2 Business context

The *vision* of TIG is “to invest in great businesses to which they can add value through organic growth initiatives, acquisitions, and operational and strategic investments”. With specific reference to the social care businesses the TIG *mission* is “to deliver positive social change through the alignment of commercial returns with social impact”. Table 21 provides an overview of the scope of TIG businesses and the social care sectors within which they operate.

Table 21. Overview of TIG businesses

Business Name	Social Care Sector					
	Supported Accommodation for Young People (16-25 years)  (Unregulated, as well as CQC and CIW Regulated depending upon context of setting)	Supported Accommodation  Unaccompanied Asylum-Seeking Children (UASC)	Supported Accommodation for Vulnerable Adults (18+)  (CQC and CIW Regulated)	Residential Children's Homes  (Ofsted Regulated)	Independent Fostering Agencies  (Ofsted Regulated)	Care settings for vulnerable adults and young people  (CQC and CIW Regulated)
CFS Care Ltd.	✓				✓	
Dimensions Care Ltd.				✓		
Juventas Services Ltd.	✓	✓		✓		
Premier Care Management	✓					
ProCare Wales			✓			✓
Sportfit Ltd.	✓					

### 6.2.1.3 CS challenges

#### Types of data

Table 22 provides an overview of data processing and retention needs aligned to social care businesses. All data stored is sensitive and must be stored securely to maintain variable conditions of privacy and confidentiality.

Table 22. TIG types of data

Data Access Requirements	Non-Sensitive Data	Sensitive Data	Processing (need)	Retention (need)
Service Users (per setting/ service only)	YES	YES	YES	YES
Employees (Operational) (HR/ Management only)	YES	YES	YES	YES
Employees (Non-Operational)	YES	YES (NEED TO KNOW)	YES	NO

Depending upon the circumstances, the above data must be shared with designated employees (only) of commissioning authorities, regulators (sector specific) and auditors subject to formal Non-Disclosure Agreements.

#### Challenges

Social Care in the United Kingdom is complex and challenging. This is reflected not only on day-to-day operational factors, but also in terms of the plethora of legislative and regulatory requirements that must be consistently met and exceeded to achieve sustainable excellence. The *service users* must remain at forefront of TIG concerns, regarding the duty to promote and maintain their welfare. Broadly speaking, this is aligned with safeguarding and ensuring the continued wellbeing of all service users. Additionally, TIG have a duty of care to employees that is underpinned by a variety of regulatory and legislative requirements. Furthermore, within every aspect of practice, TIG must ensure compliance with the GDPR.

Within GDPR, TIG must remain alert to risks associated with CS breaches and the need to mitigate and, as far as possible, eliminate or negate those risks.

Unlike many SMEs, TIG do not face the challenges associated with online transactions. This is because TIG customers are local government commissioning bodies and remuneration is facilitated directly, through BACS for example. However, there are a range of CS risks that have specific financial and operational connotations. Of particular concern, is the possibility that data required to meet the needs of a service user is locked and essential information regarding their care and support is blocked. This has the potential to be more than just a service interruption, as it has the potential to result in harm to the service user/s. A primary example can be summarised as data/digital blackmail. Ransomware and malware ‘families’ present an increasingly significant concern, and TIG – like all providers within the world of social care – rely upon a range of systems to manage day-to-day information sharing, recording and data retention. Some of these systems are more robust than others. Should, for example, a provider falls foul of ransomware such as WannaCry, it would not only present a risk to service users, there would naturally be a significant financial cost to unlock or decrypt systems in order to use them again.



Presently, TIG relies upon training their employees in data protection and CS, of which the latter seeks to inform them of essential warnings and indicators (such as ‘mousing over’ a URL or checking an email address for irregularities). TIG routinely use ICT to assess any vulnerabilities and employees are routinely presented with hoax malware that is designed to keep them alert. Additionally, it allows monitoring of employee competencies regarding potential threats.

Despite the use of systems and processes that aim to counter the threats consistent with ransomware and malware, TIG know that they remain at risk. Ransomware and malware variants evolve all the time and become ever more sophisticated. Systems and measures to mitigate associated risks are often on the back foot and work upon responses to existing threats, rather than focusing upon pre-emptive security measures that go beyond a good quality security system, for example.

In summary, the most acute CS threats are likely to come in the form of ransomware and malware attacks. These can result in significant ruptures to day-to-day operations and at its most extreme, could result in potential harm to a service user. The emphasis is therefore placed upon a need to build robust, fluid and dynamically changing CS systems that have the capacity to block threats and equally, to ensure that employees have the knowledge and skills required to avoid falling into ever-evolving security hazards such as ransomware and malware variants.

## 6.2.2 CG pilot needs

### 6.2.2.1 *Company summary and business sector*

ClinGenics (UK) Ltd (CG) is a UK company founded in late 2016, with the aim of advancing patient care and support through the development and provision of state-of-the art decision-support and cutting-edge solutions in Genomic Medicine for physicians and patients.

CG’s decision-support solutions, carefully developed and clinically evaluated over several years in hundreds of patient cases, address the complexities associated with genomic variant interpretation and new important challenges in the clinical interpretation of DNA variants associated with genetic diseases, offering a very powerful variant interpretation tool, aiding decisively in the diagnosis of hundreds of complex and rare disorders. The final variant interpretation report provided by CG has the added important feature of incorporating expert manual curation, personalized interpretation and case-specific comments and suggestions for further actions, thus fulfilling its role as a true decision support tool.

### 6.2.2.2 *Business context*

CG’s work is based on EMA - Exome Management Application: a bioinformatics platform-software pipeline, coupled to expert curation for the evaluation and reporting of actionable genomic variants. The EMA pipeline software currently provides the following types of variant data interpretation services: (a) Whole Exome Sequencing Trio (WES-trio) parents and proband variant interpretation; (b) Whole Exome Sequencing (WES) single proband variant interpretation; (c) Multi-gene NGS panel (50-150 genes) exome sequencing variant interpretation; (d) Multi-gene NGS panel (1-49 genes) exome sequencing variant interpretation; (e) BRCA1 and BRCA2 genes NGS panel exome sequencing variant interpretation; and (f) CFTR gene NGS sequencing variant interpretation.

For large scale projects or other research applications, a dedicated custom variant analysis is also available upon request, for generating population-specific common variant database(s). The same type of custom variant analysis may also be performed and may be useful for identifying common disease-related variants in multiple samples (disease cohorts). The results are made available as a database in SQL file format or custom report may be generated.

Briefly, as a first step, the user must create an account and become a registered user through the 'Create an account – login' function on the CG web site. As the services provided through the CG EMA pipeline software are intended exclusively for clinicians and genetics professionals, CG reserves the right to deny the creation of an account by a user who does not fulfil the necessary requirements. The user must then upload raw un-annotated VCF file(s) (version 4.0 or later), which are then annotated through a custom annotation pipeline. The user must also complete all the required standardized clinical information in the provided Data Submission Form (anonymised, without any patient identifiers). To further ensure data anonymization, upon upload, all data files are automatically assigned a randomly generated file name containing a unique timestamp. The submitted un-annotated vcf file is annotated using a customized annotation workflow and is subsequently imported into the CG EMA pipeline database. Duplicate variants are removed and variants are initially filtered and prioritized based on several parameters constantly updated and maintained in the EMA EMAVAR pipeline database, such as: (a) variant population frequency derived from 3 different population databases; (b) NGS platform-specific known recurrent variant calling artifacts (known false-positives related to the specific sequencing platform, derived from >800 whole exome sequencing samples maintained in the EMA database). Remaining variants are further prioritized through the EMA Disease Relevance (EMADR) pipeline module, based on the reported disease phenotypes and other relevant clinical information supplied by the submitting physician; and (c) novel variants, not previously reported in affected individuals, are assigned a EMAPathScore, derived through a built-in multi-parametric in silico pathogenicity score prediction algorithm. As a final step, remaining variants are curated by the ClinGenics team based on expert clinical knowledge and according to published guidelines (ACMG-AMP guidelines). Upon completion of variant interpretation analysis, the user is notified by email and is then able to login securely and retrieve-download the final variant interpretation report(s) and accompanying supporting data files. The original vcf data file(s) submitted for analysis may then be deleted.

CG also exploits NGS-PanelBuilder: a user-friendly tool for building phenotype-driven and/or disease-driven multi-gene NGS panels. A highly flexible solution for targeted NGS applications, from sequencing to variant interpretation (in its final stages of development).

#### 6.2.2.3 CS challenges

### Types of data

The types of anonymous data submitted by the users and maintained by CG include:

1. Human DNA sequence variants, in vcf file format (Variant Call Format, see <https://github.com/samtools/hts-specs>) generated typically by Next Generation Sequencing (NGS) applications and submitted by the users for variant prioritization and interpretation.
2. Standardized, in Human Phenotype Ontology - HPO format, phenotype and disease related information related to and accompanying the specific co-submitted vcf data file (see above).

3. Simple anonymous pro-band demographic data, such as gender, age, ethnicity, disease status (affected or not) and relevant disease inheritance information.
4. Technical/experimental data, relating to the type of NGS analysis, platform utilized, etc.

In addition, CG maintains an internal database containing user/customer-related information submitted during registration, such as name, occupation, institution/affiliation, telephone and email, for obvious administrative purposes.

A significant amount of supporting data maintained in the CG EMA pipeline database comprise variant population frequency data (mostly from public databases, e.g., gnomAD, 1000GP, etc.), human gene-specific data (e.g., disease phenotype and inheritance related data from OMIM and other sources) as well as pre-defined and calculated variant pathogenicity scores, derived through the built-in algorithms in the EMA pipeline.

In terms of data sensitivity and privacy, all pro-band/patient related data submitted by the users (see 1-4 above) are totally anonymous, without any type of personal identifiers. Furthermore, issues regarding data privacy and data anonymization are stated clearly in the Privacy Policy of the CG GDPR-compliant website as well as the Statement and the Terms of Use – Limitations and Conditions sections of the EMA pipeline description.

## Challenges

Although all pro-band/patient related data submitted by the users (see 1-4 above) are totally anonymous, without any type of personal identifiers, bearing in mind that genomic sequence data constitute sensitive personal data per se<sup>9</sup>, CG is anxious and concerned in terms of having further layers of security regarding the access of data stored in the pro-band database module of the EMA pipeline. As CG do not wish to rely solely on anonymization, they envisage implementing extra security measures, for example a more secure user login process, scanning for the presence of any personally identifiable information (PII) during the submission process, specific cyber security protection of all stored data, etc. and to generally put in place appropriated systems that limit any type of unauthorized access to the data.

## 6.3 Application of SCORE to the TIG case

This section describes the initial application of the SCORE methodology to the TIG case, following a Goal-oriented way-of-working (see Section 5.3). As mentioned in Section 6.2.1, for demonstration purposes we focus on one of TIG businesses namely that of “Juventas”.

The models presented in this section, represent the analysis of the information gathered from TIG using appropriate questionnaires (see Appendix II) as well as virtual meetings between TIG personnel and requirements engineers. The aim is not to build exhaustive and detailed models of TIG’s situation, but rather to make sure that the models built are indeed able to capture all the information required to express this situation (something that will be carried out in detail in WP6). Furthermore, the models can be used as a way of ‘proof of concept’ for SCORE and also as exemplars of the use of the methodology.

---

<sup>9</sup> GDPR, Recital 34

### 6.3.1 Identify TIG Current Situation

Following the goal-oriented way of working, we start by identifying the current TIG objectives and how these are met by current capabilities (TIG current Goal Model in Section 6.3.1.1). The structure of current capabilities is further described in the TIG current Capability Model (see Section 6.3.1.2), whilst the realisation of these capabilities is further detailed in the TIG current Actor Dependencies model (in Section 6.3.1.3).

#### 6.3.1.1 TIG Current Goals

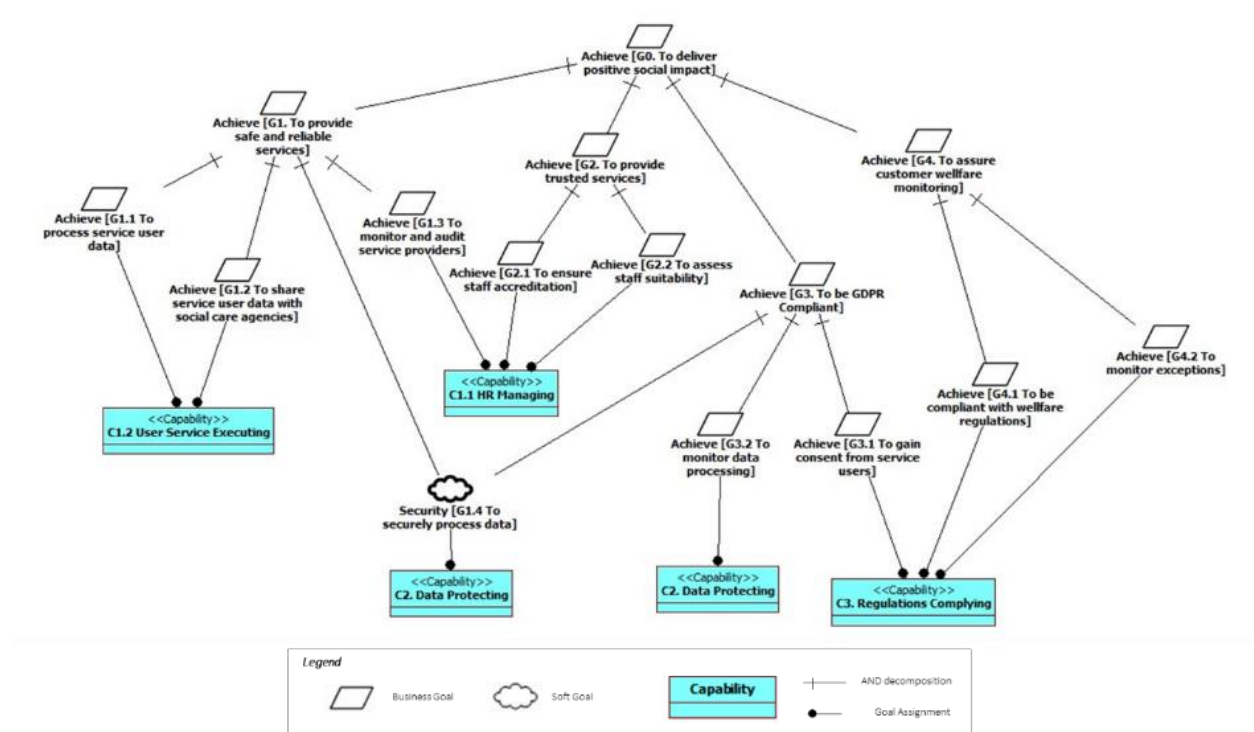


Figure 6. TIG current goals and related capabilities

Figure 6 illustrates the objectives of TIG (*the why*) as they pertain to the current setup, starting from a high-level vision and then gradually identifying the causal relationships of goals of increasing detail. The leaf operational goals are related to current capabilities through which TIG realises its objectives.

In particular, the strategic objective of TIG is “G0. To deliver positive social impact”. To achieve this TIG, should achieve four sub-goals namely, “G1. To provide safe and reliable services”, “G2. To provide trusted services”, “G3. To be GDPR Compliant” and “G4. To assure customer welfare monitoring”. The AND relationship between the top-level goal and the four sub-goals means that the achievement of the four sub-goals is sufficient to ensure the satisfaction of the strategic TIG objective.

However, these sub-goals are still too general providing little information about the way these are operationalized. Goal operationalization encompasses its ‘causal transformation’ into more concrete sub-goals that constitute the means of achieving desired ends. Each step can result in the identification of new sub-goals (more focused and often smaller in scope) that are linked to

the original one through causal relations thus forming a hierarchy of goals. The aim of the operationalization is to reach a level of detail whereby each leaf goal can be met by specific enterprise capabilities, depicted at the lowest level of the hierarchy of Figure 6. For example, the operational goal “G1.3 To monitor and audit service providers” is realised by capability “C1.1 HR Managing”.

Related to G1 is the security soft goal “To securely process data”. Soft goals are often characterised by subjectivity, in the sense that there is no clear-cut, or agreed a-priori, criterion about what constitutes the achievement of that goal. However, soft goals are important in motivating the analysis and evaluation of CS and privacy related enterprise capabilities.

### 6.3.1.2 TIG Current Capabilities

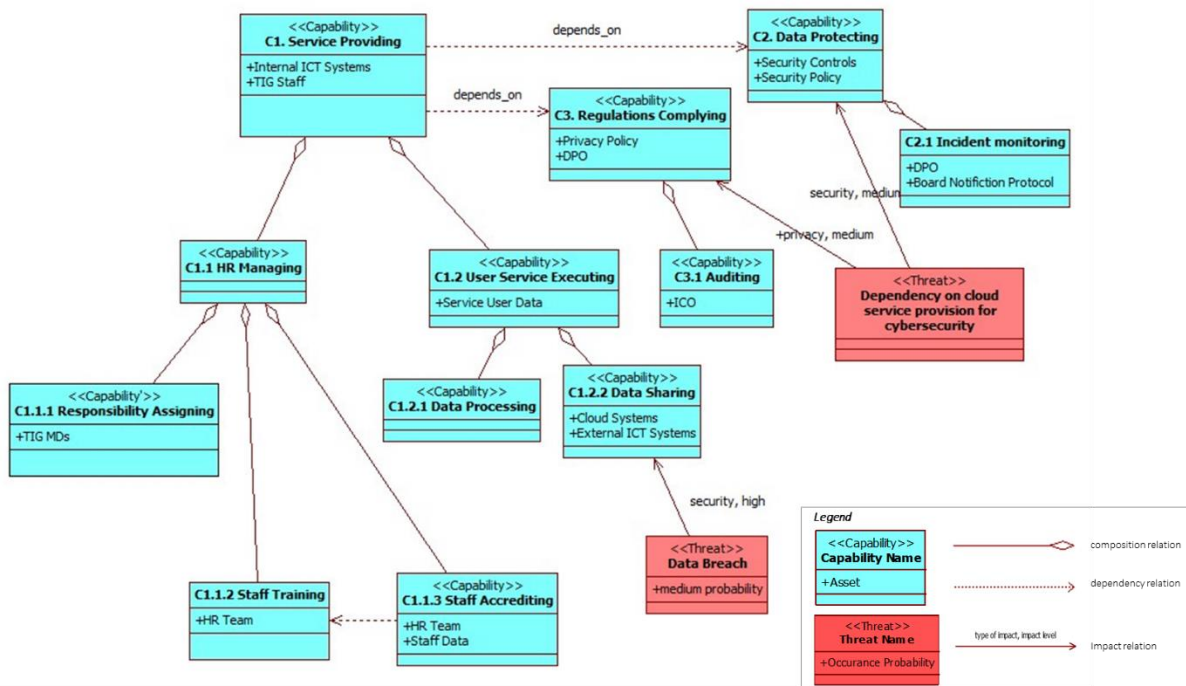


Figure 7. TIG current capabilities and perceived threats

The current Capabilities Model shown in Figure 7, expresses the current TIG capabilities (**the what**) at a business level. Capabilities may be composed of other capabilities in order for them to achieve their objective. For example, capability “C1.1 HR Managing” is composed of capabilities “C1.1.1, Responsibility Assigning”, “C1.1.2 Staff Training” and “C1.1.3 Staff Accrediting”. Also, capabilities may be dependent on other capabilities. For example, capability “C1. Service Providing” depends on capabilities “C2. Data Protecting” and “C3. Regulations Complying”.

The different assets that make up each capability are also shown. For example, capability “C1.2.2 Data Sharing” encapsulates two types of assets (automated systems) “Cloud Systems” and “External ICT Systems”.

This model also expresses the perceived threats on enterprise capabilities. For example, “Data Breach” is a threat that can affect capability “C1.2.2 Data Sharing”. The occurrence probability



of each threat as well as the type and level of perceived impact on the capabilities is also defined. For example, “Data Breach” highly impacts the security of “C1.2.2 Data Sharing” having a medium occurrence probability. This information will be used during risk analysis in calculating current CS and privacy risks (as described in Section 6.3.2).

### 6.3.1.3 TIG Current Actor Dependencies

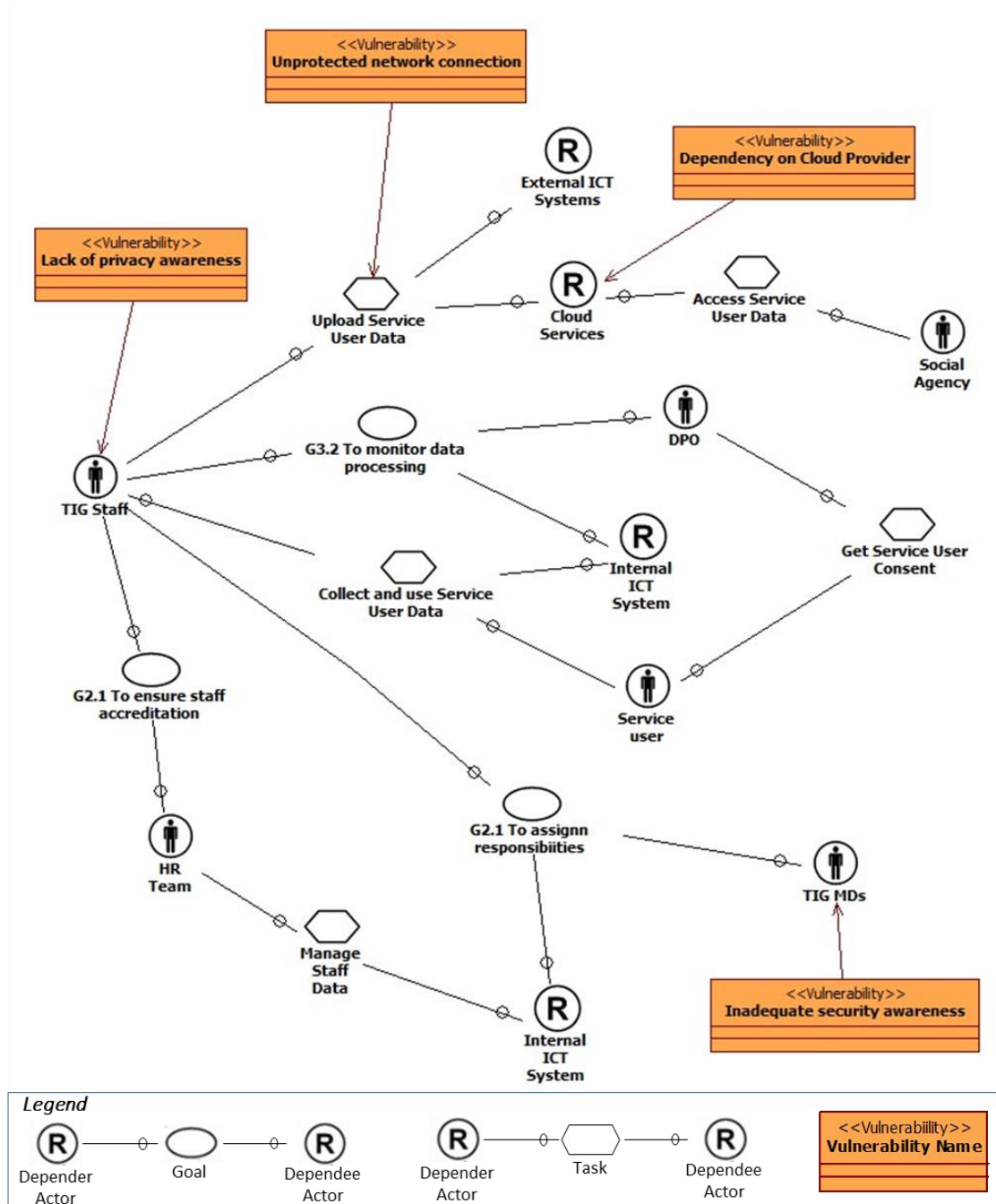


Figure 8. Current TIG actors and their dependencies and potential vulnerabilities



The Actor Dependencies Model shown in Figure 8, expresses the collaboration between TIG actors in order to realize its capabilities (*the how*). This collaboration is expressed as dependencies between actors over the achievement of some goal or the execution of some task or the availability of some resource. As can be seen in Figure 8, there is a complex relationship between TIG actors in order for them to realise their role. For example, “TIG Staff” depends on the “Cloud Services” system in order to realise the task of “Uploading Service User Data”. At the same time the “Social Agency” actor depends on the same system for the task of “Accessing Service User Data”.

In addition, to the enterprise actor collaboration this model expresses the perceived vulnerabilities (pertaining to actors or their collaboration) which are weaknesses that threats may take advantage of. For example, “Unprotected network connection” is a vulnerability pertaining to the collaboration between the “TIG Staff” and “Cloud Services” actor which can be exploited by the “Data Breach” threat. Also, the “Lack of privacy awareness” is a vulnerability pertaining to “TIG Staff” actor which could also be exploited by the “Data Breach” threat.

This analysis is important for assigning the threat occurrence capability in the current Capability Model, described in Section 6.3.1.2.

#### 6.3.1.4 TIG Informational Model

The informational model depicted in Figure 9, provides an abstract description of the data that is controlled and processed by TIG businesses. This model further details the passive assets that are depicted in the TIG capability model (e.g., “Service User Data”, “Staff Data”) also guiding the identification of sensitive data types (e.g., “Employee – Supervision record”).

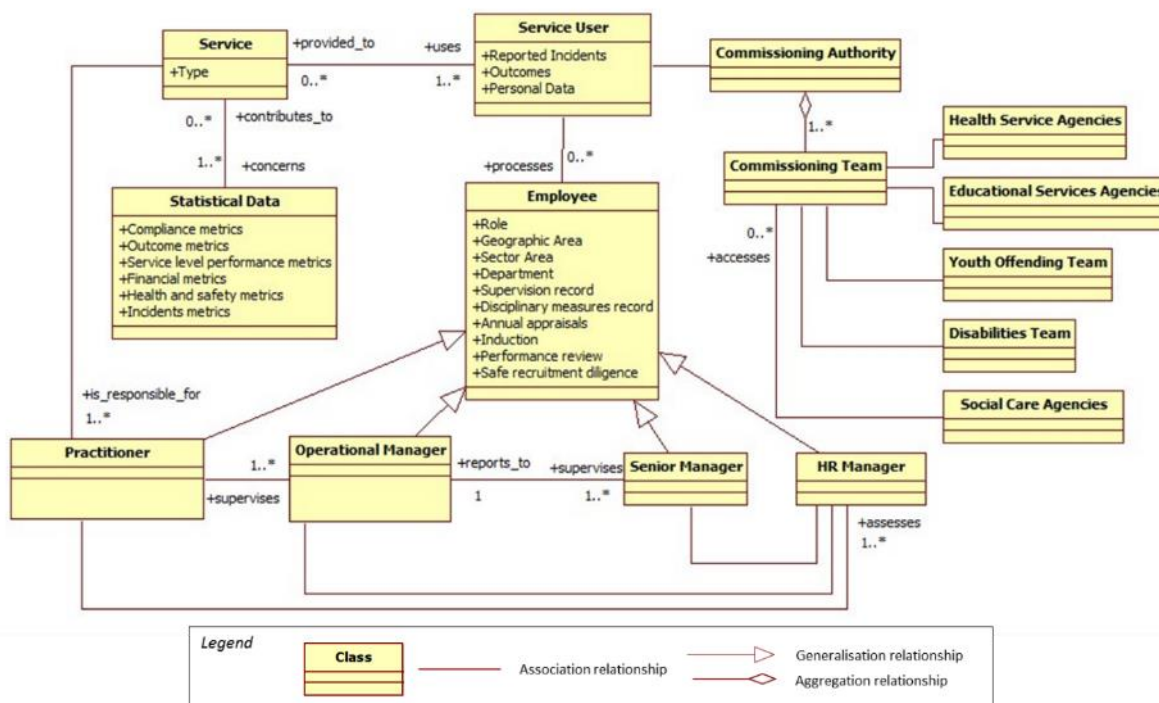


Figure 9. TIG informational model

### 6.3.2 Risk analysis

Risk analysis aims to ascertain the current CS and privacy related risk, based on the identified threats noted in the capability model. In particular, the analysis is based on: (a) the occurrence probability of each threat which is calculated based on relevant vulnerabilities pertaining to related assets and their collaboration (described in the actor dependencies model), as well as the sensitivity of relevant data (described in the informational model); and (b) the level of impact of the threat (high, medium, low) on the affected capability (described in the capability model).

This analysis is assisted by a set of relevant questions (see phase 2 questions of the SCORE questionnaire in Table 20). Answering these questions is guided by the inter-model relationships as shown in Figure 10 which presents the TIG models of the current situation. For clarity purposes we have included only excerpts of the models, which were presented in their entirety in Section 6.3.1.

As can be seen in Figure 10, the capability “C1.2.2 Data Sharing” is affected by the “Data Breach” threat. This threat exploits several vulnerabilities that pertain to the assets related to this capability and their collaboration, as shown in the actor-dependency model. Furthermore, as can be seen in the informational model the “Service User Data” involved in the data sharing include personal and therefore sensitive data. Understanding such vulnerabilities is an important step towards risk analysis as it helps us to assess the likelihood and impact of the “Data Breach” threat. In particular, TIG stakeholders have concluded that the occurrence probability of the “Data Breach” threat is medium. At the same time its impact on “C1.2.2 Data Sharing” capability is high and therefore triggers the need for change.

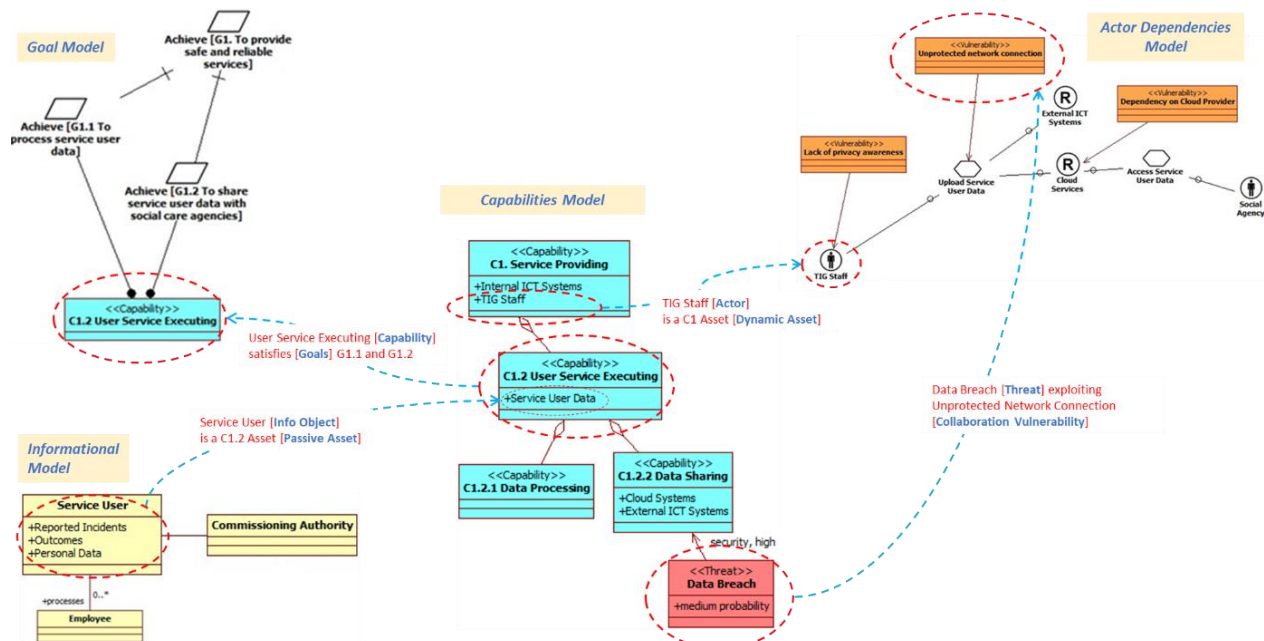


Figure 10. Inter-model relationships between TIG models of the current situation

Thus, risk analysis guides the identification of the new TIG (change) goals to ameliorate the threat, which in turn will guide the identification of the new (desired) capabilities to meet the change goals, as described in section 6.3.3.2).

### 6.3.3 Design TIG Future Situation

The desired situation uses the same set of models but from a different viewpoint, namely that of the requirements for change of TIG for improving CS and privacy. Specifically, we aim to express how the desired situation might ameliorate the risks identified in the current situation, as a result of the identified threats.

#### 6.3.3.1 TIG Change Goals

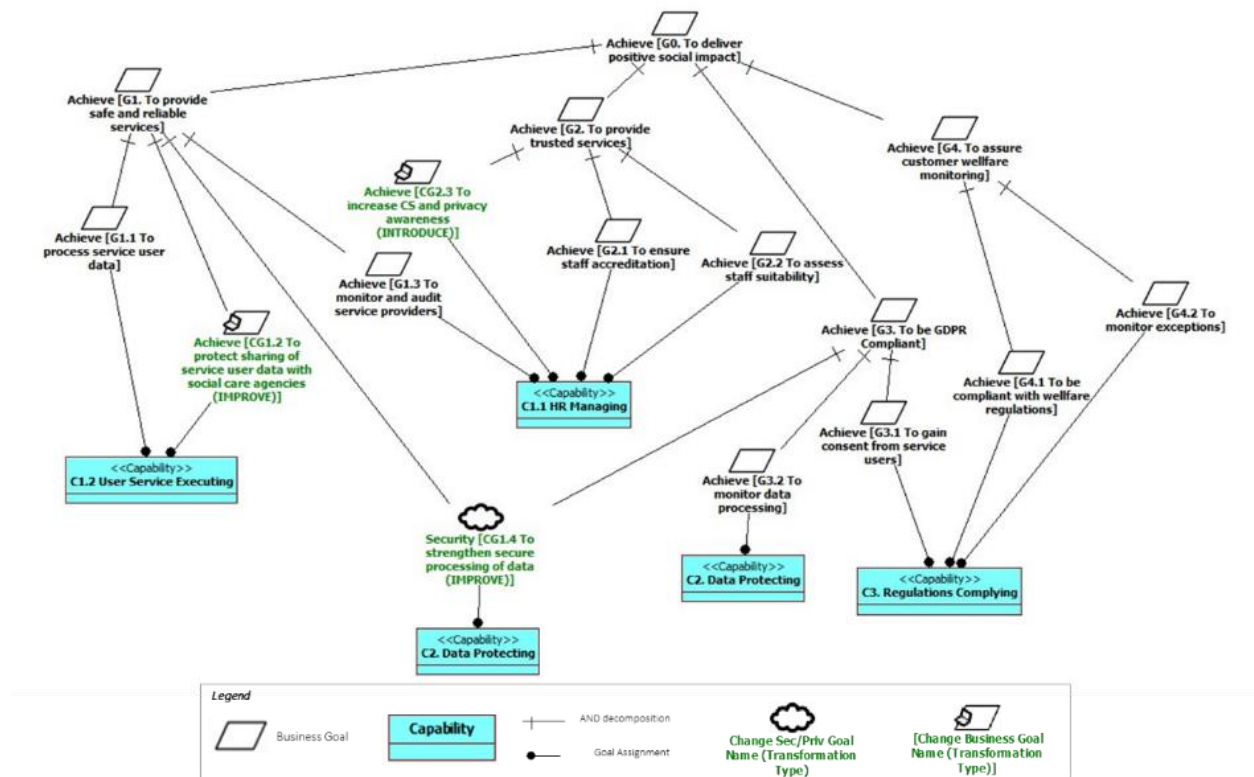


Figure 11. TIG change goals

The Change Goal Model of Figure 11, seeks to show how TIG can progress from current goals to change goals. In particular, starting from affected capabilities in the current capability model we identify relevant goals in the current goal model and try to identify change goals either as improvements of the current goals or by introducing new goals, thus modifying the current goal hierarchy to reflect these changes. The final step is to re-assign operational goals to existing or foreseen enterprise capabilities (envisioned SENTINEL components).

For example, the fact that the “Data Breach” threat affects the “C1.2 User Executing Capability” motivates the introduction of the new goal “To protect sharing of service user data with social care agencies” as a sub-goal of the relevant goal G1. Similarly, the “Dependency on cloud service provision for cybersecurity” motivates the improvement of the relevant security goal “To strengthen secure processing of data”.

In defining these new goals, we have also defined the current capabilities that are affected by them (C1.2 and C2). In other cases, this might require a completely new capability.



### 6.3.4 Assess Satisfiability of Change Goals

The aim of phase 4 is to evaluate to what degree the change goals may be satisfied. In particular, it involves the assessment of the type and level of mitigation for the perceived threat of the desired capability to satisfy the change goal.

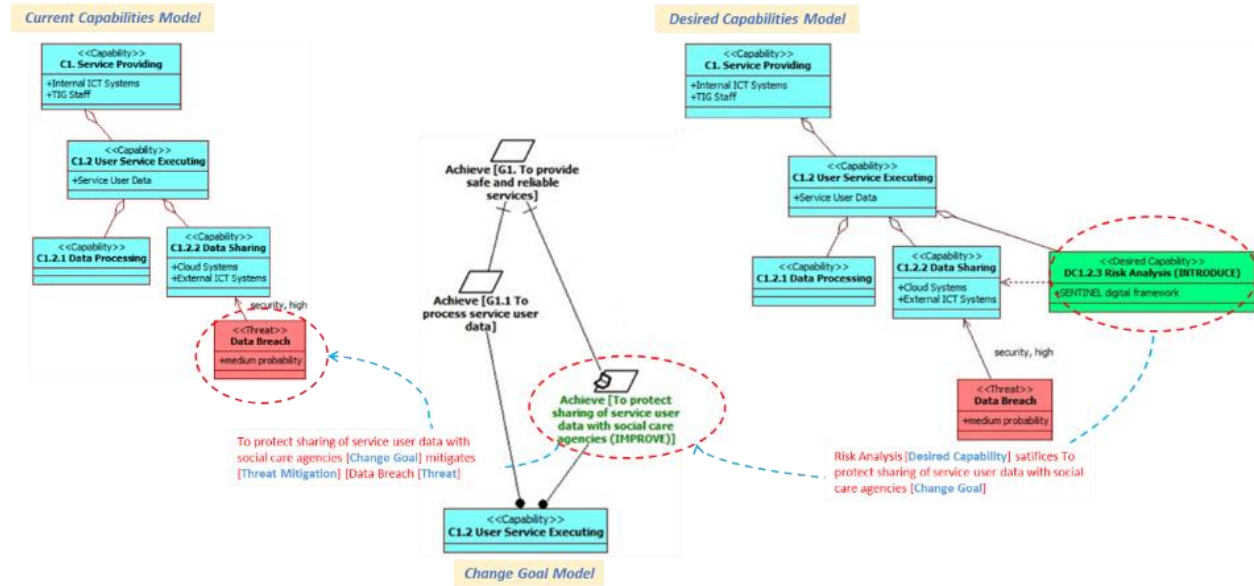


Figure 13. Tracing threat mitigation

This type of analysis is guided by the semantic relationships between the different SCORE modelling concepts as shown in the example of Figure 13. As can be seen in Figure 13, the desired capability “C1.2.3 Risk Analysis” satisfying the change goal of “To protect sharing of service user data with social care agencies”, thus providing a high level of response to the threat of “Data Breach”, which is considered by the TIG stakeholders to be satisfactory.

## 6.4 Application of SCORE to the CG case

This section demonstrates the application of SCORE to the CG case, based on the information gathered from CG using appropriate questionnaires (see Appendix II) as well as virtual meetings between CG personnel and requirements engineers.

### 6.4.1 Identify CG Current Situation

In the case, the Capability-oriented way-of-working (see Section 5.3) is followed. Once again, the aim is not to present an exhaustive and detailed set of models of CG’s situation, but rather to demonstrate how the SCORE models are able to capture all the required information.

#### 6.4.1.1 CG Current Capabilities

The CG capabilities as described by CG stakeholders, are detailed in Figure 14. For each capability the set of current active and passive assets that realise it are shown. For example, “CG Expert Staff”, “Exome Management Application”, “Genomic variant data” are some of the assets pertaining to the “Genome Data Processing” capability. In addition, the relationships between these capabilities are also presented. For example, the “Service Providing” capability consists of the



“Genome Data Processing” capability and the “Customer Data Managing” capability. At the same time the “Service Providing” capability depends on the “Regulations Complying” capability. In addition, discussion with CG stakeholders lead to the inclusion of certain threats affecting these capabilities, namely “Privacy Breach” and “Data Breach”.

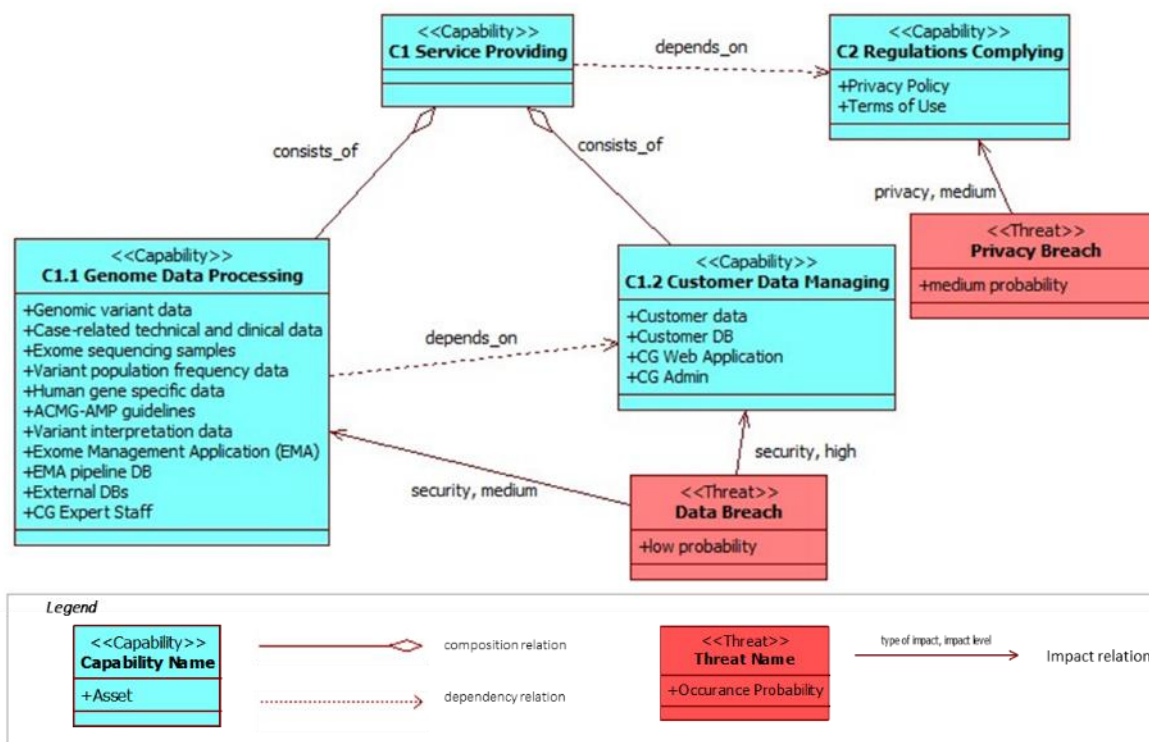


Figure 14. CG current capabilities and perceived threats

It is useful to note that some capabilities (e.g., “C1. Service Providing” and “C2. Regulations Complying” appear in both the TIG and CG cases, although their realisation might be completely different. However, this correspondence might assist us to identify ‘basic’ SME capabilities that can be used to generalise the findings if the pilot cases at a later stage.

#### 6.4.1.2 CG Current Goals

The analysis of the capabilities reveals also the purpose of their existence, which is documented in the goal model of Figure 15.

Tracing from capabilities to goals reveals a goal hierarchy that links each capability to detailed goals and from these detailed goals to a higher of goals depicting the teleology of CG business. In more detail, this bottom-up, teleological analysis reveals that the identified CG capabilities “C1.1 Genome Data Processing”, “C1.2 Customer Data Managing” and ‘C2 Regulation Complying”, achieve the operational goals of G1.1 – G3.1 depicted as leaf goals in Figure 15. These in turn, reveal to satisfy the higher-level goals “G1. To deliver secure services”, “G2. To deliver efficient services” and “G3. To be legally GDPR Compliant”, which ultimately satisfy overall current business goal of GC which is “G0. To deliver reliable services”.



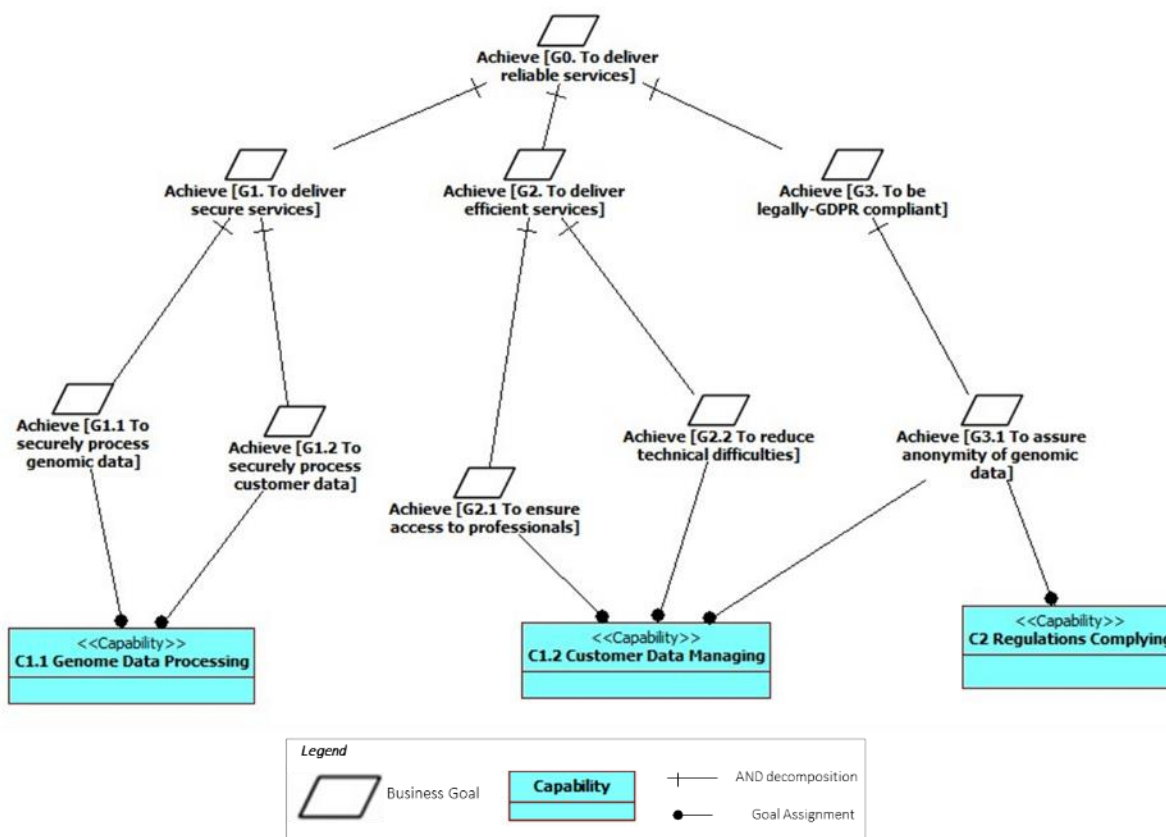


Figure 15. CG current goals and related capabilities

#### 6.4.1.3 CG Current Actor Dependencies

Figure 16, illustrates the CG actor dependency model. Central to this model is the “Exome Management Application” an important CG asset (software system) identified in the capabilities model (see the “C1.1 Genome Data Processing” capability in Figure 14). Other main actors involved are the “Genetics Professional” and the “CG Expert Staff”. Between these actors there is a network of task dependencies. For example, the “Genetics Professional” depends on the “Exome Management Application” in order to complete the tasks of “Uploading genome variant data”. At the same time the “Exome Management Application” depends on the “CG Expert Staff” for “Curating variants”.

The CG actor dependencies model assists the identification of vulnerabilities pertaining to either CG actors or their collaboration. For example, “Presence of PII data” has been identified by CG stakeholders as a vulnerability relating to the collaboration between the “Genetics Professional” and the “Exome Management Application” for completing the task of “Uploading genomic variant data”. Identifying vulnerabilities is important for estimating the occurrence probability of threats that exploit such vulnerabilities (for example, the “User’s privacy compromise” threat depicted in the current Capability Model (see Figure 14).

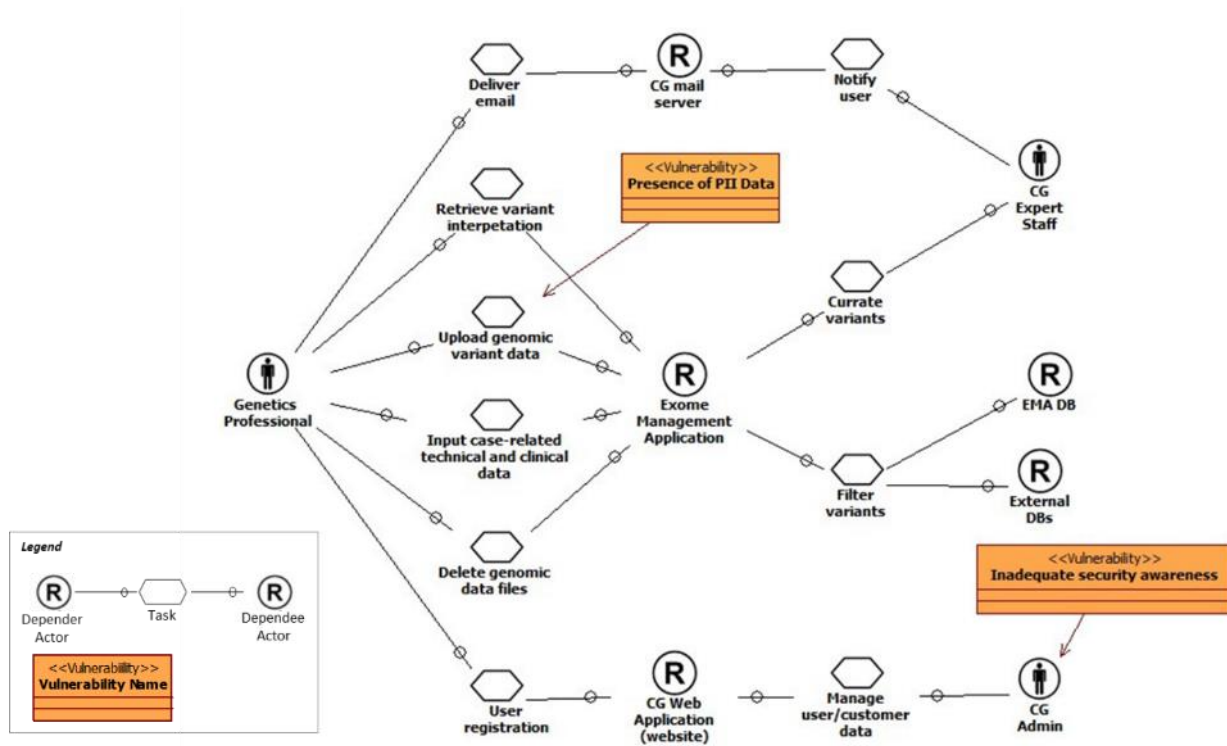


Figure 16. CG current actors and their dependencies and potential vulnerabilities

#### 6.4.1.4 CG Informational Model

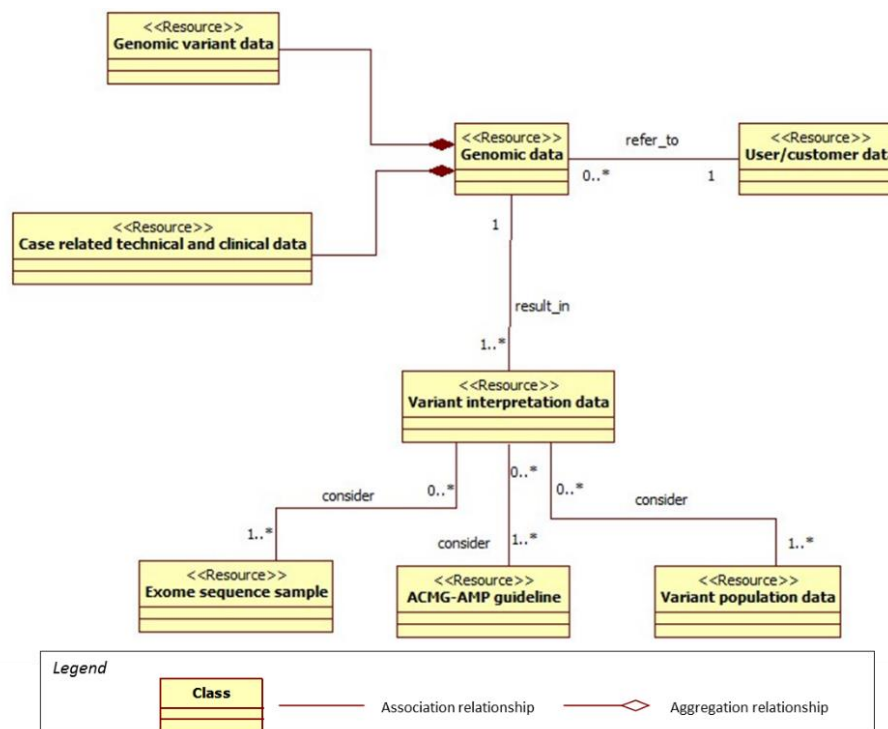


Figure 17. CG informational model

The CG informational model depicted in Figure 17, provides an abstract description of the type of information necessary for the enterprise actors to fulfil their roles. It elaborates the passive assets that are depicted in the capability model and can be used to assist identification of sensitive data.

## 6.4.2 Risk analysis

As in the TIG case the aim is to analyse the likelihood and impact of threats defined in the CG current capability model and use this analysis to define the change goals to ameliorate them.

## 6.4.3 Design CG Future Situation

The design of the future CG situation starts with the identification of the change goals aiming to address the perceived threats on current CG capabilities. This in turn leads to the transformation of CG's current capabilities by either improving existing capabilities or introducing new ones, in order to meet the change goals, as described in the following sections.

### 6.4.3.1 CG Change Goals

The CG change goal model (shown in Figure 18), includes the introduction of a new goal “CG1.3 Ensure data integrity” as well as the improvement of the current goal G3.1, namely goal “CG3.1 To improve anonymity assurance of genome data”. These two change goals, aim to ameliorate the “Data Breach”, and “Privacy Breach” threats compromising capabilities “C1. Service Providing” and “C2. Regulations Complying”, respectively.

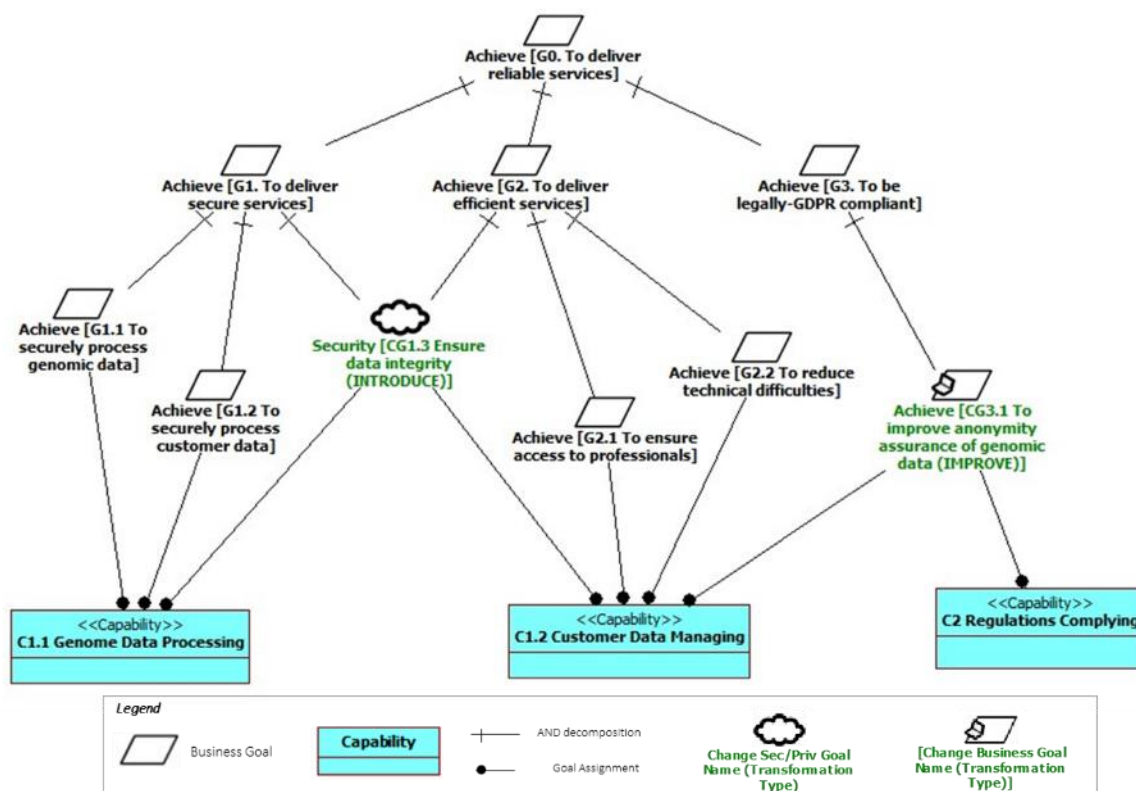


Figure 18. CG change goals

### 6.4.3.2 CG Desired Capabilities

The identified change goals trigger the introduction of two desired capabilities namely “DC1.3 Risk Analysis” and “DC2.1 Policy Enforcing” as shown in Figure 19. Both these capabilities encapsulate desired functionality of the SENTINEL digital platform which will be considered in deliverable D1.2 (‘The SENTINEL Technical Architecture’).

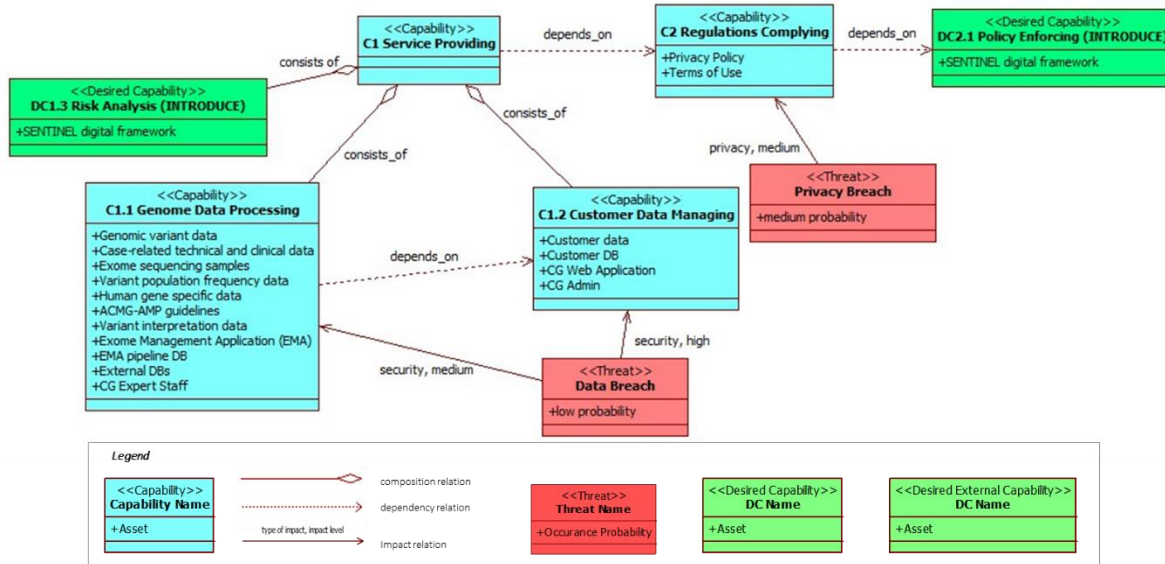


Figure 19. CG desired capabilities

### 6.4.3.3 Detailing the implementation of the CG Desired Capabilities

Implementation of desired capabilities will be based on the decisions made by CG with respect to the analysis in the previous sections. This might involve the specification of a new actor dependency model. Obviously, this is beyond the requirements stage and therefore not included in this report. However, it might be considered by CG when the full pilot case is implemented in Work Package 6.

### 6.4.4 Assess Satisfiability of Change Goals

The final phase of the SCORE process aims to assess whether the desired capabilities specified satisfy all change goals thus, mitigating perceived threats on current capabilities. As explained in Section 6.3.4 this analysis is guided through the propagation of the SCORE inter-model relationships.

## 6.5 Summary: A practical approach for eliciting user requirements

This section has sought to provide practical examples on the way that SCORE may be used by SMEs as a first step to identifying their requirements for CS for privacy prior to using the SENTINEL architecture. To this end, Sections 6.3 and 6.4 report on the SCORE way of working (defined in Section 5.3) as was applied on TIG and CG respectively. The models developed conform to the SCORE conceptual foundations (defined in Section 5.2).

Using the defined way of working the models were developed in a collaborative manner involving key personnel from the two pilot cases working with SCORE developers. This was done through (a) the use of questionnaires (see Appendix I) and (b) face to face meetings. The questionnaire provided a useful initial input to developing a first-cut set of models which were subsequently reviewed, revised and augmented with the collaboration of TIG and CG stakeholders. The use of the models was profoundly important in identifying the existing capabilities, the threats to these and the stakeholders' desires for improving these capabilities. The models provided a conceptually formal and practically useable way of ensuring that all necessary information was captured, that in turn would lead to the requirements for the use of the SENTINEL platform architecture.

Reflecting on the use of SCORE on the two pilot cases we can observe that the guidelines provided (see Section 5.3) in terms of the step-by-step use of the methodology were very clear to all participants in the modelling phases. All participants found the process well-founded in which the structured and systematic way of working made the process very definitive and speedy. The models themselves facilitated the exact, non-repeated and validated captured information that narratives in natural language could not offer. Participants with no knowledge of the SCORE notation were quick in understanding the underlying semantics of the methodology and were comfortable in using the models to review them and to suggest improvements to them.

Starting a requirements analysis process with a 'blank sheet' of paper is never easy nor is it recommended, irrespective of which methodology is used. In the case of SENTINEL, we suggest that a small amount of effort is required by modelling experts to begin the process and to 'walk through' the initial set of models with input from SME stakeholders. We found that the process can then be continued by SME stakeholders alone or with very little assistance, using appropriate modelling tools such as the one used in the two example cases or possibly an improved version to be integrated with the rest of the SENTINEL architecture (see part of the discussion in Section 7.2).

## 7 Conclusions

### 7.1 Reflections on objectives attained and related KPI

Data breaches cause massive losses to organizations. Smaller enterprises often do not possess advanced CS solutions to cope with an evolving threats landscape. Sophisticated cyberattacks can bypass traditional security systems. At the same time, we are witnessing a transition to Cloud-based services which, despite their profound value-for-money proposition for SMEs, come with opaque and pre-packaged CS provisions. As companies shift their focus to the Cloud, they face an intimidating range of options while in-house expertise and available financial resources are scarce. In today's complex infrastructures, there exist multiple endpoints, through which end users must access organizational data, including for processing customer and other personal data. Business applications have several accounts, regulations, and other diverse processes that make it difficult for cloud-based security solutions to maintain security and compliance. Today, this infrastructure is challenged by cyber threats, such as ransomware, trojans, phishing, malware, advanced persistent threats, and sophisticated attacks such as zero-day threats.

Commercial enterprise IT security solutions, available at a high cost, feature comprehensive CS, personal data protection and privacy assurance. However, they are, more often than not, beyond the capability of SMEs. On the other hand, free security options provide rudimentary protection at the endpoint level but leave what matters most for customers, sensitive personal data residing in web apps and other infrastructures, exposed.

The overarching aim of the SENTINEL project is to bridge the security and personal data protection gap for European SMEs, by raising awareness and boosting their capabilities in the domain through innovation, at a cost-effective level. Towards this end, WP1 has been designed to set the methodological scene for the project, in considering **end-user driven requirements and setting the methodological scene**. Within WP1, the first task, that of T1.1, had the mission of developing the *SENTINEL Requirements Engineering Methodology*. This document, reporting on the work carried out in producing deliverable D1.1, provides detailed explanations on the way this mission was realised. It does so in the following way. First, the challenges faced by SMEs are fully summarised as identified by standards organisations, by researchers and by practitioners. Second, the different approaches to meeting these challenges from both technological and methodological perspectives are described. Third, the components to be utilised, and further developed using the SENTINEL architecture are discussed. Fourth, the SENTINEL Requirements Engineering Methodology (SCORE) is reported upon, paying particular attention to advancing a user-centric viewpoint. Fifth, the usability and applicability of this methodology is demonstrated, using examples from the two pilot cases, both of which deal with extremely sensitive data of different nature.

In this report we discuss in detail the challenges faced by SMEs in terms of organisational awareness, financial exigencies, and technical know-how (see Section 2). As SMEs view their move from traditional IT solutions towards the Cloud, considered a financially beneficial shift from capital expenditure towards operational costs, this brings with it its own CS for privacy challenges. The critical areas affecting CS and for which management of SMEs need to be aware when adopting Cloud solutions, are presented at depth in this report. A valuable and practical output of this analysis is a summary included in this report of matching threats to Cloud concepts and



architectures. It is valuable to requirements stakeholders in understanding the critical areas in which they need to focus in order to address specific threats. It is also valuable to software and IT security engineers as background knowledge of threats to SME assets, when designing and implementing solutions to counter these threats.

The SENTINEL RE methodology, developed in task T1.1 and presented in this report, has been informed by the analysis on the challenges and needs (see Section 2) as well as by the analysis of approaches to managing risk (see Section 3). It is therefore, fully aligned with the overarching objective of considering *end-user driven requirements*. It is also fully aligned with the objective of *setting the methodological scene* which is done through its development (presented in Section 5, and demonstrated in Section 6), which represents an advance beyond current state-of-the-art in methodologies for CS for privacy specifically for SMEs.

According to the DoA a **key performance indicator** (KPI) for the work being reported in this deliverable is “*Innovative customized RE-related models deployed with respect to security- and data privacy-aware mechanisms ensuring data protection in SMEs/MEs [KR-2.1]*”. A discussion on the way that this KPI is met focuses on the methodology itself which represents a confluence of the different strands of the work presented in this deliverable. Specifically, the work is informed by (a) detailed analysis of generic and specific requirements for CS, (b) international standards and frameworks for assessing and managing risks, (c) other existing RE methodologies and (d) background knowledge and expertise on RE by SENTINEL participants.

In the RE literature there are a number of methodologies that attempt, in a variety of ways, to deal with the capture, analysis, and specification of user requirements relating to CS for privacy. The SCORE methodology, being developed exclusively for SENTINEL, provides the means by which SME users are able to engage into the requirements process by focusing on strategic issues, in a way that goes beyond the way that traditional methodologies deal with CS issues. Traditional RE methodologies for security fall mainly in two categories *risk-oriented* and *goal-oriented*.

In *risk-oriented* approaches, CS is defined as the protection of assets through the treatment of threats that put information at risk. Prominent amongst these approaches are those that are propagated by standardisation organisations such as ISO (ISO/IEC, 2012), ENISA (ENISA, 2016), NIST (NIST, 2018). The SQUARE methodology (Mead and Stehney, 2005) is a risk-driven approach that supports the elicitation, categorization, prioritization and inspection of security requirements through a number of specific steps. The methodology introduces the terms of security goal, threat and risk but does not take into consideration the assets and the vulnerabilities of the system. In (Bijwe and Mead, 2010) SQUARE was adopted in order to deal with privacy requirements as well. The extended framework includes the same steps as the original method in conjunction with the Privacy Requirements Elicitation Technique (PRET) (Miyazaki, Mead et al., 2008), a technique that supports the elicitation and prioritization of privacy requirements. Risk-oriented approaches tend to focus on predefined requirements and prescriptive solutions that do not consider the particular business context paying less attention to the business goals and objectives that form the basis for the specification of security requirements.

In *goal-oriented* approaches the requirements process focuses on identification, modelling and analysis of stakeholder goals. The NFR framework (Chung, Nixon et al., 2000) considers the non-functional requirements as soft goals that have to be achieved by the development system. The

MOSRE methodology is a framework (Salini and Kanmani, 2013) for web applications that includes the identification of non-security goals and requirements in parallel with security goals. Secure Tropos (Argyropoulos, Angelopoulos et al., 2018) introduces the concept of security constraints, i.e. a set of conditions, rules and restrictions that are imposed on a system and the system must operate in such way that none of them will be violated. In (Ahmed and Matulevicius, 2014) an asset-based approach is introduced whereby security goals are elicited from business process models and translate them into security requirements. The PRESSURE methodology (Fassbender, Heisel et al., 2014a; Fassbender, Heisel et al., 2014b) focuses on security needs during requirements analysis of software systems. The PriS methodology (Kalloniatis, Kavakli et al., 2008) is a goal-oriented approach aimed at integrating privacy requirements into the system design process. It is significant to note that these approaches concentrate on late requirements treating security requirements as the operationalisation of stakeholder goals in software functionalities but they tend to neglect strategic issues.

With the advent of Cloud computing a recent trend is the consideration of security provision as a service (Fehér and Sándor, 2019; Noor, Anwar et al., 2020). In this context RE does not focus on in-house security mechanism specification, rather it concerns the *identification of the appropriate security services offered by external providers that meet the business security requirements*. This service-oriented trend raises the need for a new RE metaphor that will enable the mapping of business security requirements onto external or internal service provision through *appropriate capabilities*.

The notion of capability in the field of RE goes beyond the traditional approaches offered by state-of-the-art methodologies in RE. It represents a most suitable metaphor that provides the means of considering the intertwining of technical, organisational and social concerns in such a way, that it is possible to connect strategic objectives and high-level organizational requirements to technological artefacts in a unified manner. SCORE offers on one hand a clear path for SME stakeholders to engage in their articulation of their requirements for CS and personal data protection and, on the other hand, for technologists to understand how these requirements may be implemented, thus achieving a much desired alignment between technical and business architectures (España, González et al., 2014; Grabis, Stirna et al., 2020).

The SCORE approach provides the methodological framework within which is it possible to yield conceptual models that are (a) of value to SME end users, IT staff and CS stakeholders (b) consistent across all representations, (c) conducive to various analyses and (d) reflective of systemic impact of changes.

## 7.2 The way forward

Deliverable D1.1, the result of work in task T1.1, is the first technical task of the SENTINEL project and is part of what is termed in the DoA “the Baseline Phase”, namely the ‘positioning of SENTINEL platform architecture and definition of technical, business and pilot requirements’. The work described in this report provides a thorough understanding of the current state of the art, the challenges faced by SMEs, and methodological framework for eliciting SME stakeholders’ requirements. The Baseline Phase includes another technical task, that of T1.2, whose objective is to propose a refined specification for the SENTINEL end-to-end architecture. Towards this end, part of the work in T1.2 will be founded on the results presented in this report.

This deliverable has also a direct input to WP6 “Real-life experiment evaluations: SENTINEL Pilots”. The SCORE methodology, together with the digital platform, will be central to the work in WP6 for using the pilots for experimenting and evaluating the outputs of the theoretical and technical work. In Section 6 we report on work that we have already begun with pilot cases stakeholders, and this early work bodes well for the future application of SCORE on the pilot cases.

Beyond the direct input of D1.1 on the rest of the project we envisage a number of desirable future developments in three areas: (a) tool support for the SCORE modelling, (b) ontological definition of problems and solutions in the domain of CS for privacy, and (c) using patterns for generic solutions to repeating problems for CS in SMEs, using the defined ontology.

### 7.2.1 Tool support for SCORE

The current version of SCORE uses a set of modelling tools for its visual part based on RE-Tools (Supakkul and Chung, 2009-2012) which itself is built upon StarUML<sup>10</sup>. As demonstrated in Section 6, the current version of the tools used was sufficient for producing user-friendly, easy to understand graphical notations. However, we believe that there is an opportunity to develop enhanced modelling facilities that would extend the modelling towards advanced functionalities for analysis and scenario building. This can be done leveraging a complete digital toolset for metamodeling such as ADOxx (Karagiannis and Visic, 2011). ADOxx is supported by the OMiLAB Digital Ecosystem which is an open platform for modelling method conceptualisation (Bork, Buchmann et al., 2019). By defining and mapping every SCORE concept into the metamodeling platform (henceforth referred to as the ‘tool’), we support the methodology and its concepts’ formal analysis and empower both developers and end-users with feature-rich modelling and representation capabilities.

In this approach, we are concerned with formally and programmatically defining the metamodel’s entities, their relationships and, critically, their appropriate attributes and constraints. These form the essential building blocks of the SCORE methodology; the tool will enable us to a) define the metamodel in a ‘library’, leveraging the platform’s flexibility and rich features, without great development effort; b) instantiate SCORE models (e.g., for SME participants), including a variety of visual representations, using the tool’s personalised modelling GUI, which can be customised for the SCORE metamodeling environment; (c) implement a SCORE-specific graphical representation language, with its dedicated RE notation and concepts; (d) dynamically interconnect entities and relationships across different SCORE metamodels, such as the capability model, the goal model, the actor dependency model and the informational object model and (e) export the associated diagrammatic representations in a variety of formats for interoperability and visualisation purposes.

Additionally, the tool’s custom-developed functionalities would allow us to algorithmically validate the meta-model, using scripting and queries. Validating the process with which models are instantiated involves identifying a path (e.g., treating the model design as a graph) which could satisfy the requirements set by both metamodel and query. Every such path essentially represents an instantiation of the metamodel. A SCORE-based example would be validating the transition from the current goals or capabilities to the desired goals or capabilities, for completeness, consistency and integrity with respect to requirements. These algorithms can be tailored to

---

<sup>10</sup> <https://staruml.io>

support even more complex functionality such as simulations, what-if scenarios and conditional model transformations, thus paving the way towards a full digitalisation of the SCORE methodology.

### 7.2.2 Ontologies

Ontologies are used in artificial intelligence, software engineering, medical informatics, library science, enterprise bookmarking, and information architecture as a form of knowledge representation (Alrumaih, Mirza et al., 2020). According to (Gruber, 1993), an ontology is “*a formal, explicit specification of a shared conceptualization, which includes terms and concepts that exist in a given domain, their properties, and the relationships between them*”.

Ontologies have been proven to be a key success factor for eliciting high quality requirements, and can facilitate and improve the job of requirements engineers, since they can reduce the conceptual vagueness and terminological confusion by providing a shared understanding of the related concepts between designers and stakeholders (Gharib, Giorgini et al., 2021). In addition, ontologies are an important methodological approach for knowledge-intensive problem solving that clearly involves reasoning about objects and concepts in a particular domain (Möller, 2020).

In the CS and privacy domains a number of ontologies have been proposed. These fall into two broad categories (Martins, Serrano et al., 2020). Firstly, *reference ontologies* aiming to clarify the intended meaning of CS and privacy terms, e.g., the Vulnerability Description Ontology (VDO) (Syed and Zhong, 2018), the Malware Ontology (Grégio, Bonacin et al., 2014). Secondly, *operational ontologies* that provide a minimal terminological structure, focusing on reasoning to fit the needs of a specific community, e.g., the IoTSec ontology (Mozzaquatro, Agostinho et al., 2018), the Incident Management Ontology (IM) (Mundie, Ruefle et al., 2014), PrOnto: Privacy Ontology for Legal Reasoning (Palmirani, Martoni et al., 2018), Industrial risk analysis ontology (Assali, Lenne et al., 2008); or on a specific application domain, e.g., e-health applications (Ciuciu, Claerhout et al., 2011), e-government applications (Karyda, M., Balopoulos, T. et al., 2006).

In the context of SENTINEL, the main objective of the target ontology would be to provide an operational ontology for describing the knowledge related to CS for privacy SME requirements. To this end, it will contain the core CS for privacy concepts along three dimensions *Organisational*, *Risk* and *Treatment* (Souag, Salinesi et al., 2015). The organisational dimension includes the concepts related to the SME environment (its assets and capabilities). The risk dimension includes the concepts related to threats and vulnerabilities. Finally, the treatment dimension is concerned with concepts related to the necessary treatments to overcome risks (e.g., CS and privacy goals, CS and privacy capabilities).

The concepts of the above ontology will be based on existing reference CS and privacy ontologies e.g., (Souag, Salinesi et al., 2015; Gharib, Giorgini et al., 2016) taking into consideration existing CS and privacy concept taxonomies, e.g., ENISA's Threat Taxonomy (ENISA, 2017a), the NIST SP800-30 (NIST, 2012) and ISO27005 (ISO/IEC, 2018) threat catalogues.

The ontology must be able to address questions regarding the risk the SME faces in the current situation, but also to determine the CS for privacy capability maturity of the desired situation. Furthermore, the ontology would be useful for indexing, organising and retrieving SENTINEL RE patterns (see Section 7.2.3).

### 7.2.3 Using patterns for best business practice in CS for privacy for SMEs

The notion of *pattern* is based on the opportunity to exploit knowledge about *best practice* in some domain. Best practice knowledge is thus constructed in patterns that are subsequently used as the starting point in some analysis, design or even software construction endeavours. Patterns are not invented but rather they are discovered within a particular domain with the purpose of being useful in many similar situations. In SENTINEL it is desirable to discover patterns that could be used as ready-made (parts of) solutions to be used in the specification of user requirements. In our case such patterns would be requirements patterns, recognising for example that certain sets of requirements are common to multiple SMEs. For example, the capability of “data sharing” would be common to many, if not all, SMEs, for which we wish to be able to capture their requirements for SC for privacy. This commonality in such a capability would be translated into common goals, actor dependency and informational models. Using these models related to the “data sharing” capability, from a patterns’ library, would greatly enhance the ease of use of the SCORE methodology and subsequently of the SENTINEL platform.

Patterns have been used in a variety of problem domains related to CS for privacy such as in security (van denBerghe A., Yskout et al., 2018), non-functional requirements (Cunha and Leite, 2014), in analysis of compliance violations (Elgammal, Turetken et al., 2012), in privacy requirements elicitation (Kalloniatis, Kavakli et al., 2007), to name but a few. Most of this work has been inspired by the work of Christopher Alexander who wrote his seminal book on the use of patterns within the domain of architecture, ‘The Timeless Way of Building’ (Alexander, 1979) in which he set the scene on the importance of patterns in such a way that, in many respects, it transcends the field of architecture. Alexander presents in this book the main arguments for the discovery of patterns and their use for achieving quality of designs. In this book (p. 69) Alexander puts forward the case that “... *our world has a structure, in the simple fact that certain patterns ... keep repeating themselves*”.

A pattern is more than just a description of something in the world. A pattern is also a ‘rule’ about when and how to create the thing. It should be both a *description of the artefact* and a *description of the process* that will generate the artefact. In SCORE we have defined the foundations for both the artefact (see Section 5.2) and the way of using the artefact (see Section 5.3). Using these generic definitions it would be desirable to identify patterns and expressing these in populating a library of patterns as well as the rules on using these. A pattern is derived after empirical observation that a certain solution applies well to a recurring problem. This raises the question of identification of the “problem-solution” patterns within SENTINEL. This can be answered by involving the stakeholders from the two pilot cases that we have engaged already but even more significantly from the involvement of many tens of SMEs scheduled to be engaged in the project through UNINOVA via the (DIH- inNOVA4TECH) and a relevant incubator / accelerator (Madan Parque) as detailed in the DoA (WP7, Task T7.4).

In designing the RE patterns for SENTINEL we envisage three main activities:

- Discover patterns by observing the domain and identifying those aspects that represent good business practice or at least generally accepted practice within that domain.
- Design a pattern ‘template’ that will be used for representing all patterns, using the capability-oriented approach and models supporting this view.

- Organise the resultant set of patterns into an indexable pattern repository.

When attempting to address requirements for CS and PDP, the appropriate patterns will have to be identified and used in order to develop more detailed and company-specific models towards the specification of requirements that could be exploited by the SENTINEL digital framework.

## Acknowledgments

We wish to thank our colleagues in the SENTINEL project for their contributions to sections 2 and 4. We are indebted to Daryl Holkham and Christopher Konialis for their contribution to the elicitation of their company requirements and for their active participation in the reviewing and editing of the SCORE models. Finally, we would like to express our gratitude to our internal project quality reviewers for their valuable contribution to ensuring the high quality of this deliverable.

**Evangelia Kavakli, Pericles Loucopoulos, Yannis Skourtis**



## References

- Ahmed, N. & Matulevicius, R. (2014).** *A Method for Eliciting Security Requirements from the Business Process Models*. CAiSE (Forum/Doctoral Consortium). pp. 57-64.
- Alexander, C. (1979).** *The Timeless Way of Building*, New York, Oxford University Press.
- Alrumaih, H., Mirza, A. & Alsalamah, H. (2020).** *Domain Ontology for Requirements Classification in Requirements Engineering Context*. *IEEE Access*, Vol. 8, pp. 89899-89908, doi: 10.1109/ACCESS.2020.2993838.
- Argyropoulos, N., Angelopoulos, K., Mouratidis, H. & Fish, A. (2018).** *Decision-Making in Security Requirements Engineering with Constrained Goal Models*. In: Katsikas, S. K., Cuppens, F., et al., (eds.) ESORICS 2017 International Workshops, CyberICPS 2017 and SECPRE 2017, Oslo, Norway, Lecture Notes in Computer Science. 10683. Springer, pp. 262-280.
- Assali, A. A., Lenne, D. & Debray, B. (2008).** *Ontology Development for Industrial Risk Analysis*. 3rd International Conference on Information and Communication Technologies: From Theory to Applications, Damascus, Syria. IEEE. pp. 1-5, doi: 10.1109/ICTTA.2008.4530312.
- Barney, J. (1991).** *Firm Resources and Sustained Competitive Advantage*. *Journal of Management*, Vol. 17, pp. 99-120.
- Benz, M. & Chatterjee, D. (2020).** *Calculated risk? A cybersecurity evaluation tool for SMEs*. *Business Horizons*, Vol. 63, No. 4, pp. 531-540.
- Bijwe, A. & Mead, N. R. (2010).** *Adapting the square process for privacy requirements engineering*. CMU/SEI-2010-TN-022, Software Engineering Institute, Carnegie Mellon.
- Bork, D., Buchmann, R. A., Karagiannis, D., Lee, M. & Miron, E. (2019).** *An Open Platform for Modeling Method Conceptualization: The OMILAB Digital Ecosystem*. *Communications of the Association for Information Systems*, Vol. 44, pp., doi: <https://doi.org/10.17705/1CAIS.04432>.
- Bravos, G., Loucopoulos, P., Dimitrakopoulos, G., Anagnostopoulos, D. & Kiouisi, V. A. (2017).** *A Capability – Driven modelling approach applied in smart transportation & management systems for large scale events*. *EAI Endorsed Transactions on Internet of Things*, Vol. 3, No. 9, pp. 1-8, doi: 10.4108/eai.31-8-2017.153051.
- Chung, L., Nixon, B. A., Yu, E. & Mylopoulos, J. (2000).** *Non-functional requirements in software engineering*. *International Series in Software Engineering*, Vol. 5, pp. 476.
- Ciuciu, I., Claerhout, B., Schilders, L. & Meersman, R. (2011).** *Ontology-Based Matching of Security Attributes for Personal Data Access in e-Health*. In: Meersman, R., Dillon, T., et al., eds. *On the Move to Meaningful Internet Systems (OTM 2011)*, Hersonissos, Crete, Greece. Springer. pp. 605-616.
- Cloud Security Alliance (CSA) (2017).** *Security Guidance for Critical Areas of Focus in Cloud Computing v4.0* [Online]. Available: <https://cloudsecurityalliance.org/artifacts/security-guidance-v4/> [Accessed 30th July 2021].
- Cloud Security Alliance (CSA) (2019).** *Top Threats to Cloud Computing: The Egregious 11*. Cloud Security Alliance.
- Cloud Security Alliance (CSA) (2021).** *Security Guidance for Critical Areas of Focus in Cloud Computing V4.0*. Cloud Security Alliance.
- Cunha, H. & Leite, J. C. S. d. P. (2014).** *Reusing Non-Functional Patterns in i\* Modeling*. The Fourth International Workshop on Requirements Patterns (RePa), Kalskrona, Sweden.

- Dardenne, A., Lamsweerde, A. v. & Fickas, S. (1993).** *Goal-directed Requirements Acquisition*. *Science of Computer Programming*, Vol. 20, No. 1-2, pp. 3-50.
- Dimitrakopoulos, G., Kavakli, E., Loucopoulos, P., Anagnostopoulos, D. & Zographos, T. (2019).** *A capability-oriented modelling and simulation approach for autonomous vehicle management*. *Simulation Modelling Practice and Theory*, Vol. 91, No. 2019, pp. 28-47.
- Elgammal, A., Turetken, O. & van den Heuvel, W.-J. (2012).** *Using Patterns for the Analysis and Resolution of Compliance Violations*. *International Journal of Cooperative Information Systems (IJCIS)*, Vol. 21, No. 1, pp. 31-54.
- ENISA (2015).** *Information security and privacy standards for SMEs: Recommendations to improve the adoption of information security and privacy standards in small and medium enterprises*. European Union Agency for Network and Information Security.
- ENISA (2016).** *Guidelines for SMEs on the security of personal data processing*. European Union Agency for Network and Information Security.
- ENISA (2017a).** *ENISA Threat Landscape Report 2016 - 15 Top Cyber-Threats and Trends*. European Union Agency For Network and Information Security.
- ENISA (2017b).** *Handbook on Security of Personal Data Processing*. European Union Agency For Network and Information Security.
- ENISA (2020).** *Stay Secure Online - 2020 Transatlantic Cybersecurity Checklist for Small Businesses*. European Union Agency for Network and Information Security.
- ENISA (2021).** *Cybersecurity for SMEs: Challenges and Recommendation*. European Union Agency for Cybersecurity.
- España, S., González, T., Grabis, J., Jokste, L., Juanes, R. & Valverde, F. (2014).** *Capability-driven Development of a SOA Platform: A Case Study*. In: Iliadis, L., Papazoglou, M., et al., (eds.) *International Workshop on Advances in Services DEsign based on the Notion of CAPability (ASDENCA'14)*, Thessaloniki, Greece, June 17, 2014, Lecture Notes in Business Information Processing (LNBIP). Springer, pp. 100-111.
- European Commission (2021).** *Entrepreneurship and Small and medium-sized enterprises (SMEs)* [Online]. Available: [https://ec.europa.eu/growth/smes\\_en](https://ec.europa.eu/growth/smes_en) [Accessed 11th August, 2021].
- Fassbender, S., Heisel, M. & Meis, R. (2014a).** *Functional requirements under security PresSuRE*. 9th International IEEE Conference on Software Paradigm Trends (ICSOFT-PT). pp. 5-16.
- Fassbender, S., Heisel, M. & Meis, R. (2014b).** *Problem-Based Security Requirements Elicitation and Refinement with PresSuRE*. *International Conference on Software Technologies*. Springer International Publishing, pp. 311-330.
- Fehér, D. J. & Sándor, B. (2019).** *Cloud SaaS Security Issues and Challenges*. *IEEE 13th International Symposium on Applied Computational Intelligence and Informatics (SACI 2019)*, Timisoara, Romania. pp. 000131-000134, doi: 10.1109/SACI46893.2019.9111529.
- Gharib, M., Giorgini, P. & Mylopoulos, J. (2016).** *Ontologies for Privacy Requirements Engineering: A Systematic Literature Review*. Cornell University, arXiv preprint arXiv:1611.10097.
- Gharib, M., Giorgini, P. & Mylopoulos, J. (2021).** *COPri v.2 — A core ontology for privacy requirements*. *Data & Knowledge Engineering*, Vol. 133, No. May 2021, pp. 101888(2021), doi: 10.1016/j.datak.2021.101888.

- Grabis, J. n., Stirna, J. & Zdravkovic, J. (2020).** *Capability Management in Resilient ICT Supply Chain Ecosystems*. 22nd International Conference on Enterprise Information Systems (ICEIS 2020). pp. 393-400.
- Grégio, A., Bonacin, R., Nabuco, O., Afonso, V. M., Lício De Geus, P. & Jino, M. (2014).** *Ontology for malware behavior: A core model proposal*. 23rd International WETICE Conference, Parma, Italy. IEEE. pp. 453-458, doi: 10.1109/WETICE.2014.72.
- Gruber, T. R. (1993).** *A translation approach to portable ontology specifications*. Knowledge Acquisition, Vol. 5, No. 2, pp. 199-220.
- ISO (1987).** *Information processing systems — Concepts and terminology for the conceptual schema and the information base*. ISO/TR 9007:1987, International Standards Organisation (ISO).
- ISO/IEC (2012).** *Common Criteria for Information Technology Security Evaluation*. 15408, International Organization for Standardization, Geneva, CH.
- ISO/IEC (2013).** *Information technology — Security techniques — Information security management systems — Requirements*. ISO/IEC 27001:2013, International Standards Organisation.
- ISO/IEC (2018).** *Information technology — Security techniques — Information security risk management*. ISO/IEC 27005:2018, International Standards Organisation.
- Jardine, D. A. (1984).** *Concepts and terminology for the conceptual schema and the information base*. Computers and Standards, Vol. 3, No. 1, pp. 3-17, doi: [https://doi.org/10.1016/0167-8051\(84\)90022-6](https://doi.org/10.1016/0167-8051(84)90022-6).
- Jarke, M., Loucopoulos, P., Lyytinen, K., Mylopoulos, J. & Robinson, W. (2011).** *The Brave New World of Design Requirements*. Information Systems, Vol. 36, No. 7, pp. 992-1008, doi: 10.1016/j.is.2011.04.003.
- Jouini, M., L. Ben Arfa Rabaia & Aissab, A. B. (2014).** *Classification of security threats in information systems*. 5th International Conference on Ambient Systems, Networks and Technologies (ANT-2014), Procedia Computer Science 32 (2014). pp. 489-496.
- Kalloniatis, C., Kavakli, E. & Gritzalis, S. (2007).** *Using Privacy Process Patterns for Incorporating Privacy Requirements into the System Design Process*. Second International Conference on Availability, Reliability and Security (ARES'07). pp. pp. 1009-1017.
- Kalloniatis, C., Kavakli, E. & Gritzalis, S. (2008).** *Addressing privacy requirements in system design: The PriS method*. Requirements Engineering Journal, Vol. 13, No. 3, pp. 241- 255.
- Kalogeraki, E. M., Apostolou, D., Polemi, N. & Papastergiou, S. (2018).** *Knowledge Management Methodology for Identifying Threats in Maritime/Logistics Supply Chains*. Knowledge Management Research & Practice Vol. 16, No. 4, pp. 508-524.
- Kalogeraki, E. M., Polemi, D., Papastergiou, S. & Panayiotopoulos, T. (2018).** *Modeling SCADA Attacks*. In: Yang, X. S., Nagar, A., et al. (eds.) "Smart Trends in Systems, Security and Sustainability". pp. 47-55.
- Karagiannis, D. & Visic, N. (2011).** *Platform-as-a-Service (PaaS): The ADOxx Metamodelling Platform*. Information Technologies - A Strategic Priority for the Knowledge Economy, Shvistov, Bulgaria.
- Karyda, M., Balopoulos, T., Dritsas, S., L., G., Kokolakis, S., Lambrinoudakis, C. & Gritzalis, S. (2006).** *An ontology for secure e-government applications*. First International Conference on Availability, Reliability and Security (ARES'06), Vienna, Austria. IEEE. pp. 1037, doi: 10.1109/ARES.2006.28.

- Loucopoulos, P. & Kavakli, E. (2017).** *Analysis of Requirements for a Cyber Physical Production System in the Automotive Industry*. AMCIS 2017, Boston, USA, August 10-12, 2017. pp. 1-10.
- Loucopoulos, P., Kavakli, E., Anagnostopoulos, D. & Dimitrakopoulos, G. (2018).** *Capability-oriented Analysis and Design for Collaborative Systems. An example from the Doha 2022 World Cup Games*. 10th International Conference on Computer and Automation Engineering, Brisbane, Australia. Association of Computer Machinery (ACM). pp. 185-189, doi: 10.1145/3192975.3192998.
- Loucopoulos, P., Kavakli, E. & Mascolo, J. (2020).** *Requirements Engineering for Cyber Physical Production Systems: The e-CORE approach and its application*. Information Systems, Vol. (In Press), No. (In Press), pp. (In Press), 10 November 2020, doi: <https://doi.org/10.1016/j.is.2020.101677>.
- Martins, B. F., Serrano, L., Reyes, J. F., Panach, J. I., Pastor, O. & Rochwerger, B. (2020).** *Conceptual Characterization of Cybersecurity Ontologies*. In: Grabis J., Bork D. (eds) *The Practice of Enterprise Modeling*. In: Grabis, J. & Bork, D., eds. *The Practice of Enterprise Modeling (PoEM 2020)*, Riga, Latvia. Springer, Cham.
- Matulevičius, R. & Heymans, P. (2005).** *Analysis of KAOS Meta-model*. Namur University, Namur, Belgium.
- Mead, N. R. & Stehney, T. (2005).** *Security quality requirements engineering (SQUARE) methodology*. Association of Computing Machinery (ACM), Vol. 30, No. 4, pp. 1-7.
- Microsoft (2005).** *The STRIDE Threat Model* [Online]. Available: [https://docs.microsoft.com/en-us/previous-versions/commerce-server/ee823878\(v=cs.20\)?redirectedfrom=MSDN](https://docs.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20)?redirectedfrom=MSDN) [Accessed 28th August 2021].
- Miyazaki, S., Mead, N. & Zhan, J. (2008).** *Computer-aided privacy requirements elicitation technique*. Asia-Pacific Services Computing Conference (APSCC'08). pp. 367-372.
- Möller, D. P. F. (2020).** *Cybersecurity Ontology*. "Cybersecurity in Digital Transformation". Springer.
- Mozzaquatro, B. A., Agostinho, C., Goncalves, D., Martins, J. & Jardim-Goncalves, R. (2018).** *An ontology-based cybersecurity framework for the internet of things*. Sensors, Vol. 18, No. 9, pp., doi: 10.3390/s18093053.
- Mundie, D. A., Ruefle, R., Dorofee, A. J., Perl, S. J., McCloud, J. & Collins, M. (2014).** *An incident management ontology*. In: Blackmond Laskey, K., Emmons, I., et al., eds. *Ninth Conference on Semantic Technology for Intelligence, Defense, and Security (STID)*, Fairfax VA, USA. CEUR Workshop Proceedings pp. 62-71.
- NIST (2012).** *Guide for conducting risk assesement*. National Insitute of Standards & Technology.
- NIST (2018).** *Framework for Improving Critical Infrastructure Cybersecurity*. National Insitute of Standards & Technology.
- Noor, U., Anwar, Z., Altmann, J. & Rashid, Z. (2020).** *Customer-oriented ranking of cyber threat intelligence service providers*. Electronic Commerce Research and Applications, Vol. 41, pp. 100976.
- Palmirani, M., Martoni, M., Rossi, A., Bartolini, C. & Robaldo, L. (2018).** *PrOnto: Privacy Ontology for Legal Reasoning*. In: Kő, A. & Francesconi, E., eds. *Electronic Government and the Information Systems Perspective (EGOVIS 2018)*, Regensburg, Germany. Springer, Cham. pp. 139-152.

- Papastergiou, S. & Polemi, D. (2017).** *Securing maritime logistics and supply chain: The medusa and mitigate approaches.* Maritime Interdiction Operations, Vol. 14, No. 1, pp. 42-48.
- Salini, P. & Kanmani, S. (2013).** *Model oriented security requirements engineering (MOSRE) framework for Web applications.* "Advances in Computing and Information Technology". Berlin Heidelberg: Springer. pp. 341-353.
- Schauer, S., Polemi, N. & Mouratidis, H. (2019).** *MITIGATE: A dynamic supply chain cyber risk assessment methodology.* Journal of Transportation Security, Vol. 12, pp. 1-35.
- Souag, A., Salinesi, C., Mazo, R. & Comyn-Wattiau, I. (2015).** *A Security Ontology for Security Requirements Elicitation.* In: F., P., J., C., et al., eds. *Engineering Secure Software and Systems (ESSoS 2015)*, Paris, France. Springer, Cham. pp. 157-177.
- Supakkul, S. & Chung, L. (2009-2012).** *RE-Tools: A Multi-notational Modelling Toolkit* [Online]. Available: <http://www.utdallas.edu/~supakkul/tools/RE-Tools/index.html> [Accessed 1st July 2021].
- Syed, R. & Zhong, H. (2018).** *Cybersecurity Vulnerability Management: An Ontology-Based Conceptual Model.* The Americas' Conference on Information Systems (AMCIS). 2018. Association for Information Systems (AIS).
- van denBerghe A., Yskout, K. & Joosen, W. (2018).** *Security patterns 2.0: towards security patterns based on security building blocks.* SEAD '18: Proceedings of the 1st International Workshop on Security Awareness from Design to Deployment. pp. 45-48.
- van Griethuysen, J. J. (1982).** *ISO - Concepts and Terminology for the Conceptual Schema and the Information Base.* N695, ISO/TC9/SC5/WG3.
- Yu, E. & Mylopoulos, J. (1998).** *Why Goal-Oriented Requirements Engineering.* In: Dubois, E., Opdahl, A., et al., (eds.) *Fourth International Workshop on Requirements Engineering: Foundation for Software Quality (REFSQ'98)*, Pisa, Italy, June 1998. pp. 15-22.



## Appendix I Objectives for Deliverable D1.1

This appendix details the objectives of Workpackage 1 and the key issues addressed in Task T1.1 all of which were used for structuring this deliverable and for ensuring that the outcomes reported within it are aligned with the description in the Grant Agreement.

The objectives of WP1 are to:

- i. Capture detailed functional requirements and technical challenges for the envisioned framework and complete a thorough requirements analysis.
- ii. Determine the detailed functionality of the SENTINEL digital architecture, according to the end-user (SMEs/MEs) needs and the state-of-the-art in privacy, personal data protection and compliance.
- iii. Describe in detail and continuously monitor the scientific (academic and industrial) and end-user needs and challenges for secure and trustworthy solutions for SMEs/MEs.
- iv. Synthesise and present the current state-of-the-art from the viewpoint of the project's highlighted problems.
- v. Design the technical framework and architecture of the integrated SENTINEL platform.
- vi. Specify the test cases for the pilots including the verification and validation approach and develop a mapping of the architecture's mechanics.
- vii. Design and implement the SENTINEL demonstration protocol.

In addition to these guiding objectives, the work in this deliverable was also motivated by a set of specific issues that are defined in the Grant Agreement as follows:

- i. To gain insight into the parameters that drive the needs for data privacy and compliance processes in SMEs.
- ii. Define the RE methodology.
- iii. Identification of environment's fundamental utilities and processes that must be facilitated by combinations of tools, technologies and services related to data privacy and compliance.
- iv. Definition of usage characteristics of the environment.
- v. Identification of common and most important challenges with respect to the implementation of cybersecurity facilitators that can affect the environment's operation.
- vi. Identification of fundamental data protection utilities that must be deployed, including their individual configurations.
- vii. Definition of SENTINEL technological innovation.
- viii. Definition of basic AI-enabling levels and principles to support the envisioned SENTINEL offerings.



## Appendix II Questionnaire for business centric information gathering

### WP1 T1.1

#### ***Business centric questionnaire***

Task T1.1 of WP1 aims to gain insight into the parameters that drive the needs for data privacy and compliance processes in SMEs/MEs and to define the relevant RE methodology. To this end, one of the actions seeks to gain an understanding the needs of the project's pilot SME consortium partners, TIG and CG, for privacy and cybersecurity. Such an understanding provides key insight into developing the SENTINEL Requirements Engineering methodology.

With this questionnaire we seek to identify both existing and desired capabilities of the participating SMEs for GDPR compliance and cybersecurity.

A **capability** is defined as a set of assets owned by an enterprise where these assets possess **capacities** and certain **abilities**. For example, an enterprise may own some digital asset with the capacity of *automated mechanism* and the ability to *seek data subject consent*.

This questionnaire is organized into two sections. Section 1 deals with issues of privacy whereas section 2 deals with issues of cybersecurity.

#### **Section 1: Privacy-related questions**

	Question	Answer	Typical concepts / examples
1	What specific <b>capabilities</b> does your company possess towards GDPR compliance?		<b>Capability = capacity + ability</b> 1) Data Protection Officer (DPO) + GDPR compliance responsibility 2) Automated mechanism + seek data subject consent 3) GDPR Privacy Policy + legal justification of data processing 4) GDPR Privacy Policy + privacy rights enforcement
2	What are your company's <b>existing capabilities</b> , potentially raising privacy & personal data protection concerns?		1) Marketing and communication, 2) Sales of services (describe privacy aspects) 3) Sales of products (online sales etc)
3	What are your company's future <b>business goals</b> , in relation to point (2)?		Either extending existing capabilities or introducing new ones
4	What <b>new</b> or <b>improved capabilities</b> does your company need to meet these new goals?		
5	Who are your data subjects?		e.g., customer <b>Data subject</b> refers to any individual person who

	Question	Answer	Typical concepts / examples
			can be identified, directly or indirectly, via an identifier such as a name, an ID number, location data, or via factors specific to the person's physical, physiological, genetic, mental, economic, cultural or social identity.
6	Who are your data processors?		e.g. HR department; marketing team; outsourced The <b>data processor</b> is a person or organization who deals with personal data as instructed by a controller (your company) for specific purposes and services offered to the controller that involve personal data processing (processing can be many things under the GDPR)
7	Do you use third parties that process personal data on your behalf?		e.g., outsourced company, consultant(s)
8	How do you currently ensure continuation of privacy and personal data protection?		How do you assess internal or external processors' capabilities to process personal data in line with the GDPR and protection of the rights of the data subjects (~ their GDPR compliance)?
8	Do you make decisions about people based on automated processes?		e.g., decision support system
9	What types of processing activities do you carry out, either internally or via third parties or automated systems?		Common types of <b>personal data processing</b> include (but are not limited to) collecting, recording, organising, structuring, storing, modifying, consulting, using, publishing, combining, erasing, and destroying data.
10	Does the data you (or your assigned third parties) process involve Personally Identifiable Information (PII)?		<b>PII</b> is data that can be used to clearly identify an individual. E.g., name, national insurance number, physical address, email address, phone number, financial data, IP address, login details, social media activity, digital images, geolocation data, behavioural data, medical data, biometric data, customer purchase & loyalty history.
11	Does your company deploy metrics to evaluate your privacy policy? If yes, what are they?		e.g., participation in a data protection impact assessment (DPIA); number of privacy-related customer complaints;

## Section 2: Cybersecurity-related questions

	Question	Answer	Typical concepts
1	What specific <b>capabilities</b> does your company possess to enforce cybersecurity and protect from privacy breaches?		<b>Capability = capacity + ability</b> e.g., technical security measure set 1 + protect data management infrastructure Endpoint protection platform + Continuous protection from malicious activity for workstations Mobile security suite + Continuous protection from malicious activity for smartphones Encryption software + protect PII VPN software + secure employee access to company infrastructure
2	What specific <b>capabilities</b> does your company possess to <b>assess</b> cybersecurity?		e.g., ITSec officer + ITSec policy, ITSec officer + ITSec audit ITSec DSS + ITSec risk assessment ITSec monitoring asset + threats identification and evaluation
3	What specific <b>capabilities</b> does your company possess to raise employee <b>awareness</b> on cybersecurity?		e.g. ITSec training program + increase ITSec awareness
4	What specific <b>capabilities</b> does your company possess to <b>notify</b> the authorities and your data subjects in the event of a data breach?		e.g. Security policy + data breach protocol Endpoint protection platform + incident response
5	What future <b>business goals</b> does your company have so that your company is cybersecure?		<b>Business goals. e.g.</b> - Improve market trust - Boost service availability / performance - Compliance (mandatory?) - Costs control - Data assurance / data quality - Reduce security liability - Culture-, policy- and governance-related <b>Cybersecurity goals. e.g.</b> - To protect the confidentiality of our customer data (encryption, access control, authentication & authorisation, physical security etc) - To preserve data integrity (backup policy, PKI-based integrity enforcement etc) - To promote data availability for employees, customers and partners (physical protection, redundancy, disaster sites etc)
6	Which of your <b>existing capabilities</b> may still be relevant?		<b>Capability = capacity + ability</b>
7	What <b>new</b> or <b>improved capabilities</b> does your company need to meet these new goals?		<b>Capability = capacity + ability</b>
8	Does your company deploy metrics to evaluate your cybersecurity? If yes, what are they?		e.g., based on IPSec assessments: Number of intrusion attempts Number of security breaches Level of preparedness (generic). Security Policy compliance Number of systems with known vulnerabilities Number of users with admin access

	Question	Answer	Typical concepts
			Mean-Time-to-Detect/Respond. Days to patch.

## Appendix III Questionnaire for technology centric information gathering

### WP1 T1.1.1

#### *Technology centric questionnaire*

Task T1.1 of WP1 aims to gain insight into the parameters that drive the needs for data privacy and compliance processes in SMEs/MEs and to define the relevant RE methodology. One of the actions focuses on understanding the provision of technologies by consortium partners (IDIR, ITML, INTRA, SHELL, TSI, LIST, FP, STS, AEGIS, ACS), for privacy and cybersecurity. Such an understanding would provide key insight into developing the SENTINEL Requirements Engineering methodology.

With this questionnaire we seek to identify both **existing and desired capabilities** of the participating companies regarding the technologies for GDPR compliance and cybersecurity. These technologies will play an important role in establishing the desired SENTINEL architecture.

A **capability** is defined as a set of assets owned by an enterprise where these assets possess **capacities** and certain **abilities**. For example, Security Infusion (SI) is an asset of ITML with the capacity of a *cloud based solution* and the ability to *collect operational data*.

This questionnaire is organized into two sections. Section 1 deals with issues of privacy whereas section 2 deals with issues of cybersecurity.

#### Section 1: Privacy-related questions

	Question	Answer	Typical concepts / examples
1	What specific <b>capabilities</b> does your company offers in support of GDPR compliance?		<b>Capability = capacity + ability</b> 1) Forensic Visualisation Toolkit + visualise abnormal operation 2) Mobile Threat Prevention (MTP) software + detect and protect malicious threats
2	What <b>new</b> or <b>improved capabilities</b> does your company consider in order to improve the GDPR compliance capabilities offered?		<b>Capability = capacity + ability</b>
3	Does your company deploy <b>metrics</b> to evaluate your GDPR compliance capabilities? If yes, what are they?		e.g., based on tool performance: Throughput, User friendliness  e.g., based on tool efficiency number of incidents detected compared to similar products

## Section 2: Cybersecurity-related questions

	Question	Answer	Typical concepts
1	What specific capabilities does your company possess to enforce cybersecurity and protect from privacy breaches?		<b>Capability = capacity + ability</b> e.g., 2 Mobile Threat Prevention (MTP) software + detect and protect malicious threats
2	What new or improved capabilities does your company consider in order to improve the cybersecurity capabilities offered?		<b>Capability = capacity + ability</b>
3	Does your company deploy metrics to evaluate your cybersecurity capabilities? If yes, what are they?		e.g., based on tool performance: Throughput, User friendliness  e.g., based on tool efficiency number of incidents detected compared to similar products



## Appendix IV Expanded list of high-level requirements

In this appendix, we endeavour a more detailed expansion of the high-level requirements presented in Section 2 and utilised in Section 4, that will eventually lead to a mapping between the actual end-user requirements and their realisation in the SENTINEL digital platform. The following table is a copy of Table 2 initially presented in Section 2.

CIA triad	PDP & compliance	PETs
Confidentiality	Data collection & flow mapping	Encryption
Integrity	Record keeping & audit management	Anonymisation
Availability	Data sovereignty & portability	Pseudonymisation
<b>CS generic</b>	DPIA	Obfuscation
Policy drafting	Data transfers, vendor & 3 <sup>rd</sup> party management	Data minimisation
Policy enforcing	DPO management	Disclosure control
Non-repudiation	Notices, consent management	Access control
AAA – Authentication, Authorisation, Accounting	Compliance & accountability	Differential privacy
Incident reporting & handling	<b>CS technical</b>	
Cyber awareness	Endpoint security - computers	Cloud security (SecaaS)
Education & training	Endpoint security – mobile	SW lifecycle security
Unlinkability	Pentesting & vuln.assessment	Monitoring - alerting
Unobservability	Email security	Logging
Self-assessment	Network security	Analytics, visualisation
Business continuity	IAM (identity/access mgmt.)	Forensics

Each requirement comes with its unique ID, identification of type, name, description, rationale within SENTINEL, and the technical means of implementation. During the technical architecture refinement phase (T1.2) and the experimentation protocol alignment phase (T6.1), these will be a) associated with lower-level technical requirements, b) linked with the specific pilot and other use cases requirements and technical dependencies and c) enriched with individual metrics for evaluation.

ID	CIA001	Name:	Confidentiality	Type:	CIA-high level
<b>Description:</b>	To protect assets from being exposed to unauthorized parties, for example in the case of a data breach.				
<b>Rationale in SENTINEL:</b>	Confidentiality is a core requirement belonging to the CIA triad, which permeates every technical implementation of both contributed and SENTINEL components, for CS and PDP.				
<b>Means of technical implementation:</b>	i) Identity management, authorisation, authentication and access control technologies (against data breaches); ii) Unobservability; iii) Encryption; iv) Anonymisation; iv) Pseudonymisation; v) Data obfuscation; v) Disclosure control; vi) Network security (secure network configurations, firewalls, WAFs, IDS etc); vii) Best CS workplace practices; viii) Endpoint protection software; ix) Email & mobile security				
ID	CIA002	Name:	Integrity	Type:	CIA-high level

<b>Description:</b>	To only allow modification of assets by authorized individuals			
<b>Rationale in SENTINEL:</b>	Integrity is a core requirement belonging to the CIA triad, which permeates every technical implementation of both contributed and SENTINEL components, for CS and PDP.			
<b>Means of technical implementation:</b>	i) Identity management, authorisation, authentication and access control technologies (against unauthorized data modification); ii) Unobservability; iii) Encryption and cryptographic integrity controls; iv) Endpoint protection software; v) Best CS workplace practices.			
<b>ID</b>	CIA003	<b>Name:</b>	Availability	<b>Type:</b> CIA-high level
<b>Description:</b>	To ensure the continuous availability of the SME services and data to authorised internal and external entities.			
<b>Rationale in SENTINEL:</b>	Availability is a core requirement belonging to the CIA triad, which permeates every technical implementation of both contributed and SENTINEL components, for CS and PDP.			
<b>Means of technical implementation:</b>	i) Endpoint protection software; ii) Identity management, authorisation, authentication and access control technologies (against service disruptions); iii) Network security (secure network configurations, firewalls, WAFs, IDS etc against DoS and similar disruptions); iv) Backup software and business continuity planning and services; v) Secure, redundant and available infrastructure, including Cloud, configurations			
<b>ID</b>	CIA004	<b>Name:</b>	Non-repudiation	<b>Type:</b> CIA-high level
<b>Description:</b>	To provide the assurance that the ownership, validity or authenticity of certain data or logged activities cannot be disputed.			
<b>Rationale in SENTINEL:</b>	We consider NR as an addition to the core CIA triad. This requirements should be satisfied by technical SENTINEL implementations which enforce authenticating identities.			
<b>Means of technical implementation:</b>	i) Cryptographic non-repudiation controls (PKI, digital signatures etc); ii) Email security; iii) IAM; iv) Logging, record keeping and audit management			
<b>ID</b>	NFR001	<b>Name:</b>	Usability	<b>Type:</b> Non-functional / quality
<b>Description:</b>	To provide cybersecurity, privacy and personal data protection that are easy and intuitive to use.			
<b>Rationale in SENTINEL:</b>	SENTINEL, as an integrated digital framework, should be intuitively presented to participant SMEs as a compliance-as-a-service offering and not add additional admin burden to their everyday process.			
<b>Means of implementation:</b>	The user journey across the SENTINEL components and building blocks should be easily navigable and the value to be gained understandable and attainable for end users (UX). Finally, the individual web implementations and front-end components should be realised with best UI practices in mind.			
<b>ID</b>	NFR002	<b>Name:</b>	Cost-effectiveness	<b>Type:</b> Non-functional / quality
<b>Description:</b>	To provide cybersecurity, privacy and personal data protection solutions at a cost-effective level for the participant SMEs.			
<b>Rationale in SENTINEL:</b>	Using SENTINEL has to be cost effective for participant SMEs. The implementation of its proposed OTMs shouldn't consume more human and financial resources compared to hiring external CS experts and implementing their recommendations.			
<b>Means of implementation:</b>	The SENTINEL recommendation engine should consider various cost factors which are weighted highly against the budget restrictions provided by the SME.			
<b>ID</b>	NFR003	<b>Name:</b>	Scalability	<b>Type:</b> Non-functional / quality

<b>Description:</b>	To deploy scalable cybersecurity, privacy and personal data protection solutions which can effectively support the SME as its business and requirements grow.				
<b>Rationale in SENTINEL:</b>	We interpret scalability as the SENTINEL platform's capability to offer a continuous service which adapts to the SME needs as the company evolves – not as a service users would only visit once, to get a set of policy recommendations.				
<b>Means of implementation:</b>	Scalability is attained by a) emphasising the usability and perceived value of components such as the observatory, the compliance centre, the enforcement centre and the incident response centre, which boost the total lifetime value which end SME users get from leveraging SENTINEL in a continuous manner; and b) enabling the core self-assessment and recommendation components to reassess the SME CS and PDP stance often and update the existing recommendations to reflect the new company scale and requirements and they grow.				
<b>ID</b>	GEN001	<b>Name:</b>	Policy drafting	<b>Type:</b>	Generic cybersecurity
<b>Description:</b>	To draft an internal policy for the SME, recommending specific organisational and technical measures to be implemented, in accordance with the risk level associated with specific data processing operations.				
<b>Rationale in SENTINEL:</b>	Policy drafting will take into account a) the risk level associated with specific identified SME personal data processing operations and b) the intelligent recommendations proposed by the digital core to draft a policy that is readable and trackable by both machine and human.				
<b>Means of technical implementation:</b>	Implementation of the policy drafting and enforcement module (T3.4)				
<b>ID</b>	GEN002	<b>Name:</b>	Policy enforcing	<b>Type:</b>	Generic cybersecurity
<b>Description:</b>	To monitor the implementation of specific policy points and track their progress.				
<b>Rationale in SENTINEL:</b>	SENTINEL proposes a hybrid policy enforcement approach where organisational and other measures which have to be human-tracked are supported by digitalised checklists and progress indicators, similar to project management tool. Specific components which enable the digital tracking of the implementation of technical measures (e.g., via agent-based security monitoring) will be taken into account for a fully automated tracking and reporting.				
<b>Means of technical implementation:</b>	Implementation of the policy drafting and enforcement module (T3.4)				
<b>ID</b>	GEN003	<b>Name:</b>	AAA	<b>Type:</b>	Generic cybersecurity
<b>Description:</b>	Authentication, Authorisation and Accounting: to provide the technical means for a) identifying users; b) granting access to resources based on their explicitly defined privileges and c) all related logging, record keeping and supporting auditing				
<b>Rationale in SENTINEL:</b>	AAA (which may be approached as IAM when emphasising identity management) is an integral part of every CS and PDP policy. SENTINEL will tackle this requirement by recommending internal and external components for both on-premises and Cloud SME infrastructures and services.				
<b>Means of technical implementation:</b>	SENTINEL will provide robust AAA capabilities through a) the IdMS component, taking over managing customers' personal data for GDPR compliance and b) through provisioning external (open source and commercial) IAM and identity management & auth proxy services as a technical measure, where recommended.				
<b>ID</b>	GEN004	<b>Name:</b>	Incident reporting and handling	<b>Type:</b>	Generic cybersecurity
<b>Description:</b>	To establish planning, procedures and technical means for ensuring and orderly and effective response to cybersecurity incidents and data breaches				

<b>Rationale in SENTINEL:</b>	Incident response in SENTINEL should be tackled during the 'lifecycle support' phase of SME participation, in the incident response centre, along with the compliance and enforcement centres.				
<b>Means of technical implementation:</b>	Implementation SENTINEL's trustworthy incident reporting and sharing module (T3.2) which interfaces with the recommendation engine, policy enforcement module, the MySentinel dashboard and the SENTINEL Observatory.				
<b>ID</b>	GEN005	<b>Name:</b>	Awareness, education, training	<b>Type:</b>	Generic cybersecurity
<b>Description:</b>	To take measurable actions towards more and better knowledge towards cybersecurity, privacy and personal data protection for participant SMEs				
<b>Rationale in SENTINEL:</b>	Cyber awareness and training is a requirement that should be present in every SENTINEL implementation that is user-facing. SENTINEL tackles this through a) simple and attainable CS recommendations and checklists to improve the workplace cyber culture; b) targeted recommendations of CS and PDP training and educational courses tailored to individual company requirements.				
<b>Means of technical implementation:</b>	a) providing external training content (e.g., educational courses) with the appropriate metadata for effective recommendations (T2.4); b) performing recommendations tailored to individual participants following self-assessment (T4.3)				
<b>ID</b>	GEN006	<b>Name:</b>	Unlinkability	<b>Type:</b>	Generic cybersecurity
<b>Description:</b>	To prevent potential attackers from linking information to natural persons or other sensitive or personally identifiable information				
<b>Rationale in SENTINEL:</b>	Unlinkability is an important technique for data minimisation for enhancing privacy, pursuant to art.32 of GDPR.				
<b>Means of technical implementation:</b>	i) Obfuscation; ii) Pseudonymization; iii) AI-assisted PETs for unlinkability. To be investigated for selection in T2.4				
<b>ID</b>	GEN007	<b>Name:</b>	Undetectability, unobservability	<b>Type:</b>	Generic cybersecurity
<b>Description:</b>	To prevent potential attackers from detecting information of interest or observing related operations				
<b>Rationale in SENTINEL:</b>	Undetectability and unobservability are important techniques for enhancing privacy, pursuant to art.32 of GDPR.				
<b>Means of technical implementation:</b>	Robust IAM. Data minimisation, encryption, data obfuscation. Disclosure control. To be investigated for selection in T2.4				
<b>ID</b>	GEN008	<b>Name:</b>	Self-assessment	<b>Type:</b>	Generic cybersecurity
<b>Description:</b>	To provide the means for participant SMEs to self-assess their current standing in terms of cybersecurity and personal data protection, including w.r.t. OTMs for GDPR compliance.				
<b>Rationale in SENTINEL:</b>	Self-assessment plays a pivotal role in SENTINEL. It provides both an entry point for SME participants and a process which they revisit as their requirements change. Self-assessment provides the basis for a) evaluating the current CS and PDP status; b) calculating RASE scoring; c) sharing critical input data to the Recommendation Engine and d) recommending targeted trainings				
<b>Means of technical implementation:</b>	Implementation SENTINEL's self-assessment centre, including for tailor-made requirement analyses, RASE scoring and training courses recommendations (T4.3)				
<b>ID</b>	GEN009	<b>Name:</b>	Business continuity	<b>Type:</b>	Generic cybersecurity

<b>Description:</b>	To implement organizational measures for business continuity as well as SME-wide data backup, restore and other technical procedures (e.g., disaster sites).				
<b>Rationale in SENTINEL:</b>	SENTINEL should a) recommend robust organisational measures for business continuity as part of the drafted policy and b) provide the technical means by which these can be enforced.				
<b>Means of technical implementation:</b>	i) Implementation of the policy drafting and enforcement module (T3.4) ii) selection and recommendation of appropriate external OS or commercial technical solutions (e.g., Cloud or local backup services etc).				
<b>ID</b>	PDP001	<b>Name:</b>	Data collection & flow mapping	<b>Type:</b>	Generic PDP
<b>Description:</b>	To perform a detailed map of the SME's data flows in order to evaluate associated privacy risk				
<b>Rationale in SENTINEL:</b>	In SENTINEL, a lightweight (due to its automated nature) approach for mapping data processing operations for GDPR compliance takes part during self-assessment, when the overall data processing environment and its different procedures are evaluated. Where a more rigorous is indicated, the appropriate external components shall be recommended.				
<b>Means of technical implementation:</b>	i) SME self-assessment for PDP; ii) selection and recommendation of appropriate external OS or commercial solutions (as part of a data governance policy).				
<b>ID</b>	PDP002	<b>Name:</b>	Record keeping & audit management	<b>Type:</b>	Generic PDP
<b>Description:</b>	To enforce companywide OTMs for documenting non-repudiable records, processes, and accountability for the data stored by the SME.				
<b>Rationale in SENTINEL:</b>	This requirement is partly satisfied by the generic CS technical requirement for AAA (Accounting). Record keeping is observed by several SENTINEL components such as the IdMS (T2.2), the GDPR compliance framework (T2.1), MITIGATE (T2.3) and the DPIAA suite (T4.2).				
<b>Means of technical implementation:</b>	The parts that relate to GDPR compliance are satisfied, in conjunction with the previous requirement (Data collection & flow mapping) by recommending technical solutions for data inventory, mapping, logging and data processing recording for each DP operation.				
<b>ID</b>	PDP003	<b>Name:</b>	Data sovereignty & portability	<b>Type:</b>	Generic PDP
<b>Description:</b>	To provide the technical means by which a) end-users are made the sovereign owners of their own personal data, with portability, updating, deletion, disclosure (e.g., to SMEs) and b) data remain physically within their legally bound sovereign geographical area(s).				
<b>Rationale in SENTINEL:</b>	Data sovereignty, as a locale-specific requirement, it is one that SENTINEL should address in every related PDP component.				
<b>Means of technical implementation:</b>	a) SENTINEL IdMS (T2.2) ; b) GDPR compliance framework (T2.1); c) external components for complex implementations as required				
<b>ID</b>	PDP004	<b>Name:</b>	DPIA	<b>Type:</b>	Generic PDP
<b>Description:</b>	Data protection impact assessment: To identify and evaluate risk associated with the SME's data processing activities				
<b>Rationale in SENTINEL:</b>	DPIAs are traditionally human-centric assessments where assessors evaluate risk by deeply understanding the environment wherein data processing operations take place within a company. SENTINEL, by automating parts of the process, cuts costs and offers benefits to SMEs which can describe their processing in a way that enables automated risk assessment.				

<b>Means of technical implementation:</b>	a) Self-assessment for PDP, based on the ENISA framework for SMEs (T4.3); b) DPIA within the Security and Privacy assurance Suite (T4.2); c) External components or human intervention when unavoidable (T2.4).				
<b>ID</b>	PDP005	<b>Name:</b>	Data transfers, vendor & 3rd party management	<b>Type:</b>	Generic PDP
<b>Description:</b>	To provide a complete and integrated third-party risk management solution for GDPR compliance, including managing risk related to processors and sub-processors.				
<b>Rationale in SENTINEL:</b>	SENTINEL should address data processor management requirements in every related PDP component.				
<b>Means of technical implementation:</b>	a) GDPR compliance framework (T2.1) – in part ; b) Self-assessment for PDP, based on the ENISA framework for SMEs (T4.3) – in part; c) External components as recommended (T2.4).				
<b>ID</b>	PDP006	<b>Name:</b>	DPO management	<b>Type:</b>	Generic PDP
<b>Description:</b>	To provide the company's assigned DPO with the technical means to organise and monitor work				
<b>Rationale in SENTINEL:</b>	SENTINEL should address DPO needs and requirements in every related PDP component.				
<b>Means of technical implementation:</b>	Compliance centre. Enforcement centre. Observatory. Incident response centre. Integrated PDP related SENTINEL components.				
<b>ID</b>	PDP007	<b>Name:</b>	Notices & consent management	<b>Type:</b>	Generic PDP
<b>Description:</b>	To provide the SME with the technical means to be able to demonstrate that personal data of third parties (data subjects) are processed in a transparent manner (right to be informed), and the means for data subjects to provide their voluntary and explicit consent to this processing.				
<b>Rationale in SENTINEL:</b>	SENTINEL should simplify the needs for implementing transparency and consent mechanisms by integrating it into PDP policy in clear terms and providing the technical means to enforce it.				
<b>Means of technical implementation:</b>	a) as a drafted policy item; b) as guidance for SMEs to self-implement (e.g., via CMS-website modules or 3 <sup>rd</sup> party technical integrations, e.g., in GDPR email campaigns) or c) external components as recommended (T2.4) when a more holistic approach is called for.				
<b>ID</b>	PDP008	<b>Name:</b>	Compliance & accountability	<b>Type:</b>	Generic PDP
<b>Description:</b>	To provide the SME with the appropriate technical means to be able to demonstrate the implemented OTMs and their effectiveness when requested, as well as monitor overall GDPR compliance.				
<b>Rationale in SENTINEL:</b>	One of the overarching benefits of SENTINEL is that it promises a 360° view of the participant SME's GDPR standing w.r.t. compliance. This view is made attainable through the integration of a number of interrelated components.				
<b>Means of technical implementation:</b>	i) All contributed and external PDP components (T2.3; T2.4)); ii) Compliance centre (T5.2, T5.1); iii) Enforcement centre(T5.2, T5.1); iv) Observatory (T4.4); v) PDP and data privacy compliance framework (T2.1)				
<b>ID</b>	PET001	<b>Name:</b>	Encryption	<b>Type:</b>	Privacy enhancing
<b>Description:</b>	To ensure the confidentiality of data at rest or in transit via cryptography.				
<b>Rationale in SENTINEL:</b>	SENTINEL will recommend technologies which apply encryption at various layers of the data stack to offer better privacy by design in the transformed data processing operations.				



<b>Means of technical implementation:</b>	Policy recommendations and external components (T3.3, T3.4, T2.4)				
<b>ID</b>	PET002	<b>Name:</b>	Data minimisation	<b>Type:</b>	Privacy enhancing
<b>Description:</b>	To provide the OTMs for the SME to limit that personal data processed to what is necessary and not hold more than is absolutely needed for the processing operation.				
<b>Rationale in SENTINEL:</b>	SENTINEL will recommend technologies that make data minimisation feasible at various layers of the data stack to offer better privacy by design in the transformed data processing operations.				
<b>Means of technical implementation:</b>	Policy recommendations and external components (T3.3, T3.4, T2.4)				
<b>ID</b>	PET003	<b>Name:</b>	Data anonymisation, pseudonymisation, obfuscation	<b>Type:</b>	Privacy enhancing
<b>Description:</b>	To provide the technical means for the SME to de-identify personal data, rendering them anonymous or unreadable to potential threats, ensuring privacy by design.				
<b>Rationale in SENTINEL:</b>	SENTINEL will recommend technologies that improve privacy by design in the transformed data processing operations.				
<b>Means of technical implementation:</b>	Policy recommendations and external components (T3.3, T3.4, T2.4)				
<b>ID</b>	PET004	<b>Name:</b>	Advanced PETs	<b>Type:</b>	Privacy enhancing
<b>Description:</b>	To provide state-of-the-art privacy enhancing techniques such as differential privacy, secure multiparty computation, homomorphic encryption and zero-knowledge proofs.				
<b>Rationale in SENTINEL:</b>	SENTINEL will recommend technologies that improve privacy by design through state-of-the-art PETs in the transformed data processing operations only in specific scenarios where such advanced techniques are suitable and attainable for the SME.				
<b>Means of technical implementation:</b>	Policy recommendations and external components (T3.3, T3.4, T2.4)				
<b>ID</b>	CS001	<b>Name:</b>	Endpoint security	<b>Type:</b>	Cybersecurity technical
<b>Description:</b>	To provide the technical means (software) for securing SME end-user devices such as desktops, laptops, and mobile devices from being maliciously exploited by CS threats.				
<b>Rationale in SENTINEL:</b>	SENTINEL should go beyond mere antivirus software recommendation and incorporate more holistic endpoint protection OTMs such as threat detection, investigation, and response, endpoint device management, data leak protection (DLP), among others, to face today's evolving threat landscape.				
<b>Means of technical implementation:</b>	Policy recommendations and external components (T3.3, T3.4, T2.4)				
<b>ID</b>	CS002	<b>Name:</b>	Vulnerability assessment, penetration testing	<b>Type:</b>	Cybersecurity technical
<b>Description:</b>	To provide the technical capabilities for identifying risks and vulnerabilities in the SME's computer and network infrastructure, hardware, applications, and other IT assets, including by means of safely exploiting these vulnerabilities.				

<b>Rationale in SENTINEL:</b>	SENTINEL provides a number of components as part of its core framework which assess and evaluate an organisation's CS vulnerabilities. Their individual capabilities will be defined in details and the resulting metadata used for smart recommendations, configuration and policy drafting.			
<b>Means of technical implementation:</b>	Security Infusion (T2.3), MITIGATE (T2.3), Integrated security and privacy assurance suite (T4.2), Airbus CyberRange (T4.1), Policy recommendations and external components (T3.3, T3.4, T2.4) when necessary.			
<b>ID</b>	CS003	<b>Name:</b>	Email security	<b>Type:</b> Cybersecurity technical
<b>Description:</b>	To provide the technical means for protecting the SME's email accounts, email content, and related communications against unauthorized access, loss or compromise, including retention for legal and forensic purposes as per statutory requirements.			
<b>Rationale in SENTINEL:</b>	SENTINEL will recommend technologies that improve email cybersecurity both at the email server level where required (e.g., email proxies and secure gateways) and at the endpoints (e.g., MFA, encryption, etc).			
<b>Means of technical implementation:</b>	Policy recommendations and external components (T3.3, T3.4, T2.4)			
<b>ID</b>	CS004	<b>Name:</b>	Network security	<b>Type:</b> Cybersecurity technical
<b>Description:</b>	To recommend and implement OTMs to protect the usability, availability and integrity of the SME's network and data from all CS threats and data breaches.			
<b>Rationale in SENTINEL:</b>	Creating a secure network infrastructure for SMEs can be a complex task that includes many policy and technical implementation points. SENTINEL will provide the means to audit the SME's current infrastructure configuration, the balance of on-premises vs Cloud resources and their individual configurations and recommend the proper policy and OTMs to secure it.			
<b>Means of technical implementation:</b>	Airbus CyberRange (T4.1), MITIGATE (T2.3), Security Infusion (T2.3), Integrated security and privacy assurance suite (T4.2), Policy recommendations and external components (T3.3, T3.4, T2.4) as necessary.			
<b>ID</b>	CS005	<b>Name:</b>	IAM (identity/access mgmt.)	<b>Type:</b> Cybersecurity technical
<b>Description:</b>	This refers to the technical implementation of generic requirement GEN003. The recommended technical means should be able to define and manage the roles and access privileges of individual entities (users and devices) to the SME's Cloud and on-premises apps, endpoint devices and network resources at both the low (e.g., network resource, infrastructure) and high (app, SSO, etc) layers of the IT stack.			
<b>Rationale in SENTINEL:</b>	SENTINEL will recommend IAM policy and OTMs which are fit for the company's size and asset configurations, taking into account potential Cloud implementations.			
<b>Means of technical implementation:</b>	Policy recommendations and external components (T3.3, T3.4, T2.4) as required.			
<b>ID</b>	CS006	<b>Name:</b>	Cloud security	<b>Type:</b> Cybersecurity technical
<b>Description:</b>	To provide third-party (Cloud)-delivered and monitored CS services			
<b>Rationale in SENTINEL:</b>	SENTINEL will recommend third-party cybersecurity-as-a-service solutions when these can fill identified gaps in the drafted policy, as far as the requirements for usability, scalability and cost-effectiveness are satisfied.			

<b>Means of technical implementation:</b>	Policy recommendations and external components (T3.3, T3.4, T2.4) as required.				
<b>ID</b>	CS007	<b>Name:</b>	Software lifecycle security	<b>Type:</b>	Cybersecurity technical
<b>Description:</b>	To provide the technical means to recommend and monitor cybersecurity requirements during software development lifecycles (SDLC)				
<b>Rationale in SENTINEL:</b>	SENTINEL will prescribe secure SDLC practices and policies for SMEs who have in-house software development as a core process.				
<b>Means of technical implementation:</b>	Policy recommendations and external components (T3.3, T3.4, T2.4) as required.				
<b>ID</b>	CS008	<b>Name:</b>	Monitoring and alerting	<b>Type:</b>	Cybersecurity technical
<b>Description:</b>	To provide the technical capabilities to continuously monitor the SME's IT assets for vulnerabilities and enforcement of policy, and send alerts to the associated event management system and personnel, in the case of incidents.				
<b>Rationale in SENTINEL:</b>	SENTINEL provides a number of components as part of its core framework which provide robust monitoring and alerting functionality				
<b>Means of technical implementation:</b>	Security Infusion (T2.3), MITIGATE (T2.3), Integrated security and privacy assurance suite (T4.2), Policy recommendations and external components (T3.3, T3.4, T2.4) when necessary.				
<b>ID</b>	CS009	<b>Name:</b>	Logging	<b>Type:</b>	Cybersecurity technical
<b>Description:</b>	Logging is the technical instantiation of the generic requirement for Accounting as part of AAA (GEN003) – to provide the technical components which will record all cybersecurity-related events in the SME's servers, networks, workstations, applications and other IT assets. These records should not be modifiable or erasable and should support auditing requirements.				
<b>Rationale in SENTINEL:</b>	SENTINEL provides a number of components as part of its core framework which provide robust logging functionality				
<b>Means of technical implementation:</b>	Security Infusion (T2.3), MITIGATE (T2.3), Integrated security and privacy assurance suite (T4.2), Policy recommendations and external components (T3.3, T3.4, T2.4) when necessary.				
<b>ID</b>	CS010	<b>Name:</b>	Analytics and visualisation	<b>Type:</b>	Cybersecurity technical
<b>Description:</b>	To provide the technical means, strategies, processes, and tools to diagnose, predict, and prevent cybersecurity incidents, along with the visualisations that can make data analysis understandable and actionable to analysts.				
<b>Rationale in SENTINEL:</b>	SENTINEL provides a dedicated component for advanced forensic visualisations and analytics.				
<b>Means of technical implementation:</b>	Forensics Visualisation Toolkit (T5.1), (T5.2). Policy recommendations and external components (T3.3, T3.4, T2.4) when necessary.				