


Tailored IoT & BigData Sandboxes and Testbeds for Smart,  
Autonomous and Personalized Services in the European  
Finance and Insurance Services Ecosystem



D2.8 – Security and Regulatory Compliance  
Specifications – Version II

<b>Revision Number</b>	3.0
<b>Task Reference</b>	T2.4
<b>Lead Beneficiary</b>	FTS
<b>Responsible</b>	Jürgen Neises
<b>Partners</b>	AKTIF ATOS ASSEN BOI BOS BPFI BS FBK FTS GFT GRAD JSI LIB NBG PI SIA SILO
<b>Deliverable Type</b>	Report (R)
<b>Dissemination Level</b>	Public (PU)
<b>Due Date</b>	2020-12-31
<b>Delivered Date</b>	2020-12-31
<b>Internal Reviewers</b>	BOUN, RB
<b>Quality Assurance</b>	GFT
<b>Acceptance</b>	WP Leader Accepted and Coordinator Accepted
<b>EC Project Officer</b>	Pierre-Paul Sondag
<b>Programme</b>	HORIZON 2020 - ICT-11-2018
	This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement no 856632

## Contributing Partners

Partner Acronym	Role	Author(s)
<b>FTS</b>	Lead Beneficiary	Jürgen Neises
<b>ASSEN</b>	Contributor	Ilesh Dattani
<b>ATOS</b>	Contributor	Nuria Ituarte
<b>BANKIA</b>	Contributor	Elena Femenia
<b>BOC</b>	Contributor	Silvio Walser
<b>BOS</b>	Contributor	Maja Skrjanc, Klaudija Jurkosek-Seitl
<b>CP</b>	Contributor	Marinos Xynarianos
<b>NBG</b>	Contributor	
<b>BOUN</b>	Reviewer	Can Özturan
<b>GFT</b>	Reviewer	Ernesto Troiano
<b>RB</b>	Reviewer	Alexander D. Kostopoulos

## Revision History

Version	Date	Partner(s)	Description
0.1	2020-11-23	FTS, ASSEN	ToC Version
0.2	2020-12-03	FTS, ASSEN, BANKIA, BOC, BOS, CP, CXB, NBG	Pilot contributions Relevant Standards List of organizational measures Requirements for Testbeds Document merge
0.3	2020-12-06	ASSEN	Description of relevant standards and TOMs
0.4	2020-12-11	FTS, BOS,	Mapping of pilots, AI focus
0.5	2020-12-14	ASSEN, FTS	Merging of requirement lists
0.6	2020-12-15	BOS	Recommendations on AI
0.7	2020-12-16	FTS	Merging, editing tables, etc., Introduction
0.8	2020-12-18	FTS	First Version for Internal Review
0.9	2020-12-28	BOUN, FTS	Version including 1 <sup>st</sup> internal Review results
1.0	2020-12-29	GFT, RB, FTS	Version including 2 <sup>nd</sup> internal Review results
2.0	2020-12-30	FTS	Version for Quality Assurance
3.0	2020-12-31	FTS/GFT	Version for Submission

## Executive Summary

The Deliverable updates the findings documented in D2.7. It specifies requirements relevant for the INFINITECH project resulting from state-of-the-art security and privacy standards, e.g. ISO 27000, NIST Cyber Security Framework, which define technical and organisational measures for achieving an appropriate level of security and privacy in ICT solutions and service provisioning.

Moreover, technical and organisational measures derive from previously outlined regulations in D2.7. The applicability of these regulations to the various pilots - based on the latest pilot descriptions,- was assessed and mapped to each pilot. As a result, requirements related to technical measures for each testbed, sandbox and technology were specified and related to the pilots.

The organizational measures resulting from standards and regulations highly overlap thus these were consolidated in a joint list.

Finally, the state of requirements resulting from AI regulations was assessed and for each pilot a list of requested activities is proposed.

Overall, the requirements are specifying technical and organizational measures for each pilot and their testbeds, sandboxes and applied technologies. However, the specific and appropriate implementation of measures needs to be defined within each pilot related to the organizational and operational framework it will be deployed.

# Table of Contents

1	Introduction .....	7
1.1	Objective of the Deliverable .....	7
1.2	Insights from other Tasks and Deliverables.....	7
1.3	Structure of the Document.....	7
2	INFINITECH related Security Requirements.....	9
2.1	Overview.....	9
2.2	Security Standards .....	10
2.2.1	ISO/IEC 27001 – Information technology: Security techniques, Information security management systems Requirements. ....	10
2.2.2	ISO 27701 Privacy Information Management System (PIMS) .....	13
2.2.3	The Payment Card Industry Data Security Standard (PCI DSS).....	14
2.2.4	National Institute of Standards and Technology (NIST) Cyber Security Framework – Financial Services Cyber Security Profile.....	15
2.3	The General Data Protection Regulation (GDPR) .....	17
2.3.1	Overview .....	17
2.3.2	Technology Impact.....	17
2.3.3	Organizational Impact.....	18
2.3.4	Privacy by Design – PRIPARE Methodology .....	18
2.3.5	PRIPARE Methodology .....	19
2.3.6	Phases .....	20
2.3.7	Security and privacy team.....	21
2.3.8	Application to INFINITECH pilots.....	22
2.4	PSD II.....	23
2.4.1	Overview .....	23
2.4.2	Technology Impact.....	24
2.5	MIFID II .....	26
2.5.1	Overview .....	26
2.5.2	Technology Impact.....	27
2.6	AMLD4 .....	28
2.6.1	Overview .....	28
2.6.2	Technology Impact.....	29
3	Impact on INFINITECH Pilots .....	30
3.1	Update on Pilots - Regulatory Impact.....	30
3.1.1	GDPR .....	30
3.1.2	PSD II .....	30
3.1.3	MIFID II.....	30
3.1.4	AMLD4.....	31

3.2	Update on Pilots’ Technical Measures .....	31
3.3	Organizational Measures for Security and Compliance .....	32
3.4	Pilot Recommendations .....	33
4	Focus Point AI.....	35
4.1	Recommendations to the INFINITECH Pilots .....	38
5	Conclusions .....	42
6	References .....	43

## List of Figures

Figure 1: PRIPARE’s methodology reference model [6] .....	19
Figure 2: PRIPARE methodology phases [6] .....	21
Figure 3: AI Model framework [14] .....	36

## List of Tables

Table 1: List of relevant requirements resulting from ISO 27001 .....	12
Table 2: List of relevant requirements resulting from ISO 27701 .....	13
Table 3: List of relevant requirements resulting from PCI DSS .....	15
Table 4: List of relevant requirements resulting from Cyber Security Framework – Financial Services Cyber Security Profile .....	16
Table 5: List of relevant requirements resulting from PSD II .....	26
Table 6: Relevant Requirements resulting from MIFID II .....	28
Table 7: Relevant Requirements resulting from AMLD4.....	29
Table 8: Applicability of Regulations in Pilots.....	32
Table 9: Organizational Measures and Requirements .....	32
Table 10: Technical and Operational Measures per pilot .....	33
Table 11: Recommendations on AI per Pilot .....	39

## Abbreviations/Acronyms

Abbreviation	Definition
AML	Anti-Money-Laundering
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
GDPR	General Data Protection Regulation
MIFID	Markets in Financial Instruments Directive
MiFIR	Markets in Financial Instruments and Amending Regulation
NDA	Non-Disclosure Agreement
NIS	Network and Information Systems
OES	Operators of Essential Services
PAN	Primary Account Number
PaaS	Platform as a Service
PCI DSS	Payment Card Industry Data Security Standard
PIA	Privacy Impact Assessment
PSD2	Payment Service Directive 2
PSP	Payment Service Provider
PSU	Payment Service User
P2PP	Peer-to-Peer Payment
RTS	Regulatory Technical Standard
QTSP	Qualified Trust Service Provider
SCA	Strong Customer Authentication
SME	Small and Medium-Sized Enterprises
SA	Supervisory Authority
SECaaS	Security-as-a- Service
TI	Threat Intelligence
3DS	Three-Domain Secure

# 1 Introduction

Security and privacy rely on numerous standards and regulations, which are usually designed for companies and related to policies and vary from company to company. Thus, the design that will aim at covering the security standards and regulations for an R&I project is a difficult task. Moreover, these standards and regulations request technical and organizational measures. Overall, compliance is not just a matter of technology, even if there often is the illusion of security or privacy being covered switching on some tool or box.

Therefore, various standards-based frameworks that are commonly used to ensure security and privacy in the financial sector have been assessed (i.e., ISO 27001, PCI DSS, NIST Standards). Likewise, security and privacy related regulations and directives (e.g., GDPR, PSD II, MIFID II, AML4) are also addressed. According to the progresses in the pilots the standards and regulations, which apply to the pilots are listed.

Considering GDPR compliance the PRIPARE methodology is described in addition to the CNIL PIA, which was introduced in the previous version of the deliverable.

This deliverable finally specifies the technology and organizational impact of relevant standards and regulations that shall be considered in the INFINITECH testbeds and sandboxes, and which shall guide the utilization of INFINITECH security and privacy technologies, and solutions used in the development. The resulting requirements are gathered per standard / regulation and mapped to the pilots and thus their testbeds, sandboxes and utilized technologies.

This way, the guideline for the INFINITECH testbeds can be applied in general, where the relevant standards or regulations apply for timely preparedness before application in business.

Finally, AI is an evolving technology, and it is critical to ensure that the regulatory environment is fit for the use of AI by promoting innovation and legal certainty. In addition to the common security standards a special emphasis is put on AI and requirements for its ethical application. Since, official recommendations or guidelines are under construction yet, only a general guideline based on the current state of discussions is presented and applied to the pilots.

Please, note, that the INFINITECH pilots #5 and #7 are confidential and that pilot #8 is restricted to the consortium. Thus, descriptions related to these pilots are excluded from this document. In case of specific interest, please, contact the INFINITECH project at <https://www.infinitech-h2020.eu/contact-us>.

## 1.1 Objective of the Deliverable

This deliverable updates the information of D2.7 with respect to changes within the pilots. Moreover, it provides the final specifications of relevant requirements based on security and privacy standards and regulations.

## 1.2 Insights from other Tasks and Deliverables

The pilot assessments of D2.4 support the final analysis, which standards and regulation apply per pilot. The results of D3.15 gave insight into technical measures taken by the pilots.

## 1.3 Structure of the Document

Section 2 elicits the INFINITECH related security Requirements. Subsection 2.1 illustrates relevant standards and regulations

- Subsection 2.2 describes the impact of the most relevant standards.
- Subsection 2.3 describes the impact of the GDPR and the PRIPARE methodology guideline

- Subsections 2.4 to 2.6 are devoted to PSD II, MIFID II and AMLD4. In all the subsections related technical measures are specified.

Section 3 maps the technical and organizational measures related to the standards and regulations to the INFINITECH pilots

In section 4 the latest information on the regulation of AI in Europe and especially for the Financial Services sector are outlined. Related requirements for INFINITECH are specified.

Section 5 concludes the document.



## 2 INFINITECH related Security Requirements

### 2.1 Overview

Considering that the INFINITECH project will innovate the landscape of financial services facilitating the deployment of BigData driven services, it is a valid approach to consider that the standards and guidelines, which apply to the specific business, are applied in the financial industry and thus the financial sector beneficiaries of the project according to the state of the art and with best industry practice.

In the previous version of this deliverable a set of regulations, with the most relevant impact on INFINITECH have been identified:

- GDPR
- PSD II
- MIFID II
- AMLD4

Moreover, general security requirements around maintaining confidentiality, availability and integrity are implemented in order to maintain the basic compliance within the services created and/or deriving from the pilots.

A financial institutions compliance with the relevant regulations like GDPR, ISO 27001, PSD II etc. does not immediately mean that any new technologies or services will inherently be compliant unless the specific measures where appropriate are implemented both in the development and governance procedures around any new product and/or service resulting from these pilots.

The adoption of security-by-design is essential for maintaining the confidentiality, integrity, availability and resilience of the data held by the organization. The adoption of privacy-by-design is key to demonstrating appropriate processing of personal information and reducing the risk of data breaches.

All pilots should ensure that the collection, storage, transmission and processing of data meet security- and privacy-by-design principles to prevent data leakage, whether by accidental or unlawful destruction, loss, alteration, unauthorized disclosure or intrusion, or accidental or unauthorized data exposure. The adoption of security- and privacy-by-design is an essential principle to minimize risk of data loss, breach, harm to individuals or other infractions.

Before data are published to external stakeholders or shared with specific organizations within the context of the pilots, the risks of these activities to the publishing of the following should be determined:

- a) intellectual property.
- b) commercially sensitive information.
- c) information on sensitive assets/systems.
- d) personal information.
- e) identity of, and impact on, individuals.

The following controls should be followed where necessary

- a) ensure private organizational or personal information and identities remain private where required;
- b) ensure that shared organizational or personal information is treated confidentially by the recipient;
- c) ensure that proprietary organizational and personal information is treated as the private property of related organizations and individuals with intrinsic value that is respected and protected and equitable means provided for realizing that value;

- d) provide individuals with a transparent view of data processing activities and the ability to exercise their rights related to any data processing of their personal information that is not required or permitted by law;
- e) ensure that data activities are respectful of, and do not interfere with, human will/ self-determination; and
- f) ensure that data processing approaches and results do not present unfair or prejudicial biases to individuals or groups of individuals.

## 2.2 Security Standards

The goal of security standards is to improve the security of information technology (IT) systems, networks, and critical infrastructures. A cyber security standard defines both functional and assurance requirements within a product, system, process, or technology environment.

These standards are cross-cutting state-of-the-art security standards and apply to all pilots, testbeds, sandboxes and technologies. However, the pilots should consider the intended operational environment when deciding to implement a specific requirement.

### 2.2.1 ISO/IEC 27001 – Information technology: Security techniques, Information security management systems Requirements.

ISO/IEC 27001 is the international standard focused on information security, from the International Organization for Standardization (ISO), in partnership with the International Electrotechnical Commission (IEC). It was developed to help organizations, of any size or any industry, to protect their information in a systematic and cost-effective way, through the adoption of an Information Security Management System (ISMS).

The ISMS is a system that helps to prevent and counteract interruptions to business activities. It facilitates management, monitoring and auditing of an organization's information security practice in a comprehensible way. Moreover, the ISMS based on ISO 27001 principles supports protection of company information, intellectual property, and personal data. It protects critical processes from the effects of information security incidents, disasters and major failures of information systems and ensures the timely continuation of normal operations. It specifically enables the following:

1. identify stakeholders and their expectations of the company in terms of information security
2. identify which risks exist for the information
3. define controls (safeguards) and other mitigation methods to meet the identified expectations and handle risks
4. set clear objectives on what needs to be achieved with information security
5. implement all the controls and other risk treatment methods
6. continuously measure if the implemented controls perform as expected
7. make continuous improvement to make the whole ISMS work better

The basic goal of ISO 27001, and from the perspective of the Infinitech Pilots, is to protect three aspects of information:

- **Confidentiality:** only the authorized persons have the right to access information.
- **Integrity:** only the authorized persons can change the information.
- **Availability:** the information must be accessible to authorized persons whenever it is needed.

The policies, processes, procedures and other requirements that make up this management system are scrutinised and tested annually by independent 3rd-party auditors.

The mandatory requirements within the standard are laid out in clause 4 through to 10 and in essence cover the following:

<b>Clause 4: Context of the organization</b> – defines requirements for understanding external and internal issues, interested parties and their requirements, and defining the ISMS scope.
<b>Clause 5: Leadership</b> – defines top management responsibilities, setting the roles and responsibilities, and contents of the top-level Information Security Policy.
<b>Clause 6: Planning</b> – defines requirements for risk assessment, risk treatment, Statement of Applicability, risk treatment plan, and setting the information security objectives.
<b>Clause 7: Support</b> – defines requirements for availability of resources, competencies, awareness, communication, and control of documents and records.
<b>Clause 8: Operation</b> – defines the implementation of risk assessment and treatment, as well as controls and other processes needed to achieve information security objectives.
<b>Clause 9: Performance evaluation</b> – defines requirements for monitoring, measurement, analysis, evaluation, internal audit, and management review.
<b>Clause 10: Improvement</b> – defines requirements for nonconformities, corrections, corrective actions, and continual improvement.

These are all made up of controls, which in effect need to be implemented. They can be broken down into:

- **Technical controls:** implemented in information systems, using software, hardware, and firmware components added to the system. E.g. backup, antivirus software, etc.
- **Organizational controls:** implemented by defining rules to be followed, and expected behaviour from users, equipment, software, and systems. E.g. Access Control Policy, BYOD Policy, etc.
- **Legal controls:** implemented by ensuring that rules and expected behaviours follow and enforce the laws, regulations, contracts, and other similar legal instruments that the organization must comply with. E.g. NDA (non-disclosure agreement), SLA (service level agreement), etc.
- **Physical controls:** implemented by using equipment or devices that have a physical interaction with people and objects. E.g. CCTV cameras, alarm systems, locks, etc.
- **Human resource controls** are implemented by providing knowledge, education, skills, or experience to persons to enable them to perform their activities in a secure way. E.g. security awareness training, ISO 27001 internal auditor training, etc.

Within the context of delivering services based on technology and thereby the development and deployment of those services data protection controls should identify the most critically important data assets, as well as policies and procedures that facilitate the meeting of legal requirements for data privacy. Basic controls should also define key roles and responsibilities for protecting data, as well as foundational protections like secure passwords, two-factor authentication, and mobile device controls. Within ISO 27001 this means specific implementation of the following clauses and controls:

<b>Clause 6.1.3 Information security risk treatment</b> Compliance with this clause of the standard requires organizations to produce a Statement of Applicability that defines the necessary controls and whether they are implemented or not.
<b>Control A.8.2.1 Classification of information</b> This control provides guidance for classifying information in terms of legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification.
<b>Control A.18.1.4 Privacy and protection of personally identifiable information</b> This control provides guidance on how to ensure privacy and protection of personally identifiable information as required in relevant legislation and regulation where applicable.
<b>Control A.6.1.1 Information security roles and responsibilities</b>

This control provides guidance on how information security responsibilities for assets and information security processes should be defined and allocated.
<b>Control A.9.3.1 Use of secret authentication information</b> This control provides guidance on how users should be required to follow the organization’s practices in the use of secret authentication information (e.g. passwords).
<b>Control A.9.4.3 Password management system</b> This control provides guidance on how password management systems should be selected and configured to be interactive and ensure quality passwords.
<b>Control A.6.2.1 Mobile device policy</b> This control provides guidance on how to adopt a policy and supporting security measures to manage the risks introduced by using mobile devices.

Conformance to ISO 27001 shows that

- steps have taken for systematic identification and management of data and other security risks
- appropriate measures have been implemented to mitigate those risks, for instance recommended technical measures related to the requirements of the GDPR.
- appropriate technical controls, policies and procedures are in place for reducing, monitoring and reviewing security risks
- the company is aware of information security and the related requirements
- the ISMS follows internationally accepted standards and good information security practice.

Table 1: List of relevant requirements resulting from ISO 27001

<b>GMS-0001 Security Information and Event Management (SIEM)</b>
Logging capabilities on security events for enterprises used to analyse and/or report on the log entries received.
<b>GMS-0002 Risk Management/Monitoring</b>
Track risk and mitigations, rank hazards by their critical value, produce reports and manage compliance
<b>GMS-0003 Security Awareness &amp; Training</b>
Provide awareness training and set out key security requirements and practices within the context of the applications and/or services being provided
<b>GMS-0004 Password Policy Enforcement</b>
Gives administrators the power to impose certain password policies on users when they choose a password such as: <ul style="list-style-type: none"> <li>• Complexity. Requires passwords to contain characters from a variety of character sets (such as digits, upper case characters and so on). The required number and selection of character sets are usually configurable.</li> <li>• Contained in a dictionary. Passwords must not be vulnerable to attack with a dictionary or hybrid cracking algorithm. The tools should be sophisticated enough to detect partial matches, character substitution and character reversal.</li> <li>• Keyboard pattern. This prohibits passwords with keyboard patterns such as “qwerty” or “asdfasdf.”</li> <li>• Repeating patterns. This disallows passwords with repeated characters, such as “aaaabbbb” or repeated patterns such as “monkeymonkey.”</li> <li>• Similarity. This detects when a user is choosing passwords with an obvious sequence, like “password1” or “password2” each time the password is changed.</li> </ul>
<b>GMS-0005 Information Asset Management</b>
To identify and record the data subjects, volumes held, retention periods and who has access to the assets and their contents.
<b>GMS-0006 Anonymization</b>
The process of removing personal identifiers, both direct and indirect, that may lead to an individual being identified. An individual may be <i>directly identified</i> from their name, address, postcode, telephone number,

<p>photograph or image, or some other unique personal characteristic. An individual may be <i>indirectly identifiable</i> when certain information is linked together with other sources of information, including, their place of work, job title, salary, their postcode</p>
<p><b>GMS-0007 Pseudonymization</b></p>
<p>A technique that is used to reduce the chance that personal <b>data</b> records and identifiers lead to the identification of the natural person (<b>data</b> subject) whom they belong too. Identifiers make identification of a <b>data</b> subject possible.</p>
<p><b>GMS-0008 Authentication and Authorization mechanisms</b></p>
<p>Strong and secure Access Management to prevent unauthorised access</p>
<p><b>GMS-0009 Data Encryption</b></p>
<p>Method where information is encoded and can only be accessed or decrypted by a user with the correct <b>encryption key</b>. Encrypted data, also known as ciphertext, appears scrambled or unreadable to a person or entity accessing without permission.</p>
<p><b>GMS-0010 Data Discovery and Classification</b></p>
<p>Visibility of sensitive data held by the organisation with efficient data discovery, classification, and risk analysis across heterogeneous data stores - the cloud, big data, and traditional environments - in the enterprise.</p>

## 2.2.2 ISO 27701 Privacy Information Management System (PIMS)

ISO/IEC 27701:2019 is a privacy extension to the international information security management standard, ISO/IEC 27001 (ISO/IEC 27701 Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines). ISO 27701 specifies the requirements for – and provides guidance for establishing, implementing, maintaining, and continually improving – a PIMS (privacy information management system).

ISO 27701 is based on the requirements, control objectives and controls of ISO 27001, and includes a set of privacy-specific requirements, controls, and control objectives.

The EU General Data Protection Regulation requires organisations to take measures to ensure the privacy of any personal data that they process. However, the legislation does not provide specific guidance on what those measures should look like. ISO 27701 is intended as a result to support organizations with guidance on the specific measures.

The standard outlines a comprehensive set of operational controls that can be mapped to various regulations, including the GDPR. Once mapped, the PIMS operational controls are implemented by privacy professionals and audited by internal or third-party auditors resulting in a certification and comprehensive evidence of conformity.

PIMS includes new controller- and processor-specific controls that help bridge the gap between privacy and security and provides a point of integration between what may be two separate functions in organizations. Privacy depends on security. Likewise, PIMS depends on ISO/IEC 27001 for security management.

The key requirements that result from this are listed in Table 1 below.

Table 2: List of relevant requirements resulting from ISO 27701

<p><b>GMS-0006 Anonymization (see above)</b></p>
<p>The process of removing personal identifiers, both direct and indirect, that may lead to an individual being identified. An individual may be <i>directly identified</i> from their name, address, postcode, telephone number, photograph or image, or some other unique personal characteristic. An individual may be <i>indirectly identifiable</i> when certain information is linked together with other sources of information, including, their place of work, job title, salary, their postcode</p>
<p><b>GMS-0011 Pseudonymization</b></p>
<p>A technique that is used to reduce the chance that personal <b>data</b> records and identifiers lead to the</p>

identification of the natural person ( <b>data</b> subject) whom they belong too. Identifiers make identification of a <b>data</b> subject possible.
<b>GMS-0012 Authentication and Authorization mechanisms</b>
Strong and secure Access Management to prevent unauthorised access
<b>GMS-0009 Data Encryption (see above)</b>
Method where information is encoded and can only be accessed or decrypted by a user with the correct <b>encryption key</b> . Encrypted data, also known as ciphertext, appears scrambled or unreadable to a person or entity accessing without permission.
<b>GMS-0010 Data Discovery and Classification (see above)</b>
Visibility of sensitive data held by the organisation with efficient data discovery, classification, and risk analysis across heterogeneous data stores - the cloud, big data, and traditional environments - in the enterprise.

### 2.2.3 The Payment Card Industry Data Security Standard (PCI DSS)

The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards formed in 2004. The compliance scheme aims to secure credit and debit card transactions against data theft and fraud. The PCI SSC (Payment Card Industry Security Standards Council) has no legal authority to compel compliance, it is however a requirement for any business that processes credit or debit card transactions. It is also considered the best way to safeguard sensitive data and information.

It ensures the security of card data through a set of requirements established by the PCI SSC. These include a number of commonly known best practices, such as:

- Installation of firewalls
- Encryption of data transmissions
- Use of anti-virus software
- restrict access to cardholder data
- monitor access to network resources

PCI compliance is divided into four levels, based on the annual number of credit or debit card transactions and business processes. The classification level determines what an enterprise needs to do to remain compliant.

<b>Level 1:</b> Applies to merchants processing more than six million real-world credit or debit card transactions annually. Conducted by an authorized PCI auditor, they must undergo an internal audit once a year. In addition, once a quarter they must submit to a PCI scan by an Approved Scanning Vendor (ASV).
<b>Level 2:</b> Applies to merchants processing between one and six million real-world credit or debit card transactions annually. They're required to complete an assessment once a year using a Self-Assessment Questionnaire (SAQ). Additionally, a quarterly PCI scan may be required.
<b>Level 3:</b> Applies to merchants processing between 20,000 and one million e-commerce transactions annually. They must complete a yearly assessment using the relevant SAQ. A quarterly PCI scan may also be required.
<b>Level 4:</b> Applies to merchants processing fewer than 20,000 e-commerce transactions annually, or those that process up to one million real-world transactions. A yearly assessment using the relevant SAQ must be completed and a quarterly PCI scan may be required.

**Twelve specific requirements for testbeds related to payment actions are listed in Table 3 below:**

Table 3: List of relevant requirements resulting from PCI DSS

<b>GMS-0013 Secure network</b>
A firewall configuration must be installed and maintained
System passwords must be original (not vendor-supplied)
<b>GMS-0014 Secure cardholder data</b>
Stored cardholder data must be protected
Transmissions of cardholder data across public networks must be encrypted
<b>GMS-0015 Vulnerability management</b>
Anti-virus software must be used and regularly updated
Secure systems and applications must be developed and maintained
<b>GMS-0016 Access control</b>
Cardholder data access must be restricted to a business need-to-know basis
Every person with computer access must be assigned a unique ID
Physical access to cardholder data must be restricted
<b>GMS-0017 Network monitoring and testing</b>
Access to cardholder data and network resources must be tracked and monitored
Security systems and processes must be regularly tested
<b>GMS-0018 Information security</b>
A policy dealing with information security must be maintained

## 2.2.4 National Institute of Standards and Technology (NIST) Cyber Security Framework – Financial Services Cyber Security Profile

The framework from NIST provides best practices for voluntary use in all critical infrastructure sectors, including, for example, government, healthcare, financial services and transportation. It is designed to help organizations develop information security protection programs. Thus, the NIST Cyber Security Framework applies to all pilots, testbeds, sandboxes and technologies.

The Framework focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization's risk management processes. The Framework consists of three parts: the Framework Core, the Framework Profile, and the Framework Implementation Tiers. The Framework Core is a set of cybersecurity activities, outcomes, and informative references that are common across critical infrastructure sectors, providing the detailed guidance for developing individual organizational Profiles. Through use of the Profiles, the Framework will help the organization align its cybersecurity activities with its business requirements, risk tolerances, and resources. The Tiers provide a mechanism for organizations to view and understand the characteristics of their approach to managing cybersecurity risk. [1]

The United States Financial Services Sector Coordinating Council (FSSCC) along with a group of leading financial trade associations have defined a financial services sector Cybersecurity Profile. It is seen as one of the more detailed Cybersecurity Framework-based, sector regulatory harmonization approaches to-date.

Following [2] the Profile seeks to provide Financial Institutions and their third-party providers with more consistent and efficient processing of examination material by firms and regulators. It also helps regulators and firms to prioritize resources and focus on cyber threats of greatest concern.

The Financial Services Sector Cybersecurity Profile (or FSP) is a Framework based on:

- Completing the NIST Cybersecurity framework
- Integrating widely used standards and supervisory expectations
- Bringing plain language to benchmarking, risk management, audit, and in-house education

- Offering compliance efficiencies that grow with a Financial institution’s complexity
- Aiding prioritization and focused use of resources
- Enhancing internal and external oversight, due diligence and risk identification using consistent terms and concepts
- More efficient third-party vendor management review and oversight

Table 4: List of relevant requirements resulting from Cyber Security Framework – Financial Services Cyber Security Profile

<b>GMS-0019 Supplier Management</b>
Maintain quality, safety and risk management processes throughout the supply chain. Monitor Supplier Compliance and Capability
<b>GMS-0001 Security Information and Event Management (SIEM) (see above)</b>
Logging capabilities on security events for enterprises used to analyse and/or report on the log entries received.
<b>GMS-0020 Risk Management/Monitoring</b>
Track risk and mitigations, rank hazards by their critical value, produce reports and manage compliance
<b>GMS-0003 Security Awareness &amp; Training (see above)</b>
Provide awareness training and set out key security requirements and practices within the context of the applications and/or services being provided
<b>GMS-0004 Password Policy Enforcement (see above)</b>
<p>Gives administrators the power to impose certain password policies on users when they choose a password such as:</p> <ul style="list-style-type: none"> <li>• Complexity. Requires passwords to contain characters from a variety of character sets (such as digits, upper case characters and so on). The required number and selection of character sets are usually configurable.</li> <li>• Contained in a dictionary. Passwords must not be vulnerable to attack with a dictionary or hybrid cracking algorithm. The tools should be sophisticated enough to detect partial matches, character substitution and character reversal.</li> <li>• Keyboard pattern. This prohibits passwords with keyboard patterns such as “qwerty” or “asdfasdf.”</li> <li>• Repeating patterns. This disallows passwords with repeated characters, such as “aaaabbbb” or repeated patterns such as “monkeymonkey.”</li> <li>• Similarity. This detects when a user is choosing passwords with an obvious sequence, like “password1” or “password2” each time the password is changed.</li> </ul>
<b>GMS-0005 Information Asset Management (see above)</b>
To identify and record the data subjects, volumes held, retention periods and who has access to the assets and their contents.
<b>GMS-0008 Authentication and Authorization mechanisms (see above)</b>
Strong and secure Access Management to prevent unauthorised access
<b>GMS-0009 Data Encryption (see above)</b>
Method where information is encoded and can only be accessed or decrypted by a user with the correct <b>encryption key</b> . Encrypted data, also known as ciphertext, appears scrambled or unreadable to a person or entity accessing without permission.

These requirements are in proportion to ISO 27000 and thus apply to all pilots, testbeds, sandboxes and technologies



## 2.3 The General Data Protection Regulation (GDPR)

### 2.3.1 Overview

At its core, GDPR is a new set of rules designed to give EU citizens more control over their personal data. It aims to simplify the regulatory environment for business so both citizens and businesses in the European Union can fully benefit from the digital economy. Under the terms of GDPR, not only do organisations have to ensure that personal data is gathered legally and under strict conditions, but those who collect and manage it are obliged to protect it from misuse and exploitation, as well as to respect the rights of data owners - or face penalties for not doing so. The regulation relates specifically from the perspective of the project to the processing of 'personal data' meaning:

*“any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.”*

Processing within this context means *“any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movement. “*

Some guidance of related requirements is given in Article 32 of the GDPR, which requires organizations to take appropriate measures as

- Pseudonymization and encryption of personal data.
- Confidentiality, integrity, availability.
- Resilience of processing systems and services.
- Ability to restore the availability and access to personal data in a timely manner in case of an incident.
- Implementation of regular testing, assessment and evaluation of the effectiveness of technical and organizational measures for ensuring secure processing.
- Identification and mitigation of risks “from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data”.

This is achievable for instance by an effective ISMS conforming to ISO 27001.

### 2.3.2 Technology Impact

The Technology Impact of GDPR especially on FinTechs has been described in [3]: GDPR has an impact on the collection of data: FinTechs must demonstrate the integrity and validity of their customers' consent to the sharing, marketing and commercial use of their personal information. FinTechs will also have to tell customers the purposes for which they process and use the data and appoint a dedicated Data Protection Officer. Finally, failure to comply with GDPR principles, including properly recording the customer journey and the registration process, will incur heavy penalties. Penalties will be discretionary and, depending on the nature of the breach, range between 2% and 4% of worldwide revenue, with upper limits of Euros 10m and Euros 20m. Faced with these issues, FinTechs must demonstrate to customers their respect for the confidentiality of personal data within the architecture of their service solutions. Finally, the right to be forgotten, introduced under GDPR, brings into question the development, deployment and use of technologies such as Blockchain within financial services.

Most relevant technology impacts for the INFINITECH pilots result from requirement to use of pseudonymised or anonymized personal data (see also deliverable D3.5). Moreover, the requirements GMS-0006 and GMS-0011 already list those technical requirements. However, as stated above, adhering to the technical requirements resulting from ISO27001 will support compliance to GDPR.

### 2.3.3 Organizational Impact

Article 32 of the GDPR requires that appropriate policies, procedures and processes are in place to protect the personal data an organisation holds. Furthermore, an organization shall be able to demonstrate compliance. However, the Article does not provide detailed guidance regarding what should be done to achieve this. Instead, the GDPR refers to existing best practices and recommendations, such as ISO 27001, to minimise the risk of a data breach.

As with ISO 27001 technical measures are not enough for GDPR compliance and technology alone will not prevent a data breach.

- A comprehensive information security programme includes people and processes for provisioning of adequate protection.
- Poor processes and lack of security awareness are the most common points of failure in data security.
- In general a commitment and a continuous improvement of information security management across the organization is required to cover data protection.
- Isolated controls have only limited effect and leave weak spots open for attacks.

Having this in mind, security awareness, security policies and regular training and checks are indispensable to achieve an appropriate level of protection.

In section 3.1 the most relevant organizational measures and resulting requirements for the INFINITECH testbeds and pilot operations will be described.

### 2.3.4 Privacy by Design – PRIPARE Methodology

The term “Privacy by Design” was coined by Cavoukian [4], and it means that privacy should be a core consideration throughout the whole engineering process, from the design phases all the way through to the implementation and deployment of the enterprise application. PRIPARE (PREparing Industry to Privacy-by-design by supporting its Application in REsearch) is a support action funded by the European Union’s Seventh Framework Programme for research, technological development, and demonstration under grant agreement no 610613.

“The mission of PRIPARE is twofold:

- facilitate the application of a privacy and security -by-design methodology that will contribute to the advent of unhindered usage of Internet against disruptions, censorship and surveillance, support its practice by the ICT research community to prepare for industry practice;
- foster risk management culture through educational material targeted to a diversity of stakeholders”[5]

The main features of PRIPARE methodology:

- Flexible: Practitioners can choose the level and granularity of the application of the methodology depending on system and organization’s features and information collected and/or processed.
- Based on configurable privacy and security principles: The methodology principles can be modified to address organization’s internal practices or specific business regulations
- Covers the whole system and personal data lifecycle: It covers all the stages of the system engineering process.

- Based on best practices: PRIPARE has been designed extending best practices such as Data Protection Impact Assessments, Data protection risk management processes and privacy engineering methodologies (OASIS PMRM)

In December 2015, PRIPARE released a set of tools that help its practitioners to effectively follow the methodology:

- PRIPARE templates,
- Privacy Patterns catalogue
- Catalogue of privacy targets
- Catalogue of threats, Catalogue of privacy Controls
- Best practices

The most important contribution of PRIPARE on privacy engineering is “The privacy-and-security-by-design methodology handbook” [6] that captures and integrates the existing standards, practices on privacy engineering.

### 2.3.5 PRIPARE Methodology

The main concepts used by PRIPARE are represented in the following figure that shows the Reference Model, which relates the different concepts or entities. This map has to be considered when applying the methodology.

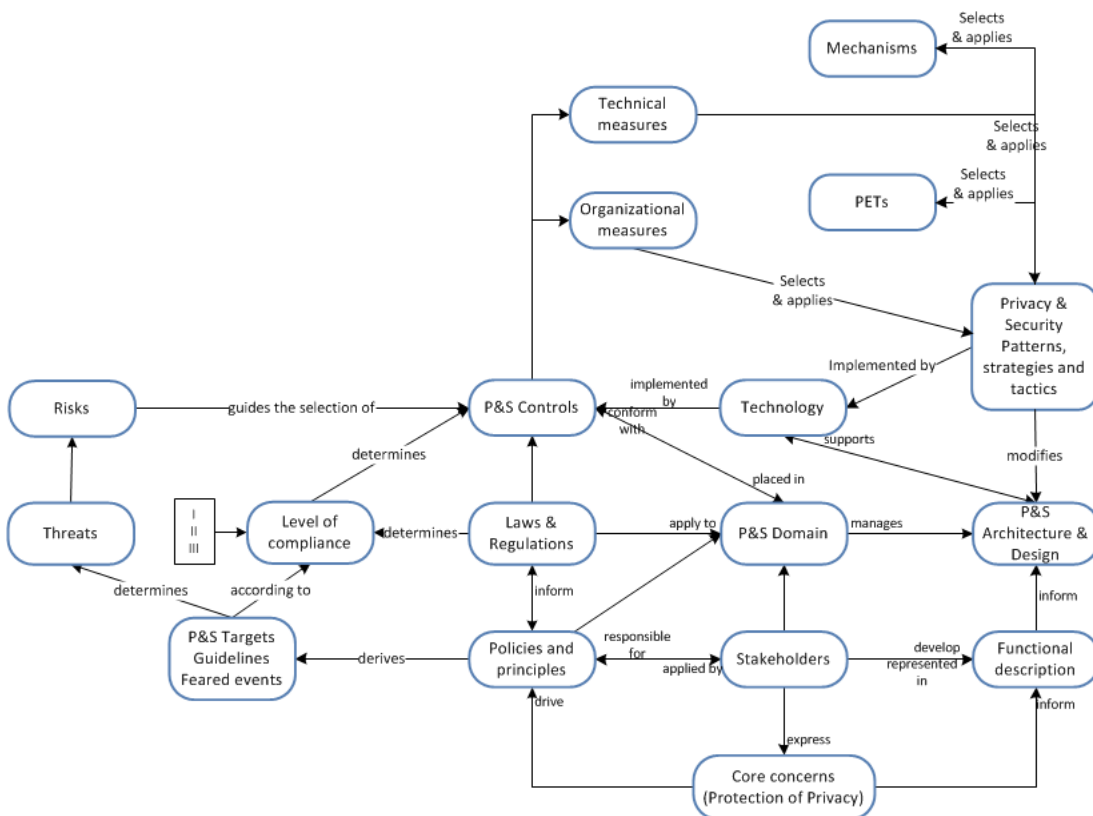


Figure 1: PRIPARE’s methodology reference model [6]

Some definitions within this reference model that need to be clarified:

- **Core concerns (Protection of Privacy):** any of the stakeholders involved (e.g. data subjects, policy makers, system developers, project owners...). This concerns help to drive policies and also prepare the functional requirements (functional description) that have to be designed and implemented in the various stakeholders’ domains.

- Privacy and security controls are measures that are used in organizations and systems to address privacy and security issues to be compliant with legislation and stakeholders' requirements. There are two types:
  - Technical measures, used at design time, e.g.: selecting a specific architecture, using specific security measure such as encryption, using specific privacy measures such as anonymous communication mechanisms, consent support, etc.
  - Organizational measures, which are management practices and processes integrated into the organization structure, e.g.: the appointment of a Data Protection Officer, designing of guidelines and policies within the organization, responsibility and accountability schemes, etc.
- Privacy & Security Domain: it refers to a physical or logical domain or area subject to the control of a Domain Owner(s).
- Threat: "Typical action used by risk sources that may cause a feared event [6]"
- Risk: "Scenario describing a feared event and all threats that make it possible. It is estimated in terms of severity and likelihood." [6]

### 2.3.6 Phases

The PRIPARE Methodology is structured in seven phases that match with system engineering phases easing the application of the methodology together with engineering practices and to standards such as ISO 15288:

- **Analysis:** The objective of this phase is to analyse the system from a security and privacy perspective to address the privacy and security issues during the design and implementation steps.
- **Design:** define all the components in the architecture, as well as interfaces the specified requirements are satisfied.
- **Implementation:** in this phase, the design is transformed to a system, and technology privacy and security principles and best practices must be followed.
- **Verification:** This phase checks that the system fulfils the privacy and security requirements. This can be checked by are performing reviews of code, audit or security testing, etc.
- **Release:** once the system has passed implementation and verification phases, there could be required final security & privacy reviews, after which it can be provided to the customer. During this phase it must be ensured that there is an action plan to respond to the privacy or security issues or breaches that may arise.
- **Maintenance:** in this phase, the system is running, so there need to be a responsible person that ensures the privacy and security by reacting to possible incidents that could happen. If an update or evolution of the system is needed, all the previous steps must be followed again to ensure the security and data protection principles.
- **Decommission:** in case the systems are dismantled, it must be ensured that this process is correctly performed and that personal data is correctly handled always complying with the current legislation and policies.



Figure 2: PRIPARE methodology phases [6]

An additional phase should exist in any organization and should be independent of the engineering process itself.

- **Environment & Infrastructure:** This phase is horizontal, and it is apart from the concrete system or project. In order to use PRIPARE methodology properly, the organization must have an appropriate organizational structure, in addition to a reasonable level of privacy and security awareness.

**Error! Reference source not found.** shows the PRIPARE phases diagram. This is an iterative process that could be performed when needed (e.g. in case of design changes, new requirements). The Organizational aspects are the key, they are in the central part of the picture, since they will support all the engineering processes. It is not linear, i.e., it is possible to go from one phase to another one.

### 2.3.7 Security and privacy team

There are two role types: the roles inherent to the system being engineered and the ones that are related to the application of the PRIPARE methodology. PRIPARE has identified an initial set of roles necessary in the processes that participate in the methodology as described in [6]:

*“System engineers: responsible for enabling the realization of successful systems; they ensure that all aspects of a project or system are considered, and integrated into a whole, during the full system's lifecycle. They can be sub-divided into:*

- *Business & system analyst: its role is to liaise with the end user and to gather an understanding of the system which has to be built.*
- *System designer: based on a requirement specification, he is responsible for developing a comprehensive plan and instructions which can be given to the developers in order to implement a system.*
- *System developer: following the design specifications, the developers build the expected system.*
- *UI designer: system designers which are specifically focused on the specification of the UI aspects.*
- *Tester: each of the roles are responsible for ensuring that their outputs are complete and free from errors, however, there is also a need for testing the system as a whole, ensuring that it meets end-user expectations. Testers are responsible for detecting errors and deviations from the requirement and design specifications.*

**Privacy & security managers & officers (PSMOs):** the senior-level executives within organizations responsible for managing the establishment and maintenance of procedures across the organization that address privacy and security issues and minimize their risks.

- *Privacy & security engineers: part of the privacy and security office, these engineers are IT experts in the design of systems. They are aware of methodological practices of privacy by design and know available PETs and techniques that lead to the development of privacy enhanced systems. Such engineers should have the knowledge and abilities to understand the legal framework in which the system will be deployed and to link this legal framework with the systems' features, privacy controls and existing risks.*
- *Privacy & Security Officer: a person with expert knowledge about data protection law and practices and the ability to fulfil tasks such as monitoring for regulatory compliance, advising the controller and processor about their obligations (regarding the legal framework), acting as the DPA contact point, etc.*

**Data protection authorities (DPAs):** independent bodies which are in charge of:

- *monitoring the processing of personal data within their jurisdiction (country, region or international organization);*
- *providing advice to the competent bodies with regard to legislative and administrative measures related to the processing of personal data;*
- *hearing complaints lodged by citizens with regard to the protection of their data protection rights.*

**Data subjects:** people whose personal data are collected, held or processed.

**Project managers:** the senior-level executives within organizations responsible for making project level decisions regarding scope, costs and schedule. They can be sub-divided depending on the role the organization has in relation to the system:

- *System owners*
- *System operators*
- *System suppliers*

**End users:** people who make use of the engineered system.” [6]

### 2.3.8 Application to INFINITECH pilots

For each pilot, the PRIPARE methodology should be applied, it is recommended to follow sections 5, 6 and 7 of “PRIPARE Methodology Handbook” [6]. This document also provides useful tables and templates that would help to follow the methodology. This is a brief guideline summary of the steps:

- Prepare the processes associated to every phase of PRIPARE methodology. For every process within the phases there should be details of the suppliers, inputs, outputs, consumers, tools, techniques and knowledge involved
- Start with the horizontal phase Environment & Infrastructure, performing these processes:
  - Organizational Privacy Architecture
  - Promote privacy awareness
- Analysis. A preliminary stage would identify roles, scope and responsibility, and after that it is necessary to identify privacy and security requirements. The processes identified are:
  - Functional Description and High-Level Privacy Analysis
  - Legal Assessment
  - Privacy and security plan preparation
  - Detailed privacy analysis
  - Operationalization of privacy requirements. The privacy principles proposed by OASIS PMRM [6] that would be used are:
    1. Consent and choice
    2. Purpose legitimacy and specification

3. Collection limitation
  4. Data minimization
  5. Use retention and disclosure limitation
  6. Accuracy and quality
  7. Openness, transparency and notice
  8. Individual participation and access
  9. Accountability
  10. Information Security
  11. Privacy compliance
    - Risk management
- Design: this phase involves technical decisions that will lead to the specification of privacy enhancing techniques [6]. The processes involved are:
    - Privacy enhancing architecture design
    - Privacy enhancing detailed design
  - Implementation, it will follow the architecture and the detailed privacy-enhancing design
    - Privacy implementation
  - Verification, as privacy by design is a continuous process. It must be verified that the techniques implemented in previous steps are effective. Moreover, compliance controls must be implemented. The processes are:
    - Accountability
    - Security and privacy static and dynamic analysis
  - Release. The processes to address in this phase:
    - Create incident response plan
    - Create system decommissioning plan
    - Final security and privacy review
    - PIA report
  - Maintenance. The processes to carry out when incidents are detected:
    - Execute incident response plan
    - Security and privacy verifications
  - Decommissioning
    - Execute decommissioning plan

## 2.4 PSD II

### 2.4.1 Overview

PSD II (Payments Service Directive 2) is a European Union directive aiming to regulate the industry of online payments across the EU and the EEA. The legislation was introduced in 2018 and its purpose is to create a more integrated and seamless payments experience across all EU member states.

PSD II also introduced Strong Customer Authentication (SCA), a measure set to enhance secure payments and reduce fraud. With the implementation of stronger identity checks, PSD II may add another layer of complexity to the payment journey. However, the directive will introduce several benefits to merchants and customers alike.

It follows on from PSD I (adopted in 2007), and as such, it continues to:

- Pave the way for Fintech companies to enter the payments market and carry out financial transactions. Before this, only banks could provide payment services.
- Require banks and other payment service providers to be transparent about their services and fees, including maximum payment execution times, fees and exchange rates.
- Accelerate the development of the Single Euro Payments Area (SEPA) to facilitate the execution of payments.

The general impact of PSD II is outlined in [7]:

The PSD II regulation drastically impacts the financial eco-system and infrastructure for banks, Fintechs, and businesses using payment data for the benefits of consumers. The revised Payment Services Directive 2 (PSD II) aims to better align payment regulation with the current state of the market and technology. It introduces security requirements for the initiation and processing of electronic payments, as well as for the protection of consumers' financial data. It also recognises and regulates Third-Party Providers (TPPs) that are allowed to access or aggregate accounts and initiate payment services. This move will shake up the payments market, particularly in the eCommerce space, by encouraging greater competition, transparency, and innovation in payment services. In short, PSD II aims at facilitating consumer access to their banking data and driving innovation by encouraging banks to exchange customer data securely with third parties.

Thus, PSD II will break down the bank's monopoly on their user's data. It will allow 'merchants', businesses like Amazon, to retrieve your account data from your bank - with consent.

For consumers who hold more than one bank account, the changes would also allow businesses, known in the legislation as Account Information Service Providers, to display all their account information in one place for them.

### 2.4.2 Technology Impact

The directive requires that security should be integrated and not deployed in isolation to ensure that payment services are "safe and secure". The ability to protect major components of the PSD2 payment ecosystem in a connected way ensures that organizations fully meet the requirements of the PSD2 allowing them to significantly reduce their threat exposure. The ability to blend external threat intelligence, risk-based authentication, behavioural analytics, and eCommerce fraud detection with both payment transaction monitoring and transaction signing will allow payment service providers to concentrate on the business of providing innovative and convenient payment solutions.

PSD II focuses on consumer protection, developing a framework that "nurtures competition, innovation and security" across the EU. The directive creates a legally binding requirement for organizations operating in the EU payments industry to deploy Strong Customer Authentication (SCA). SCA is based on the use of two or more elements:

1. Knowledge – something only the user knows, e.g. a password or a PIN
2. Possession - something only the user possesses, e.g. a card or an authentication code (One-Time-Password or OTP) generating device
3. Inherence – something the user is, e.g. biometric authenticator such as fingerprint, eyeprint or voice recognition

PSD2 also fosters payment innovation and opens up the payment infrastructure to third party providers (TTPs) through 'access to account' (XS2A) APIs. Authentication mechanisms that are convenient and work across all payment channels will differentiate these TTPs in what will be a very competitive environment.

The European Banking Authority reports a guideline on **PSD II security measures** [8].

Following [9] the core principles of the PSD2 Regulatory Technical Standards – i.e. **Strong Customer Authentication (SCA)**, **Secured Communication**, **Risk Management**, and **Transaction Risk Analysis (TRA)** – have been maintained, confirming the directive's security objectives.



To protect the consumer, PSD2 requires banks to implement **multi-factor authentication** for all proximity and remote transactions performed on any channel.

This obligation means using **two of these three features**:

- **Knowledge**: Something only the user knows, e.g. password, code, personal identification number
- **Possession**: Something, only the user, possesses, e.g. token, smart card, mobile handset
- **Inherence**: Something, the user, is, e.g. biometric characteristics, such as a fingerprint.

Besides, the elements selected must be mutually independent, which means that the breach of one should not compromise any of the others. [9]

PSD2 provides that payment service providers (PSPs) shall establish a framework with appropriate mitigation measures and control mechanisms to manage operational and security risks relating to the payment services they provide. Security Requirements do utilise existing adopted standards by the sector like ISO 27001

- Identify, establish and regularly update an inventory of their business functions, key roles and supporting processes in order to map the importance of each function, role and supporting processes, and their interdependencies related to operational and security risks.
- identify, establish and regularly update an inventory of the information assets, such as ICT systems, their configurations, other infrastructures and also the interconnections with other internal and external systems in order to be\* able to manage the assets that support their critical business functions and processes.
- ensure that they continuously monitor threats and vulnerabilities and regularly review the risk scenarios impacting their business functions, critical processes and information assets.
- PSPs should ensure that they continuously monitor threats and vulnerabilities and regularly review the risk scenarios impacting their business functions, critical processes and information assets. As part of the obligation to conduct and provide CAs with an updated and comprehensive risk assessment of the operational and security risks relating to the payment services they provide and on the adequacy of the mitigating measures and control mechanisms implemented in response to those risks.
- On the basis of the risk assessments, PSPs should determine whether and to what extent changes are necessary to the existing security measures, the technologies used and the procedures or payment services offered.
- PSPs should ensure the confidentiality, integrity and availability of their critical logical and physical assets, resources and sensitive payment data of their PSUs whether at rest, in transit or in use. If the data include personal data, such measures should be implemented in compliance with GDPR.

#### **Data and systems integrity and confidentiality**

- In designing, developing and providing payment services, PSPs should ensure that the collection, routing, processing, storing and/or archiving and visualisation of sensitive payment data of the PSU is adequate, relevant and limited to what is necessary for the provision of its payment services.
- PSPs should regularly check that the software used for the provision of payment services, including the users' payment-related software, is up to date and that critical security patches are deployed. PSPs should ensure that integrity-checking mechanisms are in place in to verify the integrity of software, firmware and information on their payment services.

#### **Access Control**

- PSPs should institute strong controls over privileged system access by strictly limiting and closely supervising staff with elevated system access entitlements. Controls such as roles-based access, logging and reviewing of the systems activities of privileged users, strong authentication and

monitoring for anomalies should be implemented. PSPs should manage access rights to information assets and their supporting systems on a ‘need-to-know’ basis. Access rights should be periodically reviewed.

- Access logs should be retained for a period commensurate with the criticality of the identified business functions, supporting processes and information assets

**Detection**

- PSPs should establish and implement processes and capabilities to continuously monitor business functions, supporting processes and information assets in order to detect anomalous activities in the provision of payment services. As part of this continuous monitoring, PSPs should have in place appropriate and effective capabilities for detecting physical or logical intrusion as well as breaches of confidentiality, integrity and availability of the information assets used in the provision of payment services

The main key technology requirements that emerge for Infnitech Pilots are listed in Table 1 below:

Table 5: List of relevant requirements resulting from PSD II

<b>GRS-0001 Strong Multi-Factor authentication (MFA)</b>
A requirement for the user to provide two or more verification factors to gain access to a resource such as an application, online account, or a VPN. MFA is a core component of a strong identity and access management (IAM) policy. Rather than just asking for a username and password, MFA requires one or more additional verification factors, which decreases the likelihood of a successful cyber attack.
<b>GRS-0002 SIEM (Security Information Event Management) systems (equals GMS-0001 above)</b>
Used to collect and aggregate log data generated throughout the organization’s technology infrastructure, from host systems and applications to network and security devices such as firewalls and antivirus filters. Identify and categorize incidents and events, as well as analyse them. It serves to achieve two main objectives, which are to <ul style="list-style-type: none"> <li>• provide reports on security-related incidents and events, such as successful and failed logins, malware activity and other possible malicious activities and</li> <li>• send alerts if analysis shows that an activity runs against predetermined rulesets and thus indicates a potential security issue.</li> </ul>
<b>GRS-0003 Patch Management</b>
Distributing and applying updates to software. It will support the following objectives: <ul style="list-style-type: none"> <li>• Security: Patch management fixes vulnerabilities on your software and applications that are susceptible to cyber-attacks, helping your organization reduce its security risk.</li> <li>• System uptime: Patch management ensures your software and applications are kept up-to-date and run smoothly, supporting system uptime.</li> <li>• Compliance: With the continued rise in cyber-attacks, organizations are often required by regulatory bodies to maintain a certain level of compliance. Patch management is a necessary piece of adhering to compliance standards.</li> <li>• Feature improvements: Patch management can go beyond software bug fixes to also include feature/functionality updates. Patches can be critical to ensuring that you have the latest and greatest that a product has to offer.</li> </ul>

## 2.5 MIFID II

### 2.5.1 Overview

A brief overview on MIFID II can be found at [10]:

MIFID II is a legislative framework instituted by the European Union (EU) to regulate financial markets in the bloc and improve protections for investors. Its aim is to standardize practices across the EU and restore confidence in the industry. MIFID II harmonizes the application of oversight among member nations and broadens the scope of the regulations. In particular, it imposes more reporting requirements and tests in order to increase transparency and reduce the use of dark pools (private financial exchanges that allow investors to trade without revealing their identities) and over-the-counter (OTC) trading. Under the new rules, the trading volume of a stock in a dark pool is limited to 8% over 12 months. The new regulations also target high-frequency trading. Algorithms used for automated trading have to be registered, tested and have circuit breakers included.

MIFID II places restrictions on inducements paid to investment firms or financial advisors by any third party in relation to services provided to clients. Banks and brokerages will no longer be able to charge for research and transactions in a single bundle, forcing a clearer sense of the cost of each, and possibly improving the quality of research available to investors. Brokers will have to provide more detailed reporting on their trades—50 more pieces of data, in fact— including price and volume information. They will have to store all communications, including phone conversations; electronic trading is encouraged since it is easier to record and track.

## 2.5.2 Technology Impact

[11] lists as major technology impact of MIFID II:

- **Data storage, aggregation, and analytical requirements:** Under MIFID II rules, all of the records that can impact or lead to a trade must be retained for posterity. This includes records pertaining to phone calls and emails. Managing this volume, variety, and velocity of data (i.e., big data and extracting numerous mandatory reports) will be a herculean task. A complete data retention and archiving strategy also needs to be designed. This might require a huge amount of storage not only at your primary data centre, but also at your disaster recovery site, which can be taxing in terms of costs and implementation.
- **Integration between disparate applications:** MIFID II will force integration of various applications with trade platforms to provide some of the key inputs. For example, your insurance portal might need to communicate with the trade system to feed the national insurance number in order to complete the transaction. There are multiple ways to carry out integrations like these, but application programming interface-based (API-based) integration is most efficient and robust in most cases.
- **Enhanced and transparent client portal:** To adhere to investor protections, organizations need to build proper client classification and client data inventories. This will be very useful for client-facing and for sales representatives to offer the appropriate products and services to the right customers. Institutions can also look forward to providing clients with real-time access to account information through these portals. Technology will once again play a key role in the development and enhancement of required portals and dashboards.
- **Mobile Device Management (MDM) strategy:** As mentioned above, the new set of rules mandates that you record and store all trade-related phone calls. As per the directive of the European parliament, “for those purposes, an investment firm shall take all reasonable steps to record relevant telephone conversations and electronic communications, made with, sent from or received by equipment provided by the investment firm to an employee or contractor or the use of which by an employee or contractor has been accepted or permitted by the investment firm.” So, what if the communication is happening over social media like Facebook or WhatsApp? It is impossible to record these discussions as they are encrypted. The solution is to roll out an MDM product, which restricts individuals from installing these sets of applications, thus compelling them to use modes of communication that will allow for compliance.

### Specific MIFID II security requirements

We must also consider the IT security requirements that come along with MIFID II. In addition to the collection and retention of enormous amounts of data, maintaining the security and integrity of that data is a major challenge.

Data security requires an access management system, which ensures that only a certain group of individuals has the specific set of privileges to access data. Multi-factor authentication should also be considered to protect your valuable data. Data integrity involves maintaining the consistency and accuracy of data until its life cycle is complete.

Data will obviously be modified over time, but a proper monitoring and auditing system should be implemented to record the identities of individuals, the data and time of entries, modifications, and deletions. Having a robust backup and recovery solution in case an unexpected event occurs is key to restoring normalcy to the organization. This should also be followed up by frequent, internal audits to make sure that all controls and processes are being followed.

The main requirements resulting from MIFID II within the context of Infinitech for pilots where MIFID II applies are listed in Table 6:

Table 6: Relevant Requirements resulting from MIFID II

<b>GRS-0002 SIEM (Security Information Event Management) systems (equals GMS-0001 above)</b>
Auditing logs for maintaining and monitoring the security and integrity of data
<b>GRS-0005 Phone Call Recording</b>
Phone call recording to maintain a record of all interactions with customers providing an evidence trail of all advice and information provided
<b>GRS-0006 Email Logging</b>
Email logs to maintain a record of all interactions with customers providing an evidence trail of all advice and information provided
<b>GRS-0001 Strong Multi-Factor authentication (MFA)</b>
Strong authentication, preferably multi-factor, and authorization mechanisms

## 2.6 AMLD4

### 2.6.1 Overview

A concise overview on AMLD4 can be found as [12]:

AMLD4 has been drafted to ensure that companies are more accountable for any connection to money laundering or terrorist financing. Non-compliance can lead to sanctions and reputational damage. Although the Directive was prepared with banks and financial institutions in mind, corporations also need to be aware of the Directive and have appropriate controls in place.

#### Key Provisions

- Wider Net - More entity types are subject to AMLD4 than its predecessor AMLD3. The following are now covered: gambling institutions, real estate letting companies, individuals or companies making single transactions over €10,000, virtual exchange currency platforms as well as foreign and domestic Politically Exposed Persons (PEPs).
- More Emphasis on Risk - Companies need to be aware of more risk factors when assessing their business dealings. Here are ten key risks:
  - a. PEPs as owners or People of Significant Control (PSC). Companies are obliged to carry out such assessments when engaging in business dealings
  - b. Industries with excessive cash, which are at the heart of the legislation. Such industries are known to be key targets of money launderers.

- c. Connection or dealing with high-risk sectors. This covers sectors like construction, pharmaceuticals, arms, extractive industries and public procurement.
  - d. Media reports. You should be especially aware of credible media sources which allege “criminality of terrorism”.
  - e. History of frozen assets. Even reasonable grounds to suspect an asset freeze should be investigated.
  - f. Complex or non-transparent ownership structures. Ownership and control structures should make sense and if they don’t should be investigated.
  - g. Ownership in the form of a non-legal person. Proposed business partners should be a “legal person”.
  - h. Beneficial owner identity. If there is any doubt about the identity of a prospective partner this needs to be assessed.
  - i. Unknown sources of wealth. Income for prospective partners should be clearly traceable.
  - j. Associations with countries subject to sanctions. Dealings with companies who have ties with sanctioned countries directly or indirectly should be investigated.
- Increased Checks on Dealing with Third Countries - The Financial Action Task Force (FATF) releases a list three times a year which details the qualifying countries, i.e. those operating in high-risk countries. Any companies operating in the countries on this list should be subject to a thorough list of checks before business commences.
  - Tougher Sanctions - Countries are being encouraged to name and shame organisations who flout regulations. This sits alongside more stringent financial sanctions.
  - Transparency with Beneficial Ownership has an Enhanced Focus - AMLD4 requires the identification and monitoring of people with beneficial ownership in companies. A beneficial owner can be defined by their share in the business but can also qualify as a beneficial owner if they are a person of significant control (PSC) regardless of their ownership stake. AMLD4 requires:
    - A national register to be updated and interconnection of national registers; Greater access, so anyone with a legitimate interest can see this information; and Expanded definition of beneficial ownership to 10% for high-risk companies.

This means that compliance professionals will need to be able to determine the risk of a company they are working with before assessing their beneficial owners. National registers not being up to date is no excuse for non-compliance.

In conclusion, companies are now more accountable for the entities they work with. Any connections to money laundering or terrorist financing – intentional or incidental – can lead to sanctions and at least reputational damage as in accordance with AMLD4 supervisory authorities have to publically disclose any measures and sanctions imposed to the obliged entity.

## 2.6.2 Technology Impact

The main impacts of AMLD4 within this context are the following requirements (Table 7)

Table 7: Relevant Requirements resulting from AMLD4

<b>GRS-0007 Examination &amp; Investigation</b>
AML compliance, AML/Suspicious transaction monitoring, trade surveillance, operational risk and anti-fraud case management
<b>GRS-0008 Customer Due Diligence</b>
Single data entry point and risk rating for all existing and new customer and account data in support of Know Your Customer (KYC) requirements incorporating third party data sources and registers
<b>GRS-0009 Name/Entity Matching</b>
Matching and scoring tools and techniques that improve the searching of account and transaction information across systems, regions and business lines to create one view of the customer or to improve the name/entity screening

## 3 Impact on INFINITECH Pilots

In this section the impact of the previous section's findings on standards and regulations is mapped to the pilots.

### 3.1 Update on Pilots - Regulatory Impact

In this section the regulatory impact on the pilots is updated considering the latest developments and the findings of section 2.

#### 3.1.1 GDPR

The relevance of GDPR in the pilots has been thoroughly analysed in the previous version of this deliverable. Only a few adaptations are observed and listed in Table 8 below.

#### 3.1.2 PSD II

##### 3.1.2.1 Pilots with no evidence that PSDII applies

Pilots #1 - #4, #6, #8-14 do not intend to deal with payment services or transactions.

Considering the updated pilot description in D2.4 PSD II does not apply to pilot #3

Pilot #5 (formerly Pilot #5b) does not deal directly with payment services. No action is triggered within the INFINITECH Reference Architecture (IRA), rather recommendations are being generated and sent from the IRA to the Users mobile/web environment. The latter environments are already operated by the bank, are subject the banking regulation rules and Users action(s) are applied within these environments.

The use case of Pilot #15 is focused on building a model able to read the internal documents of a bank (for example internal policies, internal circulars, operating guides, user manuals, etc.), to highlight the main concepts and compare them with reference taxonomies to build a common business glossary. A number of banks will provide the data set. Thus, the regulation does not apply to this pilot.

##### 3.1.2.2 Pilots with evidence of PSDII applicability and further need to inquire

None

##### 3.1.2.3 Pilots with clear evidence of PSDII applicability

Pilot #7 deals with payment data. However, no payment services are triggered within the INFINITECH pilot environment during piloting. When the pilot solution shall be applied in a real payment environment the operating banking regulation rules and user actions are applied in the bank's environment.

#### 3.1.3 MIFID II

##### 3.1.3.1 Pilots with no evidence that MIFIDII applies

Pilots #1, #3, #8 - #14 do not intend to pursue any activities related to financial instruments and/or maintain to be covered by the required license.

The use case of Pilot #15 is focused on building a model able to read the internal documents of a bank (for example internal policies, internal circulars, operating guides, user manuals, etc.), to highlight the main concepts and compare them with reference taxonomies to build a common business glossary. A number of banks will provide the data set. Thus, the regulation does not apply to this pilot.

### 3.1.3.2 Pilots with evidence of MIFID II applicability and further need to inquire

None

### 3.1.3.3 Pilots with clear evidence of MIFIDII applicability

Pilot #2 deals with financial analysis and maintains that it has conflict of interest declaration for each employee in place. Since there are more compliance requirements for distributors of investment research it is assumed that MIFID II applies to Pilot #2.

Pilot #4's scope indicates, however, a certain proximity to investment advice. Thus, it is assumed that MIFID II applies to the pilot.

Pilot #6 clearly is within the MIFIDII scope but appears to be covered by a financial services license. It refers to its legal and compliance department, so that we assume that regulatory issues are covered in-house.

## 3.1.4 AMLD4

The impact of AMLD4 is strongly related to the KYC processes. Thus, we focus on KYC related implications in this section

### 3.1.4.1 Pilots with no KYC implications

Pilots #1 - #3, as well as #10-14 do not intend to pursue any activities related to KYC.

In Pilot #6, the funds that the customer intends to invest already exist in the related bank account and the relative AML functionality is already applied to the customer. Thus, the pilot #6 is not related to KYC.

The use case of Pilot #15 is focused on building a model able to read the internal documents of a bank (for example internal policies, internal circulars, operating guides, user manuals, etc.), to highlight the main concepts and compare them with reference taxonomies to build a common business glossary. A number of banks will provide the data set. Thus, the regulation does not apply to this pilot.

### 3.1.4.2 Pilots with KYC implications and further need to inquire

None

### 3.1.4.3 Pilots with clear evidence of KYC implications

With the updated description in D2.4 pilot #3 is related to KYC processes.

Pilot #9 is within the KYC perimeter by design. Although it does not appear to be an "obliged entity" in its own right and thus does not carry any specific obligations familiarity with KYC should be essential. For the purpose of this paper, we assume that the required knowledge exists within the pilot's team.

## 3.2 Update on Pilots' Technical Measures

In general, all testbeds shall follow the best practices regarding ISO27001 as outlined in section 2.2.1, which are today's generally accepted State of the Art in Security measures. Considering privacy also the measures defined in Table 2 related to ISO 27701 apply for pilots using personal data. The technical measures related to PCI DSS do not apply to any pilot, but most of them are included in the ISO 27001. Finally, the additional technical measures GMS-0019 (Supplier Management) and GMS-0020 (Risk Management) defined by the NIST and described in section 15 should be considered on project level related to the provisioning of infrastructure.

In accordance with regulatory aspects, pilots shall follow additional technical security measures outlined in the sections 0, 2.4, 2.5, and 2.6 in their testbeds and related sandboxes. The affected pilots are listed in Table 8 below summarizing the findings of those sections.

Table 8: Applicability of Regulations in Pilots

Pilot #	GDPR / Personal Data	PSD II	MIFID II	AMLD4
1	No	No	No	No
2	No	No	Yes	No
3	No	No	No	Yes
4	No	No	Yes	No
5	Confidential – see also section 1			
6	No	No	Yes	No
7	Confidential – see also section 1			
8	Restricted to the consortium – see also section 1			
9	No	No	No	Yes
10	No	No	No	No
11	YES - no changes since previous deliverable	No	No	No
12	YES – data will be anonymized	No	No	No
13	No	No	No	No
14	YES - no changes since previous deliverable	No	No	No
15	No	No	No	No

### 3.3 Organizational Measures for Security and Compliance

The measures listed in this section are based on controls from standards and regulations like ISO 27001 and GDPR. They can be viewed as basic measures an organization might take to provide some level of protection to information and personal data that the organization and their systems/applications may hold and/or process. Some organizational security measures apply to the regulations.

Thus, these measures shall be considered deploying a testbed. Therefore, the most relevant requirements resulting from those measures result one or more requirements related to the INFINITECH project and especially for its pilot deployment (WP6) and pilot operations (WP7).

Table 9 below shows the key requirements at the core of maintaining good security practices within the organisation. Whilst they are all critical within the context of the Infinittech pilots the most important ones would be Risk Assessment, Business Continuity and Strong Passwords.

Table 9: Organizational Measures and Requirements

<b>GMS-1001 Information Security Policies</b>
Maintain an information security policy and develop appropriate procedures to support and implement that policy. The content can be dependent on the activities being undertaken and the specific data processing being undertaken. This should also cover specific areas such as remote access, asset management and password controls.
<b>GMS-1002 Business Continuity</b>
Protocols and measures should be in place to back-up personal data and ensure that it can be recovered and maintained in the event of an incident.
<b>GMS-1003 Risk Assessment</b>
Comprehensive assessments should be carried out for high-risk data and processing activities and mitigating solutions/procedures should be in place to prevent or reduce risks.
<b>GMS-1004 Policies and Procedures</b>
Implement robust policies and procedures so that the whole organisation and its employees know what their obligations are and what to do if certain situations occur. They should be easy to follow to provide intent, objectives and guidelines for adhering to regulations.
<b>GMS-1005 Management Information &amp; Reporting (does not apply explicitly to the pilots)</b>



Regular reports and information are passed to upper management is essential for ensuring that the adequate resources and funding are made available and for accountability at all levels
<b>GMS-0005 Security Awareness &amp; Training</b>
A culture of security and data protection awareness will ensure that employees, contractors and any third-party working for or with the organisation, know what is expected of them and how to maintain compliance. Regular and ongoing training sessions will ensure that the latest information, guidance, legislations and regulations are known and understood
<b>GMS-1006 Reviews &amp; Audits (does not apply explicitly to the pilots)</b>
This ensures that policies, controls and/or measures that are put in place can be monitored for effectiveness, accurate and fit for purpose.
<b>GMS-1007 Due Diligence (does not apply explicitly to the pilots)</b>
Carrying out due diligence checks on suppliers and service providers (and in some sectors, customers); is an essential and often legal requirement (i.e. fraud checks, anti-money laundering measures)
<b>GMS-1008 Building Security</b>
You should have robust measures and protocols for securing access to any office or building and ensure that all employees are aware of such controls.
<b>GMS-1009 Disposal</b>
Specify the appropriate procedures compliant with GDPR for the disposal of paperwork and devices and appropriate controls for anything that is registered as lost. This should be covered by a general INFINITECH policy to be provided by Coordinator or by the Project Security Officer.
<b>GMS-0004 Password Policy Enforcement</b>
Specify a password policy that enforces strong passwords that are changed on a regular basis. This includes employees being aware that they must not be sharing passwords or leave systems unlocked when unattended. The related policy needs to be defined according to the organizations participating in the pilots and controlled by pilot leaders.
<b>GMS-1010 Supplier Relationships</b>
Implement procedures to manage third-party risks coming into your organization and systems resulting from a failure to follow good security practice by suppliers, e.g. AWS.

### 3.4 Pilot Recommendations

With these findings on applicability of standards and regulations and the related technical and organizational measures recommendations, which shall be considered by the pilots’ testbeds and sandboxes are listed in the following Table 10. Nonetheless, the pilots should take into account the measures, which are provided already in their specific operational environment and which may cover most of the requirements already.

Table 10: Technical and Operational Measures per pilot

Pilot	Recommended Technical Measures	Recommended Organizational Measures
<i>Pilot #1 Invoices Processing Platform for a more Sustainable Banking Industry</i>	GMS-0001 to GMS-0012	GMS-1001 to GMS-1010
<i>Pilot #2 Real-time risk assessment in Investment Banking</i>	GMS-0001 to GMS-0012 GRS-0001, GRS-0002, GRS-0005, GRS-0006	GMS-1001 to GMS-1010
<i>Pilot #3</i>	GMS-0001 to GMS-0012 GRS-0007, GRS-0008, GRS-0009	GMS-1001 to GMS-1010
<i>Pilot #4 Personalised Portfolio Management</i>	GMS-0001 to GMS-0012 GRS-0001, GRS-0002, GRS-0005, GRS-0006	GMS-1001 to GMS-1010

Confidential – see also section 1		
<i>Pilot #6 Personalized Investment Management Closed-Loop Portfolio for Retail Customers</i>	GMS-0001 to GMS-0012 GRS-0001, GRS-0002, GRS-0005, GRS-0006	GMS-1001 to GMS-1010
Confidential – see also section 1		
Restricted to consortium – see also section 1		
<i>Pilot #9 Analysing Blockchain Transaction Graphs for Fraudulent Activities</i>	GMS-0001 to GMS-0012 GRS-0007, GRS-0008, GRS-0009	GMS-1001 to GMS-1010
<i>Pilot #10 Real-time cybersecurity analytics on financial transactions' data</i>	GMS-0001 to GMS-0012	GMS-1001 to GMS-1010
<i>Pilot #11. Personalized insurance products based on IoT connected vehicles</i>	GMS-0001 to GMS-0012	GMS-1001 to GMS-1010
<i>Pilot #12 Real world data for novel health insurance products</i>	GMS-0001 to GMS-0012	GMS-1001 to GMS-1010
<i>Pilot #13 Alternative and automated insurance risk selection and insurance product recommendation for SME's</i>	GMS-0001 to GMS-0012	GMS-1001 to GMS-1010
<i>Pilot #14 Big Data and IoT for the Agricultural Insurance Industry</i>	GMS-0001 to GMS-0012	GMS-1001 to GMS-1010
<i>Pilot #15</i>	GMS-0001 to GMS-0012	GMS-1001 to GMS-1010

## 4 Focus Point AI

Globally, policymakers are seeking to tackle risks associated with the development of AI. In particular, in April 2019, the EU published its guidelines on ethics in AI. In 2020 we are witnessing several initiatives to establish AI policy framework from policy makers like UN, OECD, EBA and many more.

In previous version of the deliverable, we summarized content from 3 major document areas released in 2020 regarding AI governance:

- EU
- UN and OECD
- EBA.

We specifically, focused on the practical definition of the approach to applying AI governance guidelines. Since the documents were released in 2020, at the end of 2020 there is no significant update, though there were such announcements at the beginning of 2020. Considering COVID-19 EU policymakers are reconsidering their plans and pushing them to 2021.

In February 2020, the EC stopped short of introducing legislation, instead delivering a new digital strategy. The plan proposed to conduct extensive bias testing on machine learning technologies that had been imported from outside of the EU's jurisdiction and that would be used to make life-changing decisions. It also ensures the creation of common data spaces for stake-holders businesses to share industrial data that could be exploited by researchers and engineers.

In 2020 EBA continuously drove awareness activities to spread understanding of potential benefits and risks of AI in financial domain. For instance, EBA Open Banking Working Group (OBWG) latest research currently focuses on the potential of AI in the financial services sector and the challenges and opportunities it holds when combined with data exchange enabled by Open Banking. Their latest report "Artificial Intelligence in the era of Open Banking" focuses on the potential benefits that lie in the collaboration between Financial Institutions (FIs) addressing AI challenges together and thereby creating opportunities that may help building a more efficient and resilient financial system.

Since the AI governance policy framework is still in its development phase, currently there is no legally binding documents with specific guidelines for AI governance, but several countries all over the globe have already started to address this topic. Comparison of how different countries address AI regulation can be found in the report "Regulation of Artificial Intelligence in Selected Jurisdictions" issued by The Law Library of Congress on January 2019 [13]. This report examines the emerging regulatory and policy landscape surrounding AI in jurisdictions around the world and in the European Union (EU). In addition, a survey of international organizations describes the approach that United Nations (UN) agencies and regional organizations have taken towards AI. As the regulation of AI is still in development, guidelines, ethics codes, and actions by and statements from governments and their agencies on AI are also addressed. Report covers EU approach along with individual report on national strategy of individual countries. It covers state of legal framework, related to AI.

A further approach to developing the AI regulation policy is applied in Singapore [14]. In Singapore, the Personal Data Protection Commission (PDPC), applied a collaborative bottom up approach, where they introduced a Model AI Governance framework, first version in January 2019. They provide initial version of general AI framework, which is continuously updated by providing more details regarding guidelines by various stakeholders. The second version was released in January 2020 [15]. As AI technologies evolve, so would the related ethical and governance issues. It is the PDPC's aim to update the Model Framework periodically with the feedback received, to ensure that it remains relevant and useful to organisations deploying AI solutions.

### From Principles to Practice



Figure 3: AI Model framework [14]

Unlike other documents (EC, OECD, UN EBA), The Model Framework provides practical implementable guidelines to the private sector organisations to address the key ethical and AI governance related issues when developing and deploying AI solutions. It includes two documents with several well documented use-cases which promotes good practices and lessons learned. By explaining how AI solutions work, building good data accountability practices, and creating open and transparent communication for various types of stakeholders, the Model Framework aims to promote public understanding and trust in technologies. The main guiding principles are:

- Decisions made by AI should be explainable, transparent and fair
- AI systems should be human centric

The two main principles are further divided into 4 areas: internal governance, level of human involvement, operations management and stakeholders’ interactions and communications (shown in Figure 3).

The second addition of Model AI Governance Framework comes along with Self-Assessment Guide for Organizations (ISAGO). ISAGO is the result of the collaboration with World Economic Forum's Centre for the Fourth Industrial Revolution to drive further AI and data innovation. ISAGO was developed in close consultation with the industry, with contributions from over 60 organisations [14].

The second addition is described in [14] and [15]: It added additional points-of-interest like robustness and reproducibility and introduced additional considerations on interactions and communications with wider range of stakeholders. The second edition of the Model Framework continues to take a sector-and technology-agnostic approach that can complement sector-specific requirements and guidelines.

It provides guidelines for organisations to assess the alignment of their AI governance practices with the Model Framework. It also provides an extensive list of useful industry examples and practices to help organisations implement the Model Framework. Use cases covers different business areas (banking, health, pharma) and show how organisations have effectively put in place accountable AI governance practices and benefit from the use of AI in their line of business. By implementing responsible AI governance practices, organisations can distinguish themselves from others and show that they care about building trust with consumers and other stakeholders.

### List of general recommendations

Organization which adopts and deploys AI solutions has a responsibility to assure appropriate AI governance. Since at this point, AI legislation is still in development and formal guidelines are written in a general manner, we can contribute to the process by making AI guidelines more concrete and practice by the example. We would like to encourage organizations to impose currently available guidelines for AI regulation in order to ensure and promote responsible and trustworthy use of AI.

At this point we would like to focus on the following principles:

#### “Explainability” and Interpretability:

- Enable explanation of an output of AI model:  
  
**Purpose:** provide humanly readable explanation, why the AI system (or AI model) provide one particular decision (prediction). Explanation or interpretation should be provided in a manner, which will be suitable for end user and/or consumer.  
  
One could use either different techniques from the area of Explainable AI or to provide explanation by using ML methods which enable such explanations (LN, DT, etc.)
- Report, describing AI models in terms of providing output explanations (developers describing process, how the particular explanation or interpretation is done)

#### Fairness and avoidance of bias:

- **Purpose:** provide analysis of relevant data sets that are used for development of AI models and analysis of possible biases in data
- Exploratory analysis of input data
  - Report on preliminary analysis of input data (for each input data feature report provides preliminary analysis including but not limited to distributions, min, max, missing values)
  - data quality analysis (count or percentage of missing values, distinct values (zero or negative values), frequency analysis – depends of the context)
  - Data understanding - data rules (how various input data features relates to others, what types of filters must or should be used))
- Report on evaluation:
  - How data is divided into training, maybe also validation, and test data set
  - Analysis of AI results (AI outputs correlated with input data features)

#### Traceability and auditability – accountability:

- Document to provide a report including:
  - Data process flows including DQ control
  - Data dictionaries
  - AI system architecture
- Document to provide a report on
  - Development of AI models (final report on all filters, data manipulation and ML method, list of input and final data features)
  - Evaluation of AI models (evaluation parameters and error-rate criteria)
- Document of continued evaluation (how the AI model is continuously evaluated in order to be still relevant)

#### Data protection; data quality; security:

- Document to provide the end-to end information lifecycle:
  - controls addressing access,
  - confidentiality,

- integrity, retention and movement of data
- status of data availability (regulatory and legal framework: GDPR, PSD2)
- Document to provide a report on applied data protection policies:
  - Report on applied data anonymization and pseudo anonymization or other applied data protection methods

For fair, trustworthy usage of AI is crucial that end-users understand what types of AI outputs are they using in particular phases their business processes and what are the limitations and prerequisites for using AI system.

## 4.1 Recommendations to the INFINITECH Pilots

The descriptions outlined above, provide a soft framework for the pilots to comply with. This framework will further be enhanced provided there is input from the European Council's relevant focus group.

EBA pointed out in their Report on BigData and Advances Analytics, that financial institutions (FI) which deploy AI solutions are accountable for their results, even though those AI models were developed by the 3th party. Therefore, it is crucial that FI have a comprehensive view of deployed AI solution, at different stage, but in particular their placement in appropriate business processes. The end-users, who are using AI results in their every-day work, should be aware of initial assumptions and constraints of AI models. Furthermore, measures for mitigating various risks of possible inaccuracies of AI models must be set.

To help FI to implement trustworthy and auditable AI solutions there are 3 reports which are helping running AI governance in transparent and accountable way:

- **Report 1:** Report on how the results of AI solution (scores, predictions, recommendations) are incorporated business-processes along with a clear picture that shows where human comes in the loop and what is the nature of an AI output in final decision. Report should include a description of what happens in situations that output AI model is possibly wrong:
  - What type of an AI output error can occur and how does it affect the customers and business-processes - usually not all the inaccuracies have the same consequence in terms of severity- Usually the severity of the error depends on how the AI outputs are embedded in business process.
  - What are organizational measures to mitigate the risk of inaccurate AI output
- **Report 2:** Report on AI model, which describes the development and deployment:
  - Initial assumptions and pre-requisites regarding existing data rules or processes
  - Report on AI model development:
    - definition of a problem, Data preparation,
    - Modelling - algorithms and parameters used
    - Validation and evaluation (accuracy measurements, type of validation)
    - Responsible personnel (development and business approval)
  - Report on deployment:
    - Where and how the model is used
    - What are pre-requisites
    - Continuous quality measures
    - Responsible personnel
- **Report 3:** Data Source report, which should shed some light on fairness and possible bias with the goal of making end-users aware of possible biases:
  - Data dictionary for each data source
  - Statistical analysis of input data sources
  - Legal and Regulatory restrictions (anonymization , pseudo-anonymization)
  - Analysis of possible biases and wherever all relevant data is available:

- What are the measures for risk mitigation (if possible bias exists)

Table 11 below is a first draft version of recommended steps for Infinitech pilots that should be fulfilled in applying responsible and trustworthy AI solutions. The next step is to provide actual report templates for each of proposed Reports.

Table 11: Recommendations on AI per Pilot

Pilot	Aim of AI solution	Recommended Analysis	Recommended Reports
<i>Pilot #1 Invoices Processing Platform for a more Sustainable Banking Industry</i>	The innovation of the pilot lies in the applicability of Artificial Intelligence technologies over scanned physical documents. AI will be used to extract relevant indicators from digitized invoices, further used to automatically and accurately rate notaries based on a sustainability index.	<ul style="list-style-type: none"> <li>○ Focus on data flow and accuracy in text detection (accuracy of detected indicators) and consequences of possible inaccuracies and how to handle them (risk mitigation).</li> <li>○ Where comes human in the loop? How the AI results are incorporated into business processes?</li> </ul>	Report 1, 2, 3
<i>Pilot #2 Real-time risk assessment in Investment Banking</i>	Aim is to give traders in investment banking a precise and timely indication of the risk of a given portfolio and specifically changes in risk due to market changes or changes of the portfolio. Goal is to provide a tool for support institutional traders, asset managers, risk managers and wealth management experts.	<ul style="list-style-type: none"> <li>○ Where comes human in the loop? How the AI results are incorporated into business processes?</li> <li>○ End-users should be aware of assumptions and limitations of AI models. Should also be informed if the results is based on lack of data or any other particular circumstance.</li> </ul>	Report 1, 2, 3
<i>Pilot #4 Personalised Portfolio Management</i>	The main goal is to develop and adapt an optimization algorithm and an AI engine to aid investment propositions for retail clients. The AI genetic algorithm will generate a new proposal, where the selected preferences and risk parameters have been recognised.	<ul style="list-style-type: none"> <li>○ Focus on input data analysis in terms of weather the input data is representative enough, or there should be some assumptions regarding possible biases End user should be aware of optimization criteria in order to use in a proper way.</li> <li>○ Focus also on interactions and dependencies between different AI models and associated risks.</li> </ul>	Report 1, 2, 3
Confidential – see also section 1			
<i>Pilot #6 Personalized Closed-Loop</i>	Aim is to provide personalized investment recommendations for the	<ul style="list-style-type: none"> <li>○ Provide information about possible data bias (are data representative enough)</li> </ul>	Report 1, 2, 3

<p><i>Investment Portfolio Management for Retail Customers</i></p>	<p>retail customers of the bank.</p>	<ul style="list-style-type: none"> <li>○ Focus also on interactions and dependencies between different AI models and associated risks.</li> <li>○ Explain possible different consequences of inaccurate AI output and associated measures for risk mitigation. Final decision is made by human or AI?</li> <li>○ Who is responsible for AI outputs</li> </ul>	
<p>Confidential – see also section 1</p>			
<p>Restricted to the consortium – see also section 1</p>			
<p><i>Pilot #9 Analysing Blockchain Transaction Graphs for Fraudulent Activities</i></p>	<p>Goal is to detect fraudulent activities monitoring blockchain transactions.</p>	<ul style="list-style-type: none"> <li>○ Where is human in the loop? How is this AI solution placed in business process?</li> <li>○ Who makes final decision? How are risks of possible wrong AI outputs mitigated?</li> <li>○ Data analysis – are data relevant and complete enough?</li> </ul>	<p>Report 1, 2, 3</p>
<p><i>Pilot #10 Real-time cybersecurity analytics on financial transactions' data</i></p>	<p>Goal is to improve the detection of cases of suspected fraudulent transactions, to detect anomalies faster (i.e. in real time) and to unveil potential hidden patterns of cyber-attacks</p>	<ul style="list-style-type: none"> <li>○ Where is human in the loop? How is this AI solution placed in business process?</li> <li>○ Who makes final decision? How are risks of possible wrong AI outputs mitigated?</li> <li>○ Data analysis – are data relevant and complete enough?</li> </ul>	<p>Report 1, 2, 3</p>
<p><i>Pilot #11 Personalized insurance products based on IoT connected vehicles</i></p>	<p>Two AI powered services:</p> <ul style="list-style-type: none"> <li>○ Pay as you Drive, that allows the insurance company to adapt prices by classifying the driver according the way he/she drives</li> <li>○ Fraud Detection which helps to identify the actual driver of a vehicle involved in an incident.</li> </ul>	<ul style="list-style-type: none"> <li>○ Where is human in the loop? How is this AI solution placed in business process?</li> <li>○ Explain possible different consequences of inaccurate AI output and associated measures for risk mitigation</li> <li>○ Focus also on interactions and dependencies between different AI models and associated risks. How happen in case of an inaccurate driver classifier, which has direct consequence in price for particular customer?</li> <li>○ Data analysis Special focus to possible biases:                             <ul style="list-style-type: none"> <li>○ Drivers profiles (diversity of drivers)</li> <li>○ Driver classifier</li> </ul> </li> </ul>	<p>Report 1, 2, 3</p>



<p><i>Pilot #12 Real world data for novel health insurance products</i></p>	<p>Two AI services:</p> <ul style="list-style-type: none"> <li>○ Risk assessment, that allows the insurance company to adapt prices by classifying the client according to their lifestyle;</li> <li>○ Fraud Detection which helps to identify fraudulent behaviour of the clients in using the activity trackers and answering the questionnaires.</li> </ul>	<p>Pilot data will be expanded with synthetic data (simulated users). Therefore, the profiles and patterns cannot be used for actual business decisions, but can be used for proving that technical pipeline is developed and functioning.</p> <p>In case of using real data:</p> <ul style="list-style-type: none"> <li>○ Life style profile – how are validated and maintained?</li> <li>○ Lifestyle classifiers: how is it updated?</li> </ul>	<p>Report 2</p>
<p><i>Pilot #13 Alternative and automated insurance risk selection and insurance product recommendation for SME's</i></p>	<p>AI solution will monitor risk's changes, so it will be able to radically improve the risk management that companies (SMEs) face in the development of their daily activity.</p>	<ul style="list-style-type: none"> <li>○ Where is human in the loop? How is this AI solution placed in business process?</li> <li>○ Explain possible different consequences of inaccurate AI output and associated measures for risk mitigation</li> <li>○ The solution incorporates data from social media, opinion platforms, etc, - what measures will be taken to mitigate possible bias coming from social platforms?</li> </ul>	<p>Report 1,2,3</p>
<p><i>Pilot #14 Big Data and IoT for the Agricultural Insurance Industry</i></p>	<p>The objective of Pilot #14 "is to deliver a commercial service module that will empower insurance companies to better design new products and to enables actuators to be better informed from various data sources.</p>	<ul style="list-style-type: none"> <li>○ Where is human in the loop? How is this AI solution placed in business process?</li> <li>○ Explain possible different consequences of inaccurate AI output and associated measures for risk mitigation</li> <li>○ If risk assessment is directly linked to pricing, partners should provide service which enables humanly readable explanation for AI decision.</li> </ul>	

## 5 Conclusions

This deliverable is an update to its previous version and in its current version it is assessing the most relevant standards and regulations, aiming at specifying the most relevant technological and organizational impact on INFINITECH including technical and organizational measures related to the pilots, their testbeds, sandboxes, and applied technologies. Finally, requirements on dealing with AI in a responsible way are outlined per pilot.

Firstly, the presented security standards define the state of the art of security and privacy measures and thus apply in each testbed, sandbox and technology. It remains upon the pilot leaders and respective participants to decide, which measures will be appropriately implemented.

Secondly, considering the regulations, in an analogous approach the most relevant technical and organizational impacts of the regulations GDPR, PSD II, MIFID II and AMLD 4 have been assessed. The applicability of these regulations has been mapped to the pilot this way; assigning related technical measures to the pilots' testbeds, sandboxes and technologies.

Conclusively, Common organizational measures apply to all organizations/pilots and are listed in a separate section.

## 6 References

- [1] <https://advisera.com/27001academy/what-is-iso-27001/>, page 1 (accessed in December 2020)
- [2] <https://fcicyber.com/top-5-ways-the-financial-services-industry-can-leverage-nist-for-cybersecurity-compliance/> (accessed in December 2020)
- [3] <https://financialservices.mazars.com/gdpr-psd2-issues-fintechs/> (accessed in December 2020)
- [4] Dr. Ann Cavoukian, former Information and Privacy Commissioner of Ontario, Canada; for PbD see <https://iapp.org/resources/article/privacy-by-design-the-7-foundational-principles/> (accessed in November 2020)
- [5] PReparing Industry to Privacy-by-design by supporting its Application in REsearch, Project Description, <https://cordis.europa.eu/project/id/610613> (accessed in November 2020)
- [6] Alberto Crespo García, Nicolás Notario McDonnell, Carmela Troncoso et al, Privacy- and Security-by-Design Methodology Handbook, December 2015, <https://fr.slideshare.net/richard.claassens/prepare-methodologyhandbookfinalfeb242016> and [https://ipen.trialog.com/images/ipen/a/a1/PRIPARE Methodology Handbook Final Feb 24 2016.pdf](https://ipen.trialog.com/images/ipen/a/a1/PRIPARE_Methodology_Handbook_Final_Feb_24_2016.pdf) (accessed in November 2020)
- [7] <https://www.thalesgroup.com/en/markets/digital-identity-and-security/banking-payment/digital-banking/psd2> (accessed in December 2020)
- [8] [https://eba.europa.eu/sites/default/documents/files/documents/10180/2060117/d53bf08f-990b-47ba-b36f-15c985064d47/Final%20report%20on%20EBA%20Guidelines%20on%20the%20security%20measures%20for%20operational%20and%20security%20risks%20under%20PSD2%20\(EBA-GL-2017-17\).pdf](https://eba.europa.eu/sites/default/documents/files/documents/10180/2060117/d53bf08f-990b-47ba-b36f-15c985064d47/Final%20report%20on%20EBA%20Guidelines%20on%20the%20security%20measures%20for%20operational%20and%20security%20risks%20under%20PSD2%20(EBA-GL-2017-17).pdf) (accessed in December 2020)
- [9] <https://www.thalesgroup.com/en/markets/digital-identity-and-security/banking-payment/digital-banking/psd2> (accessed in December 2020)
- [10] <https://www.investopedia.com/terms/m/mifid-ii.asp> (accessed in December 2020)
- [11] Verbatim text from <https://resources.whitesourcesoftware.com/legal/mifid-ii-reforms-and-their-impact-on-technology-and-security> (accessed in December 2020)
- [12] <https://www.redflagalert.com/articles/data/what-is-the-fourth-aml-directive-aml4d> (accessed in December 2020)
- [13] <https://www.loc.gov/law/help/artificial-intelligence/regulation-artificial-intelligence.pdf> (accessed in December 2020)
- [14] <https://www.pdpc.gov.sg/Help-and-Resources/2020/01/Model-AI-Governance-Framework> (accessed in December 2020)
- [15] <https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Resource-for-Organisation/AI/SGModelAIGovFramework2.pdf> (accessed in December 2020)