Integrated Framework for Predictive and Collaborative Security

of Financial Infrastructures

Start Date of Project: 2018-05-01

Duration: 36 months

D2.2 Report on applicable Standards and Regulations

Deliverable Details	
Deliverable Number	D2.2
Deliverable Title	Report on applicable Standards and Regulations
Revision Number	2.1
Author(s)	INNOV
Due Date	31/10/2018
Delivered Date	31/10/2018
Reviewed by	CCA & ORT
Dissemination Level	PU
EC Project Officer	Christoph CASTEX

Contributing Partners	
1.	INNOV-ACTS (responsible)
2.	GFT
3.	SIA
4.	NEXI
5.	LIB
6.	JRC
7.	HDI

This project has received funding from the European Union's Horizon 2020 research and innovation programme 2014-2020 under grant agreement No 786727

Document Status

☒ draft
☒ WP leader accepted
☒ Consortium reviewed
☒ Project coordinator accepted

Revision History

Version	By	Date	Changes
0.4	INNOV	24/07/2018	initial ToC, indicative items
0.5	INNOV	30/07/2018	version circulated to partners
0.8	INNOV	21/09/2018	Contributions from JRC, NEXI, SIA, GFT
1.0	INNOV	29/09/2018	working version circulated to partners
1.9	INNOV	16/10/2018	New version for review
1.91	INNNOV-HDI-GFT	18/10/2018	Update information from HDI-GFT
1.92	GFT	24/10/2018	Update information about BaFin
1.93	CCA	25/10/2018	Internal review from CCA
1.94	ORT	28/10/2018	Internal review from ORT
2.1	INNOV	29/10/2018	Final version

Abbreviations

AEI	Automatic Exchange of Information
ADC	Account Data Compromise
AML	Anti Money Laundering
BAIT	Bankaufsichtliche Anforderungen an die IT
BCP	Business Continuity Plan
BCM	Business Continuity Management
BCMS	Business Continuity Management System
CA	Competent Authorities
CEBS	Committee of European Banking Supervisors
CERT	Computer Emergency Response Team
CMDB	Configuration Management Database
CIA	Confidentiality, Integrity and Availability
CSIRT	Computer Security Incident Response Team
CI	Critical Infrastructure
CSC	Common and Secure Communication
DPA	Data Protection Authority
DPO	Data Protection Officer
DSP	Digital Service Providers
EBA	European Banking Authority
ECB	European Central Bank
EU	European Union
EUC	End-User Computing
FATCA	Foreign Account Tax Compliance Act
GDPR	General Data Protection Regulation
GLB	Gramm-Leach-Bliley Act
ICT	Information Communication Technologies
IEC	International Electrotechnical Commission
IDS	Intrusion Detection System
eID	electronic Identification
eIDAS	electronic IDentification, Authentication and trust Services
eTS	electronic Trust Services
IaaS	Infrastructure as a Service
ISMS	Information Security Management System
ISO	International Organization for Standardization

ISP	Internet Service Provider
KYC	Know Your Customer
LOPD	Law for Protection of Personal Data
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

Executive Summary

This deliverable reports on regulations, directives and standards that underline the security of the infrastructure employed in the financial sector. Aimed at complementing the requirements elicitation effort of T2.1, this deliverable identifies additional requirements arising from the need for financial organizations to comply with certain regulations and standards. To this end, it reviews existing laws, regulations, standards and directives that apply for financial infrastructures and analyses their impact on the security of financial services. More specifically, this deliverable provides an extensive description of the regulations relevant to financial institutions as defined by supervising authorities and regulatory bodies such as the Markets in Financial Instrument Directive MFID II, the European Central Bank Cyber Incident Reporting Regime, the Payments Services Directive (PSD2), the Payment Card Industry Data Security Standard (PCI DSS) and many others. Additionally, it also provides an overview of the standards associated to the financial sector such as the ISO 27000 family of standards. Beyond regulations that are directly relevant to the financial sector, it also provides an insightful analysis of general regulations that have an impact on FINSEC the most prominent example being the GDPR, as well as e-Privacy and eIDAS (electronic IDentification, Authentication and trust Services). The deliverable then reflects on the regulations, standards and directives with respect to the pilots included in the FINSEC project as well as their implications for the components of the FINSEC project and the design of the project's architecture (e.g. APIs, CCTV etc.). As a result of this analysis, the deliverable provides a list of recommendations that could be employed by the FINSEC project. To illustrate, following the emergence of data-extrapolation and de-anonymisation services that make undesirable and anti-privacy deductions about end-users, the role of DPO may well expand to using applicable standards to protect the profile of end-users; FINSEC work packages can provide the basis for institutions to expand their privacy services in such ways.

TABLE OF CONTENTS

List of Tables

List of figures

1. Introduction

1.1. Motivation and Objective

The FINSEC project aims to develop, demonstrate and bring to market an integrated, intelligent, collaborative and predictive approach to the security of critical infrastructures in the financial sector. To achieve this goal, it is necessary to understand the regulations that underline the security of the infrastructure employed in the financial sector. Given the complexity of the financial services sector and the different requirements regarding financial security, there is a plethora of different regulations, standards and directives that frame the way in which financial infrastructures acquire, handle, store, communicate and process information. Such regulations and standards may apply at a national, regional or global level, whereas they may aim at fulfilling limitations, extending or complementing existing regulations or standards. Overall, there exists a large variety of regulations and trends relevant to the security of financial services. At the same time, the standardization landscape for the financial sector is evolving at a very fast pace. Hence, this introduces significant challenges for the financial technologies sector. As a result, striking the right balance between ensuring the safety of the banking system and minimising the risk of introducing unnecessary barriers to innovation in the financial sector is a challenging task for all relevant stakeholders.

This deliverable provides an in-depth review of the existing laws, regulations, standards and directives that apply to financial infrastructures. More specifically, it reports on the work and the outcomes of Task 2.2, "Review of Applicable Laws, Regulations and Standards". The main outcome of the task is a set of requirements that should be taken into account in the development of the FINSEC architecture and toolbox. The content of this deliverable complements the insights arising by the activities of the requirements' definition achieved in T2.1, with additional requirements stemming from the need for financial organizations to comply with regulations and standards.

The deliverable comes at a period of time almost five months after the General Data Protection Regulation (GDPR) entered into force, transforming the requirements for privacy, and also four months after the deadline for the adoption of the important Network and information systems (NIS) directive by national legislation. The recent advent of Payment Service Directive 2 (PSD2) is also important as it brings notable changes in the security associated with customer payments. Beyond providing an extended analysis of this regulations and directives with respect to the security of financial infrastructures, this deliverable also includes thorough analysis of other existing or forthcoming financial regulations imposed by supervising authorities and regulatory bodies including MiFiD II.

Subsection 1.2 provides more information on the methodology followed for extracting insights through a variety of sources relevant to each regulations. It also clarifies the approach followed in this task for organising and presenting existing regulations so as to ensure that the deliverable will provide value to the project's partners.

1.2. Methodology

The elicitation of information presented in this report was based on the combination of the results of a desktop survey of known standards and regulations applicable to organizations active in the financial sector including insurance as well as on the collection and processing of the information provided by the end users.

Interaction with end users was based on one-to-one e-meetings that took place on M1, the subsequent distribution of the questionnaire on the Month M2 and the discussions that followed the analysis of the filled questionnaires based both on one-to-one meetings during M3 and the discussion with all the end-users (M3-M4). Furthermore as the document was nearing its completion, the

reviewers' comments triggered more feedback from users; this helped to further clarify some of the regulatory requirements especially in terms of novel schemes (e.g. P2P payment security).

This deliverable emphasizes the laws, regulations and directives of the European Union, as they are applicable to all the partners included in the FINSEC project. However, in a few cases the deliverable also makes reference to regulations applicable in other regions such as the U.S. (e.g. beyond its extensive analysis of the impact of GDPR, it also includes a small summary of the US privacy rules included Gramm-Leach-Bliley Act) so as to highlight similarities and differences between the region.

All laws, regulations, directives and standards that are reviewed in this deliverable were organised based on their nature or purpose. In particular, regulations that are directly relevant to the financial sector are grouped under the 'Financial regulations' category. 'Information security and standards' (e.g. NIS), are reported as a separate category whereas 'General purpose regulations' that are also relevant to the financial sector (e.g. GDPR) are reported as a third category of regulations. These categories are reported in this deliverable in Sections 2, 3 and 4 respectively. For each regulation, its impact on the FINSEC sector is discussed whereas this deliverable also makes a first attempt to analyse the impact of these regulations with respect to each pilot included in the project.

2. Financial regulations, supervising authorities and regulatory bodies

2.1. Markets in Financial Instruments Directive II – MiFiD II

MiFiD II [1] encapsulates both legislations on Markets in Financial Instruments Directive ("MiFID") and the Regulation on Markets in Financial Instruments and Amending Regulation ("MiFIR"). MiFiD has been generated by the European Commission and it relates to a Europe-wide legislative framework for regulating the operation of financial markets in the European Union. The framework was put in force in January 2018. It represents a major overhaul of the existing law, building on and extending the scope of the first MiFID. MiFID regards the framework of trading venues/structures in which financial instruments are traded, whereas MiFIR focuses on regulating the operation of those trading venues/structures, looking to processes, systems and governance measures adopted by market participants and to their future supervision.

Scope of the Regulation. The legislation aims to establish a safer, sounder, more transparent and more responsible financial system [2]. More specifically, MiFID II includes objectives which are relevant to Fintech and Financial Security, including algorithmic trading activities, which are enhanced by MiFID II as the directive introduces trading controls for algorithmic trading activities, which have led to much increased speed of trading and thus the possibility of causing systemic risks. Investment firms that are providing direct electronic access to trading venues are enforced to have in place systems and risk controls such that they could effectively prevent trading that may contribute to a disorderly market or involve market abuse.

Impact on financial service providers. MiFID II is widely viewed as significant legislation which will fundamentally reshape European financial markets. For the financial sector and trading in particular, one of the main MiFiD II effects is that traders are provided with enhanced transparency as the system enforces the brokers to increase the information reported. It also has a major impact on algorithmic trading, as it mandates the testing of algorithms and the need to add new tags to precisely identify the origins of an order.

2.2. Payments Services Directive (PSD 2) - Directive 2015/2366

The revised Payment Services Directive (PSD2) [3] enhances innovation potential, competition and efficiency in electronic markets. It offers consumers more and better choice in the EU retail payment market. At the same time, it introduces higher security standards for online payments. The directive's

deadline to transpose PSD2 in member states was January 2018, whereas it is expected to be put into force in April 2019 [4]. Reflecting the challenges of digital economy, the actions of all the active members of the payments value chain are affected.

Scope of the Regulation. PSD2 will bring changes with respect to the range of transactions, the scope of stakeholders, liability and information and security assessment [5]. In particular, PSD2 will extend the EU's regulatory framework on transactions and will also enhance the Payment Service Provider (PSP) with an additional category, the Third-Party Service Providers (TPSPs) – including Account Information Service Providers (AISPs) and Payment Information Service Providers (PISPs). AISPs will provide a complete view of the payer's accounts to any relevant financial institution. Information Service Providers (ISPs) will connect the payer's and the payee's banking platforms.

To enable the operation of TPSPs, financial institutions will be required to fulfil account information and payment initiation requests by providing TPSPs with the necessary information via Application Programming Interfaces (APIs)—given that they will be authorised by the payer. In this way, the directive will allow the payers to gain additional protection for the case of any incorrectly executed payments as payments will need to be processed through "strong customer authentication" and hence it will be impossible, for information related to the payer that will be exchanged through APIs, to be retained for any other purposes than completing the payment.

Impact on financial institutions and service providers. Financial institutions will have to ensure their compliance with additional information and technology requirements. This will be relevant to setting up APIs such that it will encapsulate specific monetised services, existing margins, and simplified and optimised infrastructure. PSD2 will also contribute on setting up the mechanisms that will foster strong customer authentication. In the case of Third Party Service Providers (TPSPs) PSD2 will enable TPSPs to extend their consumer base as consumers are expected to increase their interest in initiating their payments through TPSPs. TPSPs will have to as a payment institution with the local regulator, set up risk and control frameworks, comply with all relevant reporting obligations, and perform AML and KYC controls.

2.2.1. PSD2 - Regulatory Technical Standards (RTS)

PSD2 [6] empowers the Commission to adopt regulatory technical standards (RTS) on the basis of the draft submitted by the European Banking Authority (EBA), thereby enabling consumers to benefit from safer and more innovative electronic payments. RTS for strong customer authentication (SCA) and secure open standards of communication (CSC) are the basis for the implementation of PSD2 [7].

Scope of the Standards. The RTS makes SCA the basis for accessing one's payment account, as well as for making payments online. RTS formulate specific security measures to ensure the effective and secure communication between relevant actors. More specifically, SCA requires that the customer's identity is verified using at least two mechanisms of the a) knowledge (i.e. something that only the user knows e.g. Password), b) possession (i.e. something only the user possesses, e.g. a card, mobile phone), c) inheritance (i.e. something the user is, e.g. biometric). CSC is the second major principle described in the RTS. The RTS regulates the way the customer's account is shared between the ASPSP and the AISP or PISP. The RTS requires customers to provide their explicit consent to the AISP or PISP to share their payment account details or initiate a payment transaction. A secure communication channel will be established to provide access to the payment account.

Impact on payment service providers. Payment services providers (PSPs) need to ensure that their technology and infrastructure provides customers with the ability to identify themselves using more than one authentication mechanism. Additionally, to foster SCC, a dedicated communication interface needs to be implemented. There are two different options for achieving SCC. The first option is to create an API that will provide identical level of availability and performance as the customer's online interface and it will also enable the provider to also offer a payment initiation of account information services without any obstacle. There also be a fall-back mechanism designed such that measures will

be made available to restore access to the customer payment account if the API is not available. The second option is to offer an adaptation of the customer's online banking interface. In other words, through the proposed adaptation the customer's payment account will be accessed using personalized security credentials by the TPP such that it can be adjusted to desired interface. To implement this, the ASPSP needs to know when access to the account is initiated by the customer. It also requires that there is consent by the customer on the access, use and processing of their payment information.

2.3. PCI DSS and PCI 3DS

The Payment Card Industry Data Security Standard (PCI DSS) issued by the Payment Card Industry Security Standards Council, is a worldwide information security standard, for securing card payments. It was originally designed for the handling of credit card information by payment companies such as Visa and MasterCard and its main purpose is to prevent credit card fraud. Among the main goals of the standard is to ensure that 'cardholder data' as the full Primary Account Number (PAN) or the full PAN along with Cardholder name, the expiration date, the service code and sensitive authentication data (full magnetic stripe data, CAV2, CVC2, CVV2, CID, PINs, PIN blocks) are protected.

The Three-Domain Secure (3DS) is a messaging protocol that enables consumers to authenticate themselves with their card issuer when making e-commerce purchases. The additional security layer helps prevent unauthorized transactions where the "Card is not Presented" (e-commerce transactions also called CNP transactions in the industry) and protects the merchant from fraud [8].

Scope. The PCI DSS is very specific to the payment card sector and it is relevant to the payment functions of business systems. Compliance of PCI DSS is imposed by Credit card processors to card issuers and merchant banks. The standard introduces a number of requirements, which include the establishment of an effective operational and security risk management framework; processes that detect, prevent and monitor potential security breaches and threats; risk assessment procedures; regular testing; and processes that raise awareness to Payment Service Users on security risks and risk-mitigating actions. Additionally, specific Vulnerability Scans must be conducted by a PCI Approved Scanning Vendor (ASV) at Payment gateways.

Impact on financial services. The requirements of the directive aim to establish that any physical access to data or systems that house cardholder data should be appropriately restricted. These requirements have significant impact on the protection expected from cyber-physical threats.

2.4. National regulatory bodies – German supervisor authority (BaFIN)

BaFin is the (German) acronym for the Federal Financial Supervisory Authority in Germany. BaFin published in November 2017, introduced the supervisory requirements for IT in financial institutions ("Bankaufsichtliche Anforderungen an die IT" – BAIT). BAIT addresses the requirements that will lead to the secure design of IT systems and of the associated processes, as well as to the relevant requirements related to IT governance. It contains interpretation of the legal regulations according to KWG (Kreditwesengesetz = German Banking Act), MaRisk (Mindestanforderungen Risiko Management = Minimum Requirements for Risk Management) and the supervisory authority's expectations, concerning appropriate technical and organisational equipment of IT systems with respect to information security and adequate contingency planning. Furthermore, requirements on outsourcing and IT services supplied by third parties are covered in a dedicated module.

2.4.1. Supervisory requirements for IT in financial institutions - BAIT

BAIT [9] is structured into nine (9) modules with the aim of raising IT risk awareness, especially at management levels, where the term "IT risk" shall address:

- all risks to the institution's financial position and financial performance that arise from deficiencies relating to IT management;

- the availability, confidentiality, integrity and authenticity of data;
- the internal control system for IT organisation; and
- the IT strategy, IT guidelines and IT topics in the rules of procedure, or the use of information technology.

The nine modules are described below:

1. **IT strategy**. The central requirement with regard to the IT strategy is that the management board must regularly deal with the strategic implications of IT's various aspects for the institution's business strategy and the resulting measures to achieve its goals which have to be published internally within the institutions.
2. **IT governance**. The management board must ensure that the functions of information risk management, information security management, IT operations and application development are appropriately staffed and monitored.
3. **Information risk management.** As part of its information risk management policy, each institution must ascertain its respective protection requirements, determine target measures based on them and compare these to the measures which have been successfully implemented.
4. **Information security management**. An information security policy must be defined and published internally. The protection requirements defined as part of information risk management must be fleshed out in the form of information security guidelines.
5. **User access management.** The concept of a user's access rights must be specified in written form and adhere to the "need-to-know" principle. This principle means that user's access rights are only to be granted if they are needed to fulfil a specific task. The same can be said of the recertification process, in which the access rights granted are checked and any deviations from the need-to-know principle are detected.
6. **IT projects and application development.** The management and monitoring of IT projects must give particular consideration to the risks relating to such projects' duration, use of resources and quality. The management board must ensure that a full overview of the IT project risks have been conducted and those risks that arise from interdependencies between different projects have been addressed. Even when applications are first being developed, precautions must be taken to safeguard the confidentiality, integrity, availability and authenticity of the data to be processed. These provisions serve to reduce the risk of any unintentional alteration or intentional manipulation of applications and data.
   In BaFin's view, end-user computing (EUC) applications developed or operated by an institution's organisational units should be divided into risk classes. This policy achieves transparency within the institution in relation to the risks arising from the use of such applications. Furthermore, banking supervisors expect the institution to maintain a central register of all EUC applications, especially those that are important for banking business processes, for risk management and monitoring or for accounting purposes.
7. **IT operations**. Awareness about IT risks is also significantly raised by taking into account the risks that arise from outdated IT systems and associated practice. In order for product and process lifecycles to be managed accordingly, it is nonetheless necessary for the components of the IT systems, including inventory data, to be subject to the appropriate administration. To this end, the institutions should use a configuration management database (CMDB). Suitable criteria must be set for informing the management board about unplanned deviations from regular operations (disruptions) and their causes, about the contingency measures taken to maintain or re-establish business operations and about the remedying of deficiencies. This enables the board to manage IT risk in an appropriate manner.
8. **Outsourcing and other external procurement of IT services**. Any outsourcing of IT services must be evaluated in a risk analysis. The risks originating from any other external provision of IT services must also be evaluated, as otherwise it is not possible to comprehensively ascertain

the risk situation or detect concentration risks in the area of IT services. Furthermore, the measures determined from the risk analysis influence the formulation of the contracts.

9. **KRITIS.** Ensure the availability, integrity, authenticity and confidentiality of information processing for critical infrastructures. KRITIS operators (and in the case of outsourcing, in addition to their IT service providers) are entitled to take appropriate measures such that they can effectively ensure the safe operation of critical infrastructures.

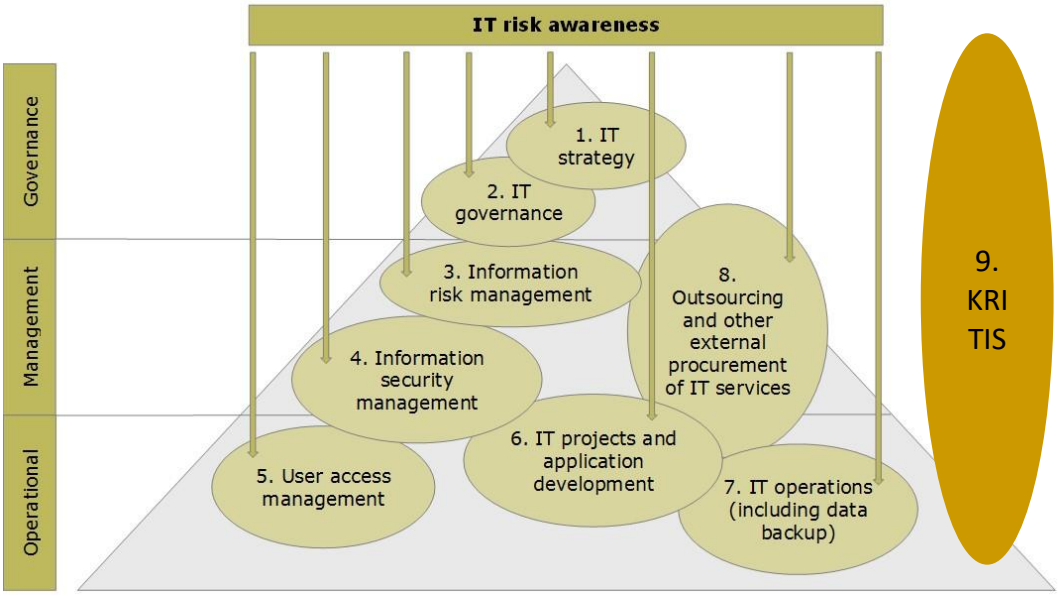

Figure 1: Improving risk awareness with the BAIT (source: BaFin [9])

The BAIT regulation explicitly does not intend to be technically exhaustive and therefore specifically mentions the obligation to comply with standards for information security as e.g. defined by the German BSI (Bundesamt für Sicherheit in der Informationstechnik = Federal Office for information security) in the IT-Grundschutz Catalogues (IT-Grundschutzkataloge) and the international security standards ISO/IEC 2700X.

One of the essential features of the BAIT is that the principle of dual proportionality applies without restriction. This principle stipulates that both the management instruments of the bank and the intensity of monitoring by banking supervisors should be proportional to the bank's risks. This principle **differentiates rules and supervisory practices for SMEs** and relieves SMEs from some of the strong specifications that are not relevant to them.

2.4.2. Further development of the BAIT

BaFin is currently examining whether the Fundamental Elements for Cyber Security, published by the G7 in October 2016, can be implemented by adjusting the BAIT. A further addition to the BAIT dealing with IT contingency management, including test and recovery procedures, is being planned as well. In the context of the planned Europe-wide harmonisation of supervisory requirements for the management of IT risks in financial institutions, BaFin will be actively drawing the BAIT into the

discussion process. Table 2 covers all of the nine [9] modules of the BAIT[1] and derives impacts to the FINSEC SECaaS pilot[2].

2.5. National regulatory bodies – IVASS

IVASS is the Italian Institute for the Supervision of Insurance. It pursues the stability of the financial system and markets. National regulation 38/2018 (*related to the provisions on the corporate governance system of insurance companies and groups* (Private Insurance Code)) is of relevance to financial security services as explained in section 5.6. Insurance Risk Assessment.

2.6. European Banking Authority III

The European Banking Authority (EBA) is an independent EU Authority which works to ensure effective and consistent prudential regulation and supervision across the European banking sector. Its overall objectives are to maintain financial stability in the EU and to safeguard the integrity, efficiency and orderly functioning of the banking sector.

As part of its task of establishing consistent, efficient and effective supervisory practices across the EU and ensure uniform application of Union law, the European Banking Authority (EBA) issues regulatory guidelines and recommendations in its fields of competence. Regulation (EU) No 1093/2010 establishing the EBA requires that competent authorities and financial institutions make every effort to comply with the EBA guidelines and recommendations (Article 16).

Scope of the regulation: The Article 9(2) of the EBA's Founding Regulation mandates the Authority to monitor new and existing financial activities. This obligation extends to all areas of the EBA's competence, including the field of activities of credit institutions, financial conglomerates, investment firms, payment institutions, and electronic money institutions.

The following section is a selection of EBA Recommendations with relevance to the project.

2.6.1. Recommendations on outsourcing to cloud service providers

On 2006 the guidelines for Outsourcing were published, in order to pursue harmonisation at the EU level in the area of outsourcing undertaken by credit institutions and additionally to promote greater consistency of approach where possible within the national legal frameworks. The recommendations were actually a response to the pressing need for a common approach to converge nation-specific policies into one common EU supervisory framework.

Scope of the recommendations. These recommendations further specify conditions for outsourcing as referred to in the guidelines published by the *Committee of European Banking Supervisors* (CEBS) on outsourcing of 14 December 2006 [10] and apply to outsourcing by institutions as defined in point (3) of Article 4(1) of Regulation (EU) No 575/2013 to cloud service providers. The guidelines are consistent with the Markets in Financial Instruments Directive (MiFID) and its application to credit institutions. Competent Authorities must notify the EBA as to whether they comply or intend to comply with these recommendations, or otherwise with reasons for non-compliance, by 28.05.2018 (as indicated in Article 16(3) of Regulation (EU) No 1093/2010).

The first recommendation indicates that prior to any outsourcing of their activities, actors must assess which activities should be considered as "material" on the basis of guideline 1(f) of the

[1] (Source text only available in German) Rundschreiben 10/2017 (BA) in der Fassung vom 14.09.2018 https://www.bafin.de/SharedDocs/Downloads/DE/Rundschreiben/dl_rs_1710_ba_BAIT.pdf?__blob=publicationFile&v=9

[2] Initially eight modules were prescribed. A ninth module, that refers to KRITIS (Kritische Infrastrukturen) critical infrastructures, was added by BaFin on 14/09/2018, in response to the German Federal Act to "Strengthen the Security of Federal Information Technology": https://www.bsi.bund.de/EN/TheBSI/BSIAct/bsiact_node.html

CEBS guidelines and, as regards outsourcing to cloud service providers in particular, taking into account all of the following:

a) the criticality and inherent risk profile of the activities to be outsourced, i.e. whether these activities are critical to the business continuity/viability of the institution and its obligations to customers;
b) the direct operational impact of outages, and related legal and reputational risks;
c) the impact that any disruption of the activity might have on the institution's revenue prospects; and
d) the potential impact that a confidentiality breach or failure of data integrity could have on the institution and its customers.

The second recommendation indicates the duty to adequately inform the competent authorities of material activities [11] to be outsourced to cloud service providers. A risk analysis is advised, stressing Business Continuity aspects including "*the availability by the cloud service provider of a business continuity plan that is suitable for the services provided to the outsourcing institution; the existence of an exit strategy for the outsourcing institution in case of termination by either party or disruption of provision of the services by the cloud service provider; and whether the outsourcing institution maintains the skills and resources necessary to adequately monitor the outsourced activities*".

A third recommendation is that outsourcing institutions should ensure that they have in place a written agreement with the cloud service provider whereby "*the latter undertakes the obligation to provide full access to its business premises*" where the term "*right of access*" to the buildings, installations and equipment involved in the delivery of services is required, as well as "*to reserve for itself unrestricted rights of inspection of the cloud service provider*". The availability of the subcontractor for a notified on-site inspection is stressed.

A further recommendation focuses on the outsourcing contract, which should oblige the outsourcing service provider to protect the confidentiality of the information transmitted by the financial institution. The need for a service level agreement is highlighted: "*the respective needs of outsourcing institutions with respect to quality and performance should feed into written outsourcing contracts and service level agreements.*"

Another recommendation has to do with the location of the premises inside the EEA; as stated in guideline 4(4), "*institutions should take special care when entering into and managing outsourcing agreements undertaken outside the EEA because of possible data protection risks and risks to effective supervision by the supervisory authority*". The selection of the location should include considerations "*on the wider political and security stability of the jurisdictions in question; the laws in force in those jurisdictions (including laws on data protection); and the law enforcement provisions in place in those jurisdictions, including the insolvency law provisions that would apply in the event of a cloud service provider's failure*".

A final recommendation is to identify cases of chain outsourcing. The recommendation indicates that institutions should take account of the risks associated with 'chain' outsourcing, where the outsourcing service provider subcontracts elements of the service to other providers. According to the recommendation "*The outsourcing institution should agree to chain outsourcing only if the subcontractor will also fully comply with the obligations existing between the outsourcing institution and the outsourcing service provider. Furthermore, the outsourcing institution should take appropriate steps to address the risk of any weakness or failure in the provision of the subcontracted activities having a significant effect on the outsourcing service provider's ability to meet its responsibilities under the outsourcing agreement*".

2.6.2. Guidelines on security measures for operational and security risks under the PSD2

The Guidelines "on security measures for operational and security risks under the PSD2" [12] specify requirements for the establishment, implementation and monitoring of the security measures that

the Payment Service Providers (PSPs) must take, in accordance with the Article 95(1) of the Directive (EU) 2015/2366, on how to manage the operational and security risks relating to the payment services that they provide.

Scope of the guidelines. The guidelines address to all PSPs, who are expected to comply with all the provisions set out in these Guidelines. The level of detail should be proportionate to the PSP's size and to the nature, scope, complexity and riskiness of the particular services that the PSP provides or intends to provide [13]. These Guidelines apply from 13 January 2018.

Protection. In the specific "Protection" guideline the PSPs are asked to establish and implement a 'defence-in-depth' approach by instituting multi-layered controls covering people, processes and technology, with each layer serving as a safety net for preceding layers. The Defence-in-depth should be understood as having defined more than one control covering the same risk, such as the four-eyes principle, two-factor authentication, network segmentation and multiple firewalls.

Integrity and Confidentiality. Part of the protection guidelines, is the specific "Data and systems integrity and confidentiality" Guideline, by which the PSPs are required to 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 order to verify the integrity of software, firmware and information on their payment services.

Physical security. In the "Physical security" guideline, the PSP are (in a quite generic way) asked to have "appropriate" physical security measures in place, to protect the sensitive payment data of the Payment Service Users (PSUs) as well as the ICT systems used to provide payment services.

Access Control. In the "Access Control" guideline the provision of physical and logical access on a "Need-to-know" basis as well as the establishment of specific role-based access rules are highlighted.

Detection. In the "Continuous monitoring and detection" guideline section, the PSPs are required to 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. PSPs are also required to implement detective measures to identify possible information leakages, malicious code and other security threats, and publicly known vulnerabilities for software and hardware, and to check for corresponding new security updates. In case of incidents (operational and security), the PSPs are required to monitor and report them. This requires that appropriate criteria and thresholds for classifying an event as an operational or security incident are determined, as well as early warning indicators that should serve as an alert for the PSP to enable early detection of operational or security incidents. Appropriate processes and organisational structures to ensure the consistent and integrated monitoring, handling and follow-up of operational or security incidents, need also to be established.

Business continuity. The PCP is required to have a Business Continuity Plan (BCP) in place to make sure that it can react appropriately to emergencies and that is able to maintain its critical business activities; and identify and be ready to implement specific mitigation measures in the event of termination of its payment services and termination of existing contracts, in order to avoid adverse effects on payment systems and on PSUs and to ensure execution of pending payment transactions.

Scenario-based BCP. The PSP should consider a range of different scenarios, including extreme but plausible ones, to which it might be exposed, and assess the potential impact such scenarios might have. Based on the plausible scenarios identified the PSP should develop response and recovery plans, which should a) focus on the impact on the operation of critical functions, processes, systems, transactions and interdependencies; b) be documented and made available to the business and

support units and readily accessible in case of emergency; and c) be updated in line with lessons learned from the tests, new risks and threats identified and changed recovery objectives and priorities.

Testing the BCP. The PSPs should test their BCPs for the operation of their critical functions, processes, systems, transactions and interdependencies at least annually. Plans should be updated at least annually, based on testing results, current threat intelligence, information-sharing and lessons learned from previous events, and changing recovery objectives, as well as analysis of operationally and technically plausible scenarios that have not yet occurred, and, if relevant, after changes in systems and processes. What is really important is that the updated plans should be designed to challenge the assumptions on which BCPs rest, including governance arrangements and crisis communication plans.

Crisis communication. The PSPs are required to have effective crisis communication measures in place, so that all relevant internal and external stakeholders, including external service providers, are informed in a timely and appropriate manner.

2.6.3. Opinion document on RTS for SCA and CSC

More recently, the European Banking Authority (EBA) publishes opinions of interest about FINSEC.

The most recent one is "On the implementation of the regulatory technical standards (RTS) on strong customer authentication (SCA) and common and secure communication (CSC), which will apply from 14 September 2019". In the Opinion, the EBA clarifies a number of issues identified by market participants and Competent Authorities (CAs) to assist in this implementation.

2.6.4. Regulatory Framework for Mitigating Key Resilience Risks

With the increased digitalisation of the financial services, financial institutions are becoming more intertwined and dependent on computer networks and third party service providers. An insufficient level of protection against cyber incidents and a failure of critical IT infrastructure could lead to major damage in individual financial institutions and have potential spillover effect on the whole financial system. This explains why ICT related risks, and in particular cybersecurity, are high on the agenda of policymakers, regulators and supervisors of the financial sector.

In line with its mandate to ensure effective and consistent prudential regulation and supervision across the European financial sector, the EBA has undertaken several initiatives to adjust the regulatory framework and promote consistent supervisory practices, both for payment and for financial institutions include in the field of cybersecurity.

While some pieces of our work are still in the pipeline, the regulatory and supervisory framework related to operational resilience is built around the following three areas:

- Regulation: strengthening governance and risk management arrangements;
- Supervision: common framework for supervisory assessment and knowledge sharing; and
- Resilience testing: sound and proportionate resilience testing.

2.7. Regulation for insurance security

The directives affecting the operation of the insurance sector are presented below, along with the guidance from the national and European supervision authorities.

IVASS is the Italian Institute for the Supervision of Insurance. It pursues the stability of the financial system and markets. National regulation 38/2018 [14] is particularly important and imposes a series of obligations for the insurance companies, impacting the following functions: Board of Directors; Corporate Bodies; Internal Controls System; Risk Management System; Fundamental SII Functions (Risk Management, Compliance, Actuarial Function, Internal Audit); ICT / Cyber security; Reinsurance; Capital Management; Professionalism, integrity and independence; Compensation; Outsourcing; Corporate Group Governance.

With regard to the strategic Information and Communication Technology plan, the definition and approval by the Board of a corporate governance policy, including data quality and cyber security profiles, are of particular importance. The regulation states that IVASS will receive notification of any serious IT security incident.

The **European Insurance and Occupational Pensions Authority (EIOPA)** is a European Agency commissioned aiming to monitor and identify trends, potential risks and vulnerabilities stemming from the micro-prudential level, across borders and across sectors. Its core responsibilities are to support the stability of the financial system, transparency of markets and financial products as well as the protection of policyholders, pension scheme members and beneficiaries.

Solvency is a Directive in European Union law that codifies and harmonises the EU insurance regulation. The framework states that insurance organizations must guarantee business continuity through the development of business continuity plans which should include cyber security implementation measures.

2.8. European Central Bank (ECB) cyber incident reporting regime

The ECB cooperates with EU national central banks to ensure the confidentiality, availability and integrity of data. Its aim is to protect against cyber-attacks, limit the impact of a data breach and ensure that the bank system continues to operate. ECB collaborates with other EU institutions such as the EU Computer Emergency Response Team (CERT-EU); CERT EU warns its members about new threats, provides testing and offers advisory services. The ECB facilitates exchanges of security information among a global network of central banks and international financial organisations.

The ECB confirmed that the mandatory cyber incident reporting requirements do not stem directly from a specific EU directive (e.g. NIS) or regulation. Instead, it states that the requirements were developed by its Governing Council, using requirements set out in two previous regulations, including the REGULATION OF THE EUROPEAN CENTRAL BANK (EU) No 795/2014 of 3 July 2014, on oversight requirements for systemically important payment systems.

The ECB's responsibility for determining the security of network and information systems or the notification of cyber-security incidents, is indeed recognized by the NIS Directive (presented in section 3.3 of the report). The NIS Directive specifically allows the exemption of organizations who might otherwise be classed as "operators of essential services" from the NIS regime, if there are already "Union legal acts" that set out sector-specific security requirements. It is clearly indicated that the sector specific requirements "are at least equivalent in effect" to the obligations set out in the NIS Directive.

The ECB has not however (as of the time of writing of this report) published the cyber incident reporting requirements that it has issued for the banks, as the documents are deemed confidential.

3. Information Security standards and directives

3.1. ISO/IEC 27000 standards' family

The ISO/IEC 27000-series [15] comprises information security standards published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). The series provides best practice recommendations on information security management - the management of information risks through information security controls - within the context of an overall Information security management system (ISMS), similar in design to the management systems for quality assurance (the ISO 9000 series), environmental protection (the ISO 14000 series) and other management systems. The series is deliberately broad in scope, covering more than just privacy, confidentiality and IT/technical/cyber-security issues. It is applicable to organizations of all shapes and sizes. All organizations are encouraged to assess their information risks, then treat them (typically using information security controls) according to their needs, using the guidance and suggestions where relevant. Given the dynamic nature of information risk and security, the ISMS concept incorporates continuous feedback and improvement activities to respond to changes in the threats, vulnerabilities or impacts of incidents.

Scope of the Standard. ISO/IEC 27000 describes the fundamentals on information technology with respect to security techniques and information security management systems. In particular, the ISO/IEC 27000 provides additional support to the financial industry to set up an appropriate information security management system for the provisioning of their financial services, while giving more confidence to their customers.

The adoption of the standard is not universal in the finance and banking sector, although the compliance of financial organisations is recommended. The benefits of implementing an ISMS will primarily result from a reduction in information security risks (i.e. reducing the probability of, and/or impact caused by, information security incidents). However, a supplement to the ISO/IEC 27001 family of standards, ISO/IEC TR 27015: 2012 "Information technology – Security techniques – Information security management guidelines for financial services" (more details at section 3.2), provides sector-specific guidance for the financial sector with respect to information security of assets, as well as information processing for organizations providing financial services, in order to support the information security management of their assets and processed information. Financial services organisations process sensitive financial and customer data and ISO/IEC 27002:2005 can contribute by providing additional guidance to the information security of financial services organisations such that they can effectively manage their information security risks.

The ISO 27000 series includes a sequence of standards with respect to some particular areas of information security. In particular, ISO/IEC 27001 regards information security management and specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving formalized ISMS within the context of the organization's overall business risks. It specifies requirements for the implementation of information security controls, customized to the needs of individual organizations or parts thereof. ISO/IEC 27001 provides normative requirements for the development and operation of an Information System Management Systems, including a set of controls for the control and mitigation of the risks associated with the information assets, which the organization seeks to protect by operating its Information System Management Systems. Organizations operating an Information System Management Systems may have its conformity audited and certified.

ISO/IEC 27001 formally defines the mandatory requirements for an Information Security Management System (ISMS). However, ISO/IEC 27002 provides a code of practice certification standard with respect to Information Security Management System (ISMS). It outlines recommendations on information security controls such that information security control objectives arising from risks to the confidentiality, integrity and availability of information can be addressed. Organizations that adopt

ISO/IEC 27002 are required to own information risks, clarify their control objectives and apply suitable controls (or indeed other forms of risk treatment) using the standard for guidance.

The standard is structured logically around groups of related security controls. Many controls could have been put in several sections but, to avoid duplication and conflict, they were arbitrarily assigned to one and, in some cases, cross-referenced from elsewhere. For example, a card-access-control system for, say, a computer room or archive/vault is both an access control and a physical control that involves technology plus the associated management/administration and usage procedures and policies. This has resulted in a few oddities (such as section 6.2 on mobile devices and teleworking being part of section 6 on the organization of information security) but it is at least a reasonably comprehensive structure. It may not be perfect but it is good enough on the whole.

Impact on FINSEC. The Annex A, where all the requirements are stated, has a number of requirements that have relevance to FINSEC.

- Section A.6.2 "*External parties*", defines specific requirements for "*maintaining the security of the organization's information and information processing facilities that are accessed, processed, communicated to, or managed by external parties*". The clause about "*Agreements with third parties involving accessing, processing, communicating or managing the organization's information or information processing facilities, or adding products or services to information processing facilities*" requires that they "*cover all relevant security requirements*".
- Section A.10.8 on the "*Exchange of information*", whose objective is to "*maintain the security of information and software exchanged within an organization and with any external entity*" which leads to need to share and exchange information with other parties in a supply chain.
- Section A12.6 is about reducing risks resulting from exploitation of published technical vulnerabilities and indicates that "*Timely information about technical vulnerabilities of information systems being used shall be obtained, the organization's exposure to such vulnerabilities evaluated, and appropriate measures taken to address the associated risk*".
- The section A.13.1 is about reporting information security events and weaknesses, thus ensuring "*that information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken*".

3.1.1. ISO/IEC 27015:2012 Information technology - Security techniques – Information security management guidelines for financial services

Continuous developments in the information technology have led to an increased reliance by organizations providing financial services on their assets processing information.

Consequently, management, customers and regulators have heightened expectations regarding an effective information security protection of these assets and of processed information.

Whereas ISO/IEC 27001:2005 and ISO/IEC 27002:2005 address information security management and controls, they do so in a generalized form. Organizations providing financial services have specific information security needs and constraints within their respective organization or while performing financial transactions with business partners, which require a high level of reliance between involved stakeholders.

ISO/IEC 27015:2012 is a technical report which is intended, as a supplement of the ISO/IEC 270xx family of International Standards, to be used by organizations providing financial services. In particular, the guidance contained in this technical report complements and is in addition to information security controls defined in ISO/IEC 27002:2005.

3.1.2. ISO/IEC 27033 - Information technology — Security techniques — Network security

ISO/IEC 27033 aims to provide guidance on the management, operation and use of information system networks, and their inter-connections from a security perspective. In particular, it provides advice on implementing the network security controls of ISO/IEC 27002. It includes an overview of network security and related definitions, as well as advice on identifying and analyzing network security risks and then define network security requirements. It also provides guidance on how to develop good quality technical security architectures. This standard is applicable to the security of networked devices and the management of their security, network applications/services and users of the network. This is additional to the security of information that is being transferred and is more relevant to network security architects, designers, managers and officers.

3.1.3. ISO27034 - Information technology — Security techniques — Application security

ISO/IEC 27034 is relevant to information security with respect to the design and development or procurement, implementation and use of application systems. In particular, it provides guidance on specifying, designing/selecting and implementing information security controls. This includes all aspects including the identification of information security requirements, protection of information accessed by an application and prevention of unauthorized use and/or actions of an application. The standard complements other systems development standards and methods without conflicting with them. Guidance provided in this standard is more relevant to business and IT managers, developers and auditors, and end-users. Its objectives is to ensure that computer applications deliver the desired or necessary level of security in support of the organization's Information Security Management System and addressing security risks arising.

3.1.4. ISO/IEC 27038 - Information technology — Security techniques — Specification for digital redaction

The standard is relevant to removal of confidential (or sensitive in general) content from documents as well as indicating the location in the document where content was removed. In other words, this standard regards redaction, defined as the "permanent removal of information within a document". It specifies, redaction requirements and describes the process for redaction, reflects on techniques for conducting digital redaction on documents as well as defines the requirements for tools in charge of testing that digital reduction was successfully and securely done. It also provides guidance on keeping records so as to justify or explain redaction decisions. Although the standard regards information redaction, it does not encapsulate database redaction.

3.1.5. ISO/IEC 27041 - Information technology — Security techniques — Guidance on assuring suitability and adequacy of incident investigative methods

ISO/IEC 27041 is relevant to the mechanisms employed to ensure the adequacy of the methods and processes followed to investigate Information Security Incidents. The standard provides guidance on best practices with respect to the elicitation analysis of functional and non-functional requirements relating to an Information Security (IS) incident investigation, provide guidance and describe the use of validation means to indicate the suitability of processes involved in the investigation. It also aims at the delivery of evidence that implementations of methods meet the requirements and guide the assessment the levels of validation required and also provide advice on incorporating how to external testing and documentation in the validation process. It also reflects on vendor and third-parties with respect to the testing approaches that can be employed to assist this assurance process.

3.1.6. ISO/IEC 27042 - Information technology — Security techniques — Guidelines for the analysis and interpretation of digital evidence

This standard emphasizes on the forensics process. It particular, it focuses on providing guidance on the process of analyzing and also interpreting digital evidence. It includes insights on how evidential

controls such as the maintenance of chain of custody or scrupulous documentation is managed. Additionally, it focuses on analytical and interpretational processes so as to ensure their integrity in case different investigators are working on the same digital evidence. It also provides guidance on the selection and use of forensic tools, plus proficiency and competency of the investigators.

3.1.7. ISO/IEC 27043 - Information technology — Security techniques — Incident investigation principles and processes

ISO/IEC 27043 provides guidance on idealized models with respect to common incident investigation processes. It reflects on the processes followed for investigating various incident scenarios involving digital evidence. It captures the processes from pre-incident preparation to providing returning evidence in order for it to be stored and disseminated. It also provides dissemination as well as any general advice and caveats on such processes. It provides an overview of all incident investigation principles that could be applicable to various kinds of investigations, however, it does not focus on proscribing particular details to specific categories or groups of incident.

3.2. Directive on security of network and information systems (NIS Directive)

The Directive on security of network and information systems (NIS Directive [16]), provides legal measures to boost cyber-security in the EU. The directive requires Operators of Essential Services (OESs) to implement appropriate and proportionate security measures to achieve the outcomes set out by the NIS principles and notify the relevant national authorities of serious incidents and events [17].

The NIS Directive is the first EU-wide legislation on cyber-security. It aims to achieve harmonization of the levels of protection of the Network and Information Services (the internet as a whole).

The NIS Directive needs to be transposed into national legislation by 9 May, 2018. The deadline for the identification of operators of essential services by 9 November, 2018, i.e. 21 months after the deadline.

Scope. Financial services and financial market infrastructure providers (including trading venues and central counterparties) are included in the scope of the new NIS Directive — in Article 3, they are specifically defined as "Operators of Essential Services" (OES). OES are private businesses or public entities with an important role for the society and economy. According to NIS, the entities have several obligations in case of a cyber-attack. The OES have to take appropriate and proportionate technical and organizational measures to manage the risks posed to the security of networks and information systems that they use in their operations (according to Article 14). They need to prevent and minimize the impact of cyber incidents. Serious incidents need to be notified to the relevant national authority (i.e. Computer Security Incident Response Teams) that each EU country will need to set up. An incident can be classified as "significant" depending on the number of people affected by it, the duration of the incident, and the geographical spread (for example, whether the incident affects services in several branches of a bank). The final text places a great deal of responsibility on the essential services providers. For example, even if a financial services company has outsourced the cloud computing services to a third party, the delegating entity still holds the main responsibility of any cyber attack data breach.

It is understood in NIS that harmonization in the banking sector has been achieved. According to the statutory statements of the directive, "*Regulation and supervision in the sectors of banking and financial market infrastructures is highly harmonized at Union level, through the use of primary and secondary Union law and standards developed together with the European supervisory authorities*". It is understood that "*Within the banking union, the application and the supervision of those requirements are ensured by the single supervisory mechanism*" and thus the requirements of NIS have been mostly reached or even exceeded by the banking and financial infrastructure.

Impact on banking and financial services. The approach towards the banking sector considers the particularities of the business environment. The notification about incidents in the banking sector is indicated to be specified by member states: "*requirements for notification of incidents are part of normal supervisory practice in the financial sector and are often included in supervisory manuals. Member States should consider those rules and requirements in their application of lex specialis*". Furthermore, as noted by the European Central Bank in its opinion of 25 July 2014 [18], "*this Directive does not affect the regime under Union law for the Eurosystem's oversight of payment and settlement systems. It would be appropriate for the authorities responsible for such oversight to exchange experiences on matters concerning security of network and information systems with the competent authorities under this Directive*".

3.3. NIST Cybersecurity framework

In the US, the National Institute of Standards and Technology (NIST) released in 2018 the version 1.1 of the "Framework for Improving Critical Infrastructure Cybersecurity", commonly referred to as the "Cybersecurity Framework" [19]. The version 1.1 refines, clarifies, and enhances Version 1.0, which was issued in February 2014.

The NIST Cybersecurity Framework provides a common language and mechanism for organizations to describe current cybersecurity posture; describe their target state for cybersecurity; identify and prioritize opportunities for improvement within the context of risk management; assess progress toward the target state; foster communications among internal and external stakeholders. 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 Implementation Tiers, and the Framework Profiles. The Framework Core is a set of cybersecurity activities, outcomes, and informative references that are common across sectors and critical infrastructure. Elements of the Core provide detailed guidance for developing individual organizational Profiles. Through use of Profiles, the Framework will help an organization to align and prioritize its cybersecurity activities with its business/mission 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, which will help in prioritizing and achieving cybersecurity objectives.

Scope. The framework addresses the needs of industries that are important to the national and economic security, including energy, financial services and communications. Although it originates from the US and is not a mandatory requirement for European organizations, corporations, organizations and countries around the world, including Italy [20] and Israel [21], have built on the NIST framework. It has proven flexible enough to be adopted by large and small companies and organizations across all industry sectors.

Impact on banking and financial services. The version 1.1 has significant correlation to FINSEC goals and objectives as (among others) it contains greatly expanded explanation of using Framework for Cyber Supply Chain Risk Management purposes. In the most advanced level, the Tier 4 ("Adaptive"), the organization is expected to consider the External Participation; it understands its role, dependencies, and dependents in the larger ecosystem and contributes to the community's broader understanding of risks. It receives, generates, and reviews prioritized information that informs continuous analysis of its risks as the threat and technology landscapes evolve. According to NIST, The organization shares that information internally and externally with other collaborators. The organization uses real-time or near real-time information to understand and consistently act upon cyber supply chain risks associated with the products and services it provides and that it uses.

4. General purpose regulations & standards

4.1. EU Privacy Rules – GDPR

The General Data Protection Regulation (GDPR) 2016/679 of the European Parliament and of the European Council, finalized on the 27th April 2016 was put in full effect on the 25th of May 2018. This Regulation was designed in order to adapt the existing data protection legislation with respect to the way in which data is currently being used in the digital setting. The objective of the Regulation is to empower EU citizens by making them aware of the kind of data held by institutions and the rights of the individual to protect their personal information. In this way it provides additional control to EU residents on over how their personal information is accessed, communicated and stored. All organisations must ensure compliance by 25th May 2018. Failure to comply with the GDPR principles will incur significant penalties for the institution. This will be discretionary and, depending on the nature of the breach, it will range between 2% and 4% of its worldwide revenue, with upper limits of Euros 10m and Euros 20m.

Scope of the regulation. This regulation will be extremely useful in protecting EU citizens and making them feel more secure on their data, and in creating a simpler and clearer legal environment for companies to operate in it. However, GDPR prompts serious consequences for companies. As GDPR standardises data privacy laws and mechanisms across industries, regardless of the nature or type of operations, financial institutions are equally affected by this Regulation. Given that financial organizations collect large amounts of customer data which are used in a variety of processes and activities, such data may easily be collated. Such processes may include client or customer on boarding, relationship management, trade-booking, and accounting. In these processes customer data is exposed to different people, at different stages, and hence GDPR needs to be applied in any of the processes that requires the handling of any type of customer data.

Impact on banking and financial services. Overall, GDPR impacts significantly the financial institutions, especially with respect to the collection of customer information. Institutions need to demonstrate the integrity and validity of their customer's consent with respect to how their data is shared and used for marketing and commercial purposes. They also need to inform customers on how they plan to process and use the data. Additionally, each institution needs to appoint a Data Protection Officer (DPO).

The rest of this subsection outlines the areas of the GDPR that are relevant to the financial services domain.

- **Data subject consent:** GDPR ensures that customers retain the rights over their own data. This concerns personal data and mandates firms to gain customer consent from their customers about the personal data that is gathered, such that customers are aware of what information organisations are holding. This data might be related but not limited to anything that could be used to identify an individual (or to keep them anonymous via pseudonymisation as defined by GDPR but deduce their core propensities to invest, to vote and other personal characteristics), e.g. including as data sources their neighbours, colleagues and friends), as well as their GDPR-related data such as name, email address, IP address, social media profiles or social security numbers. Firms are obliged to provide a clear outline of the purpose for which the data is being collected and gain additional customer consent especially for the case that the firm wants to share some of the customer information with third-parties.
- **Right to data erasure and right to be forgotten:** Beyond the right to data privacy, GDPR, under the terms, also allows Data Portability. Data Portability implies that individuals can request access to, or the removal of, their own personal data from financial institutions. Financial institutions may keep some data to ensure compliance with other regulations, but in all other circumstances where there is no valid justification, the individual's right to be forgotten applies.

- **Minimizing the possibility of a breach:** The DPO must report a data breach to the supervisory authority of personal data within 72 hours. The information to be communicated by the D P O includes details on the nature of the breach, the categories and approximate number of individuals impacted, and contact information of the DPO. As soon as the possible outcomes of the breach become clear, the company is required to inform impacted customers 'without undue delays' (if needed). Penalties in cases of serious violations such as failing to gain consent to process data or a breach of privacy by design, could be up to €20 million, or 4 per cent of the company's global turnover (whichever is greater). Lesser violations, such as records not being kept in order or failure to notify the supervisory authorities, will incur fines of 2 per cent of global turnover. Hence, financial organisations need to ensure that there is an adequate level of security with respect to the risk. Firms need to act with consciousness, diligence and proactive attitude towards data processing and apply the necessary security measures.
- **Vendor management:** GDPR is a regulation that relates to the personal data of clients. Hence, it is essential for firms to understand all their data flows across their various systems. Given the wide deployment of outsourcing development and support functions, firms need to ensure that personal client data is not accessible to external vendors, thus significantly increasing the data's net exposure. According to GDPR, vendors cannot disassociate themselves from obligations towards data access. Additionally, it is essential for Non-EU organisations that collaborate with EU banks or serving EU citizens, to ensure vigilance while sharing data across borders. GDPR in effect imposes end-to-end accountability to ensure client data stays well protected by enforcing not only the bank, but all its support functions to embrace compliance.
- **Privacy by design**: Under GDPR (Article 25, Recital 78) controllers should embed privacy features and functionalities into products, systems from the time that are first designed throughout all the processing operation. It suggests that appropriate measures can be applied such as minimizing the collected data, pseudonymisation techniques (replacing personally identifiable material with artificial identifies) and improved security features, like encryption (encoding messages so only those authorized can read them).
- **Pseudonymisation:** GDPR applies to all potential client data wherever it is found, whether it's in a live production environment, during the development process or in the middle of a testing programme. It is quite common to mask data across non-production environments to hide sensitive client data. Under GDPR, data must also be pseudonymised into artificial identifiers in the live production environment. These data-masking or pseudonymisation rules, aim to ensure the data access stays within the realms of the 'need-to-know' obligations.
- **Impact assessment:** Another new obligation established by the GDPR is to carry out an impact assessment (Privacy Impact Assessment - PIA) for organizations that perform data processing that may involve a high risk for the rights and freedoms of natural persons. The origin, nature, particularity and severity of such risk must be assessed (Recital 84 of the GDPR).
- **Data Protection Officer (DPO)**: GDPR requires that a responsible individual is identified as the Data Protection Officer within each organisation. The DPO is expected to be the company's advisor on Data Protection and they should be competent in the matters of coordination and control of compliance with data protection regulations. Although not mandatory in all organizations, this role is considered as necessary for public firms, firms that have large-scale processing or firms that collect particularly sensitive data or data related to convictions or criminal offenses. A dedicated DPO is required for large organisations with more than 250 employees. Beyond the main duties of the D P O, this role also encapsulates several additional functions including: monitoring the implementation and application of internal policies, training staff with respect to GDPR, organizing and coordinating audits, managing the data subjects' data and the requests presented in the exercise of their rights, ensuring the conservation of documentation, supervising the execution of the impact evaluation and acting as point of contact for the supervisory authority.
- **Biometrics as identifiers for financial transactions***:* Financial services may consider the use of biometrics, such as for example fingerprints and eye scans to identify their customers. In this

respect, beyond obtaining the explicit consent for the use of biometric data of their customers, financial institutions are also required to have controls in place that protect them. Such controls will ensure that data controllers take the necessary technical and organisational measures to prevent this special data from being exposed, as a consequence their systems being poorly managed.

4.2. US Privacy Rules - Gramm-Leach-Bliley Act

Gramm-Leac-Bliley (GLB) Act refers to the corresponding U.S. regulatory framework with respect to customer data protection in the financial sector.

Scope of the Act. The Gramm-Leach-Bliley (GLB) Act [22] requires financial institutions to provide information to their customers regarding their information-sharing practices as well as to safeguard sensitive data. In particular, the GLB Act requires financial institutions to take measures such that customer information is safeguarded. This is implemented by deriving a written information security plan that describes the company's plan to protect customer information. The plan is based on the company's size and complexity, the nature and scope of its activities, and the sensitivity of the customer information it handles. As part of its plan, each company needs to identify employees that are coordinating this information security program, identify and assess the risk to customer information in each operation of the company and evaluate the effectiveness of current safeguard measures, design and implement a safeguards program, select service providers that can maintain appropriate safeguards, evaluate and adjust the program in light of relevant circumstances, including changes in the firm's business or operations, or the results of security testing and monitoring.

Impact on financial institutions. The GLB Act does not have a direct impact on the FINSEC project, as the latter is implemented in the European regional area, where the GDPR regulation is applicable. However, the GLB Act has been included in this deliverable as the Act is explicitly addressing financial institutions and therefore provides additional support for the sections of the GDPR that have been identified as relevant to FINSEC in the previous section.

4.3. e-Privacy

e-Privacy [23] regards a proposal for regulation concerning the respect for private life and protection of personal data in electronic communications. This proposal repeals Directive 2002/58/EC (Regulation on Privacy and Electronic Communications, e-Privacy directive). The e-Privacy directive will come into force towards the end of 2018 or the beginning of 2019.

Scope of the Regulation. The provisions included in this proposal particularise and complement the GDPR by identifying certain rules for the rights of natural and legal persons on electronic communication. In particular, the e-Privacy proposal (finalized in March 2017) identifies the rules regarding the protection of fundamental rights and freedoms of natural and legal persons with respect to the use of electronic communications services. It regards the rights of natural and legal persons for respect on private life and communications and the protection of natural persons with regard to the processing of personal data. The proposal also encapsulates the free movement of electronic communications data and electronic communications services within the EU territory.

The proposal defines electronic communications data in a broad and technology neutral way such that it includes any information concerning the content transmitted or exchanged (electronic communications content) and the information concerning an end-user of electronic communications services processed for the purposes of transmitting, distributing or enabling the exchange of electronic communications content.

This also includes data to trace and identify the source and destination of a communication, geographical location and the date, time, duration and the type of communication. As the content of

electronic communications may reveal highly sensitive information about the natural persons involved in the communication, from personal experiences and emotions to medical conditions, sexual preferences and political views, the disclosure of which could result in personal and social harm, economic loss or embarrassment, e-Privacy aims to provide additional provisions for natural and legal persons.

Similarly, e-Privacy is also relevant to any metadata derived from electronic communications may also reveal very sensitive and personal information. These metadata may include the numbers called, the websites visited, geographical location, the time, date and duration when an individual made a call etc., allowing precise conclusions to be drawn regarding the private lives of the persons involved in the electronic communication.

Additionally e-Privacy also aims to provide protection for electronic communication data that may also reveal information concerning legal entities, such as business secrets or other sensitive information that has economic value, and thus the provisions of this Regulation apply to both natural and legal persons.

Overall, the regulation provisions that legal persons have the same rights as end-users that are natural persons regarding e-Privacy. Supervisory authorities in charge of this regulation should also be responsible for monitoring the application of this regulation regarding legal persons.

Impact on financial institutions. The scope of e-Privacy is to particularise and complement the GDPR with respect the entire content of any electronic communication. To this end, e-Privacy will impact the financial services sector with respect to the following [24]:

- Protection of legal persons: All electronic communications exchanged in the financial sector are subject to stricter requirements, especially in the case that they contain personal or confidential data. This translates into additional measures to ensure the protection of such data.
- Protection of electronic communication*:* e-Privacy aims to protect all kinds of data processing within electronic communications. Hence, additional security requirements for the transmission of personal and confidential data through electronic means might need to be developed in the financial sector. Beyond email communication, this might prompt changes in existing processes such as fund transfers (where the data of the payer and payee is transferred between banks) or information exchanges related to regulations such as AEI (Automatic Exchange of Information), FATCA (Foreign Account Tax Compliance Act) or MiFID (Markets in Financial Instruments Directive).
- Protection of terminal equipment information: The e-Privacy also refers to the information related to the terminal equipment of end-users. Hence, financial institutions will have to consider these requirements in applications developed (such as web-banking or mobile banking apps) where data such as transaction details are stored by the user.
- Metadata restrictions: The processing and/or storage of metadata is restricted by e-Privacy and hence this may affect the ability of the financial institutions to use and analyse such data.
- Effects on internal screenings: The regulation will prohibit the processing of electronic communications without prior consent. Hence, internal screenings of e-mails and other electronic files will require the prior consent by any user communicating with the institution.

4.4. eIDAS

eIDAS [25] (electronic IDentification, Authentication and trust Services) is an EU regulation on a set of standards for electronic identification and trust services for electronic transactions in the European Single Market.

Scope of the Regulation. Electronic identification (eID) and electronic Trust Services (eTS) are key enablers for secure cross-border electronic transactions and central building blocks of the Digital Single Market. eIDAS took effect on July 2016. In particular, the eIDAS Regulation aims to ensure that

individuals and businesses can use their own national electronic identification schemes (eIDs) to access public services in other EU member states if the eID schemes are available. Along the same lines, it creates a European internal market for eTS - namely electronic signatures, electronic seals, time stamp, electronic delivery service and website authentication - by ensuring that they will work across borders and have the same legal status as traditional paper based processes. Therefore, these regulations provide certainty on the legal validity of all these services, businesses and citizens that will use the digital interactions as their natural way of interaction. To this end, through eIDAS, it has allowed the EU to provide right foundations and a predictable legal framework for people, companies (in particular SMEs) and public administrations, to safely access services and do transactions online and across border in just "one click". Indeed, the release of eIDAS provides higher security and more convenience for any online activity.

Impact on financial institutions. eIDAS is the last step in the process of converting all paper-based processes to e-processes. In particular it provides the financial sector with [26]:

- Legal effects for qualified electronic signatures, seals, certificates for electronic seals, timestamps and documents, as well as e-signature and e-seal creation devices.
- A legal framework for e-registered delivery services and website authentication services.
- The basis for eID schemes notified under the regulation in one member state to be recognised in one another.
- Security of personal data and breach notification requirements for all trust service providers.
- Supervision for Qualified Trust Service Providers (QTSPs), trusted lists and a trust mark for QTSPs to demonstrate compliance with the regulation.

4.5. Specification for security management systems for the supply chain (ISO 28000:2007)

ISO 28000:2007 specifies the requirements for a security management system, including those aspects critical to the security assurance of the supply chain. Security management is linked to many other aspects of business management. Aspects include all activities controlled or influenced by organizations that impact on supply chain security. These other aspects should be considered directly, where and when they have an impact on security management, including transporting these goods along the supply chain.

The standard was last confirmed in 2014 and still applies today.

Scope of the standard. Security Management is a challenge within supply chains, as the supply chain partners are often located in varying locations worldwide, meaning that they are subject to varying regulations and processes. The benefits associated with complying with the standard include identifying potential threats which originate from outside the organization, control and influence activities that impact on supply chain security and ensure continuity of business. A certified ISO 28000 management system can reduce a company's liability for security incidents.

Impact on banking and financial services. The primary focus and interest of the standard is on the transportation and logistics businesses and not in banking. The standard requires the organization to review and document the processes and procedures and identify the areas that do not meet the standard requirements with regard to the security of the supply chain. Nevertheless, the standard in case it is adopted by a financial organization would primarily indicate the special emphasis placed on identifying threats from the external environment that affect the internal operation of the organization and ensure the continuity of business. FINSEC places specific emphasis on the inter-organization sharing of information about threats and vulnerabilities as a means for collaborative risk assessment. It will implement a supply chain collaboration module that specifically addresses the financial supply chain.

4.6. Business continuity management systems (ISO 22301:2012)

Business continuity is the planning and preparation of a company to cope with serious incidents or disasters and resume its normal operations within a reasonably short period. It is deemed nowadays the essential complementary stage to an integrated risk management approach. Business Continuity Management (BCM) includes the following three key elements:

- Resilience, i.e. the design of critical business functions and of the supporting infrastructure that makes sure that they are not affected by disruptions; for example through the use of redundancy and spare capacity;
- Recovery, i.e. the arrangements planned to recover or restore critical and less critical business functions that have failed; and
- Contingency, i.e. the readiness to cope effectively with whatever major incidents and disasters occur, including those that were not, and perhaps could not have been, foreseen. Contingency preparations constitute a last-resort response if resilience and recovery arrangements should prove inadequate in practice.

The ISO 22301:2012 standard sets out the requirements for a best-practice business continuity management system (BCMS). A BCMS is by itself a comprehensive approach to organisational resilience and helps organisations cope with incidents that affect their business-critical processes and activities. It provides a structure for organisations to update, control and deploy effective plans, taking into account organisational contingencies and capabilities, as well as business needs.

The ISO22301:2012 standard specifies requirements to plan, establish, implement, operate, monitor, review, maintain and continually improve a documented management system to protect against, reduce the likelihood of occurrence, prepare for, respond to, and recover from disruptive incidents when they arise.

While ISO 22301 may be used for certification and therefore includes rather short and concise requirements describing the central elements of BCM, a more extensive guidance standard (ISO 22313) is being developed to provide greater detail on each requirement in ISO 22301 [27].

Scope of the standard. The requirements specified in ISO 22301:2012 are generic and intend to be applicable to all organizations, or parts thereof, regardless of their nature. The extent of application of these requirements depends on the organization's operating environment and complexity. Those businesses that recognize their dependence on each other and seek assurance that their key suppliers and partners continue to operate and provide their products and services, even when incidents occur, seem to be the ones that pursue certification.

Impact on Banking and Financial Services. The adoption of the standard is not universal in the finance and banking sector. However, given the advent of new directives such as the EU General Data Protection Regulation (GDPR) and the NIS Directive, ISO 22301, compliance is recommended as a useful tool for implementing a well-defined incident response and reporting structure, so organisations can demonstrate they are taking steps to comply with regulatory requirements. Thus we expect that the standard will increasingly be adopted by the financial sector and lead to the development of service models that adhere to its principles by adopting best practices fault-tolerance and resilience.

5. Impact of regulations and standards on FINSEC pilots

A review of the compliance requirements for each of the use cases in FINSEC is presented.

5.1. Protection from Cyber and Physical Attacks on ATMs

The combined Cyber and Physical (hosted by partner WIRE) pilot use cases are mainly to evaluate, the FINSEC solution, based on Logical-Cyber and combined Physical and Cyber-attacks for ATM network in electronic payment domain. The pilot process is affected by the aforementioned regulations and laws as GDPR, BNR (National Bank of Romania) regulations, PCI DSS, PCI PA-DSS and ISO 27001.

According to the GDPR, retrieved logs and events in the ATM should be either anonymized or pseudonymized and also the CCTV camera recordings should have a retention policy, to keep the data for a certain period and not associate with the physical persons, but in the pilot in Romania there is an additional law to regulate the physical security in financial organizations that permits and/also mandates to video recording the area that the ATM located.

The PCI-DSS and/or PCI PA-DSS directives, provide recommendations on the security of sensitive data that are enclosed with the Card number (PAN), Expiry data, Service code, Card verification Values (Cvv, Cvv2, iCvv) and Pin (password) for the Card. Within the financial domain, especially for the electronic payments, the solutions and/or the systems should not keep the sensitive data in file logs and/or in Databases if they are not encrypted. So, the FINSEC solution should not make such types of data retrievable from the ATM. The PCI-DSS directives are more related with the organizations and eco-systems, to mandate the procedures and preventive actions to process the sensitive data. The FINSEC operations' centre should also comply with this. Furthermore, the PCI PA-DSS, is dealing with the solution itself, the solutions should be certified by the PCI, if it is accessing to the payment data.

The IEC/ISO 27001, based on the main criteria of the directive which is the CIA triad (Confidentiality, Integrity and Availability), the project should have the related procedures for "Classifying collected data in terms of their value, sensitivity and criticality" and the rights for accessing and using/modifying the data. Specifically, the defined security basis should not interfere with the availability of the ATMs which is crucial.

5.2. Protection from Cyber and Physical Attacks on the hosting infrastructure

The main impact of regulation on the protection from Cyber and Physical Attacks may be focused on the GDPR using the following principles:

- limitation of data retention, in this case for the storage of CCTV recordings that for example in Italy is defined with a time period of 7 days ("Provvedimento in materia di videosorveglianza - 8 aprile 2010") only for cases where the data controller, such as NEXI, perform particularly risky activities (e.g. banking);
- the existence of appropriate safeguards, which may include encryption or pseudonymisation of data to guarantee the lawfulness of processing and protection of personal data;
- privacy by design/by default that require to implement appropriate technical and organisational measures which are designed to implement data-protection principles in an effective manner and to integrate the necessary safeguards into the processing. It requires also implementing appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed.

5.3. Protection of payments' infrastructure

The NEXI pilot is focused on the correlation of physical and logical security events related to an environment that hosts the ACS 3DS service.

The 3-D Secure is an authentication protocol designed by Visa (Verified by Visa) and Mastercard (Mastercard SecureCode) that enables the secure processing of online payment through credit card transactions. NEXI, as an issuer, offers such a service to its customers.

Such a service is subject to the following regulations and related requirements imposed by the PCI standards:

- Payment Card Industry Data Security Standard (PCI DSS) - Requirement 9, Restrict physical access to cardholder data;
- Payment Card Industry 3-D Secure (PCI 3DS) - Requirements:
  - P2-4.2 (Secure internal network connections)
  - P2-4.4 (Restrict wireless Exposure)
  - P2-6.2 (Secure logical access to HSMs)
  - P2-6.3 (Secure physical access to HSMs)
  - P2-7.1 (Data Center Security)
  - P2-7.2 (CCTV)

Furthermore, NEXI use cases require the acquisition and processing of Personally Identifiable Information (PII), that are subject to the following regulation:

- General Data Protection Regulation (GDPR) 2016/679:
  - storage limitation;
  - the existence of appropriate safeguards, which may include encryption or pseudonymisation; and
  - privacy by design/by default

5.3.1. Payment Card Industry Data Security Standard (PCI DSS)

The requirement #9 ("Restrict physical access to cardholder data") of the PCI DSS establish that any physical access to data or systems that house cardholder data provides the opportunity for persons to access and/or remove devices, data, systems or hardcopies, and should be appropriately restricted. In order to meet this requirement it is necessary to:

- use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment;
- develop procedures to easily distinguish between onsite personnel and visitors, especially in areas where cardholder data is accessible;
- ensure all visitors are authorized before entering areas where cardholder data is processed or maintained; given a physical token that expires and that identifies visitors as not onsite personnel; and are asked to surrender the physical token before leaving the facility or at the date of expiration;
- use a visitor log to maintain a physical audit trail of visitor information and activity, including visitor name and company, and the onsite personnel authorizing physical access. Retain the log for at least three months unless otherwise restricted by law;
- store media back-ups in a secure location, preferably off site;
- physically secure all media;
- maintain strict control over the internal or external distribution of any kind of media. Classify media so the sensitivity of the data can be determined;
- ensure that management approves any and all media moved from a secured area, especially when media is distributed to individuals;

- maintain strict control over the storage and accessibility of media; and
- destroy media when it is no longer needed for business or legal reasons.

5.3.2. Payment Card Industry 3-D Secure (PCI 3DS)

In order to guarantee logical and physical security, the applicable requirements of PCI 3DS are:

The P2-4.2 (Secure internal network connections), applying a multi-factor authentication for all personnel with non-console access to ACS, DS, and 3DSS;

The P2-4.4 (Restrict wireless Exposure), prohibiting the use or the connection of the 3DS components to any wireless network;

The P2-6.2 (Secure logical access to HSMs) establishes that:

- Personnel with logical access to HSMs must be either at the HSM console or using an HSM non-console access solution that has been evaluated by an independent laboratory to comply with the sections of the current version of the standards for the security characteristics for secure cryptographic devices;
- All non-console access to HSMs originates from a 3DE network(s);
- Devices used to provide personnel with non-console access to HSMs are secured as follows:
  - Located in a designated secure area or room that is monitored at all times;
  - Locked in room/rack/cabinet/ drawer/safe when not in use;
  - Physical access is restricted to authorized personnel and managed under dual control;
  - Authentication mechanisms (e.g., smart cards, dongles, etc.) for devices with non-console access are physically secured when not in use;
  - Operation of the device requires dual control and multi-factor authentication;
  - Devices have only applications and software installed that are necessary;
  - Devices are verified as having up-to-date security configurations;
  - Devices cannot be connected to other networks while connected to the HSM; and
  - Devices are cryptographically authenticated prior to the connection being granted access to HSM functions.
- The loading and exporting of clear-text cryptographic keys, key components, and/or key shares to/from the HSM is not permitted over a non-console connection;
- Activities performed via non-console access adhere to all other HSM and key-management requirements.

The P2-6.3 (Secure physical access to HSMs) establishes that:

- HSMs are stored in a dedicated area(s);
- Physical access to the HSMs is restricted to authorized personnel and managed under dual control.

The P2-7.1 (Data Center Security) establishes that:

- ACS and DS systems are hosted in data center environments;
- Data centers supporting ACS and DS are equipped with a positively controlled single-entry portal, that requires positive authentication prior to granting entry and grants entry to a single person for each positive authentication;
- Doors to areas within the data center that contain 3DS systems are fitted with an electronic access-control system (e.g., card reader, biometric scanner) that controls and records all entry and exit activities;
- Multi-factor authentication is required for entry to telecommunications rooms that are not located within a secure data center;
- Entry controls prevent piggy-backing by granting access to a single person at a time, with each person being identified and authenticated before access is granted;

- A physical intrusion-detection system that is connected to the alarm system is in place; and
- Physical connection points leading into the 3DE are controlled at all times.

The P2-7.2 (CCTV) establishes that:

- CCTV cameras are located at all entrances and emergency exit points and capture identifiable images, at all times of the day and night;
- CCTV recordings are time stamped.

5.4. P2P Payments Infrastructure

As a payments solution, Peer-to-Peer payment needs to comply with these laws and regulations:

- EU Central Bank and relevant National surveillance directives for payments and digital currency institutions;
- EU GDPR and applicable National laws on personal data protection;
- EU PSD2 (including EBA RTS) is of course to be considered, particularly for guidance on security and interoperability aspects, albeit some do not apply or are already satisfied in a Peer-to-Peer blockchain scenario due to end-users accessing the solution directly using Commercial Banks only as intermediaries;
- AMLD4 (Anti Money Laundering) laws, regulations and directives are obviously relevant in a Peer-to-Peer payment scenario because potential anonymity and lack of end-to-end transaction visibility must be overcome with additional provisions, still preserving the advantages of such a functional model.

5.5. Implementing Security-as-a- Service (SECaaS)

5.5.1. The case of an assets trading organization based in Germany (JRC)

The SECaaS pilot addresses regulated SMEs in the financial sector. A range of international and national laws, directives and regulations have to be complied with and their impact on the pilot will be considered here. The partner JRC is regulated by the German financial supervisory authority BaFin. Therefore, the focus of these considerations will lie on the German legislation and regulation that interprets the European regulation for financial institutes. BaFin recognises that in a globalised financial world IT governance and information security have gained the same high significance as capitalisation and liquidity of the supervised organisations. Therefore, they have published a document, BAIT (Bankaufsichtliche Anforderungen an die IT = Supervisory Requirements for IT in Financial Institutions), that since Nov. 2017 represents the central building block for the German banking and financial services sector with respect to IT and security.

Table 1 - Nine modules of the BAIT and impact to the FINSEC SECaaS pilot

Topic	Provision	Recommendation	Main impacts
IT strategy	Secure and appropriate organization of IT systems and processes	Scope and quality of IT systems and processes have to be geared to the company's internal requirements, business activities and risk situation.	The pilot shall be adaptable and scalable to different levels of requirements, business activities and risk situations.
IT governance	In order to allow control of operation and further development of IT systems, quantitative and qualitative criteria have to be defined and monitored.	Possible criteria are: (a) quality of service / service level, (b) availability, (c) maintainability, (d) adaptability to new requirements, (e) security of IT systems and processes, (f) costs	The pilot shall provide a performance measurement system and collect statistics about measurements.
Information Risk Management	The institute has to define and coordinate the related tasks, competences, responsibilities, control and communication channels.	Establish appropriate monitoring and control processes and define reporting commitments.	The pilot has to implement appropriate monitoring and control processes and support the defined reporting.
	The institute has to have an up-to-date overview over all elements of the given information network, its dependencies and interfaces.	The information network comprises all business relevant information, business processes, IT-systems as well as network and building infrastructure.	The pilot shall support the (automatic) documentation of active components of the information network.
	The method for the determination of protection requirements (i.e. for the protection targets, integrity, availability, authenticity and privacy of data) has to allow for a consistent comparison with actually measured protection levels.	The definition of requirements may use categories as e.g. 'low', 'medium', 'high' and 'very high'.	The pilot shall provide measures for protection levels for the protection targets - integrity, - availability, - authenticity and - privacy of data
Information security management	In case of an information security incident potential impacts on information security have to be analysed and appropriate follow-up measures have to be initiated.	The term "information security incident" has to be defined, in particular discriminating from "operational incidents". This may also include the breach of at least one of the protection targets (availability, integrity, privacy, authenticity), if a defined threshold is exceeded.	The pilot shall support the detection and analysis of information security incidents.

	Quarterly and event driven reporting to the management about the information security status.	Assessment of the information security situation with respect to the previous report, incidents as well as penetration test results.	The pilot shall support the documentation and reporting of information security incidents and penetration test results.
User authorisation management	Authorisation concepts that determine scope and conditions of user authorisation shall be consistent with the specified protection needs. They have to follow the “need-to-know” principle, protect the separation of user functions and avoid conflicts of interest for the staff.	Possible terms of use are time limits or personalisation of granted authorisations.	The pilot shall allow limitation of user authorisation in time and personalised access rights.
	Non-personalised access rights (like “admin”) have to be attributable to a person (preferably automated) any time.	Activities of non-personalised or technical users have to be attributable to natural persons.	The pilot shall link user names / IDs with natural persons.
	Assignment, change, deactivation and deletion of access rights and the recertification have to be documented traceably and analysable.		The pilot shall provide traceable and analysable documentation about assignment, change, deactivation and deletion of access rights.
	Accompanying technical and organisational measures have to prevent the circumvention of the requirements of the authorisation concept.	technical and organisational measures are e.g.: - selection of appropriate authentication procedures - implementation of a guideline for secure passwords - automated password protected screen saver - data encryption - tamper proof implementation logging - measures for the sensitisation of staff	The pilot shall implement as many of the listed measures as possible.
IT projects, application development	All substantial changes in the IT systems of the institute have to be evaluated by an impact study. Risks with respect to duration, resource consumption and quality of IT projects have to be considered appropriately.	Standardised templates may be used for risk analysis in order to ensure a uniform approach and sufficient informative value of the results.	The pilot may assist in risk analysis.

	The portfolio of IT projects has to be appropriately monitored and controlled. It has to be considered that dependencies of different projects may raise additional risks.	The view as a portfolio enables an overview of IT projects with the corresponding project data, resources, risks and dependencies.	The pilot shall provide an electronically evaluable overview of all projects, their data, resources, risks and dependencies.
	As part of application development adequate precautions have to be taken with respect to securing privacy, integrity, availability and authenticity of the processed data after production roll-out.	Adequate precautions may be: - input data validation - system access control - user authentication - transaction authorisation - logging of system activities - audit logs - tracing of security relevant events - exception handling	The pilot shall implement as many of the listed elements as possible.
	As part of application development precautions have to be taken that allow to identify, whether an application was changed inadvertently or manipulated by purpose.	An appropriate precautionary measure, taking into account protection requirements, could be the revision of source code.	The pilot shall be able to block suspicious applications. It should be able to archive and protect tested and released versions against changes.
	Applications and their development have to be documented clearly and comprehensibly.	The documentation of applications comprises at least the following content: - user documentation - technical system documentation - operation manual Versioning of source code and documents supports traceability.	The pilot shall support documentation of applications.
	A test methodology for applications has to be defined and introduced. Test activities and results have to be documented.	Test documentation shall at least cover the following topics: - description of test cases - parametrisation of test cases - test data - expected test results - achieved test results - deduced measures	The pilot may support test documentation by monitoring system behaviour during tests and collecting performance data.

	After production roll-out potential deviations from normal operation have to be monitored, causes examined and eventually rectification measures have to be initiated.	An accumulation of incidents can e.g. be an indication for deficiencies.	The pilot shall assist in operation monitoring, logging of incidents and in the detection of deviation sources and provide basic incident management functionality.
	Guidelines for the identification, documentation, test- and development, protection needs and access rectification process for all applications developed and used by end users have to be managed.	For keeping the overview and avoiding redundancies, a central register of such applications has to contain at least the following information: - name and purpose of the application - version, data - external or internal development - technically responsible person - technology Result of the risk classification /protection need classification and derived protection measures.	The pilot shall support the registration of new or unknown applications.
IT operation (incl. Data backup)	Every change request of IT systems has to be documented and evaluated with respect to implementation risks.	Risk analysis shall include existing IT systems (in particular the network and upstream and downstream IT systems) also with respect to potential security- or compatibility problems.	The pilot may assist in risk analysis (potentially in form of a data base of known security- and incompatibility problems)
	Every change request of IT systems has to be securely implemented.	Changes have to be tested for potential incompatibilities and potential security critical issues before production roll-out. Patches have to be tested considering their criticality (e.g. security- or contingency patches).	This concerns the SECaaS pilot itself in its deployment as an additional IT system. The pilot may also assist in testing and test documentation.
		Data backups of concerned IT-systems have to be carried out.	The pilot may control and document, that all necessary backups have been carried out.
		Plans for reversal of the changes and return to previous versions have to exist. In addition, alternative recovery options have to exist, in case that the primary plan should fail.	
	Reports in case of unplanned deviations from normal operation (incidents) and their causes		The pilot shall support incidents reporting.

	have to be collected, evaluated and prioritised according to potentially resulting risks. Problem solving steps and processes have to be well documented.		
	A well-regulated process for the analysis of potential correlation of incidents and their causes has to be in place.		The pilot may include a basic incident management system.
Outsourcing and 3rd party IT services procurement	A risk evaluation has to take place in advance. Derived measures have to be considered in the contract with the service provider. Service delivery has to be monitored by the institute according to the risk evaluation results. Risk evaluations have to be reviewed regularly.	Contracts shall contain regulations concerning Information risk management, information security management and contingency planning.	The pilot has to deliver the agreed protection levels.
Critical infrastructures	Ensure the availability, integrity, authenticity and confidentiality of information processing for critical infrastructures. KRITIS operators (and in the case of outsourcing, in addition to their IT service providers) are entitled to take appropriate measures such that they can effectively ensure the safe operation of critical infrastructures.	Take appropriate measures to ensure that the critical infrastructures are designed in the frame of a resilient architecture.	

5.5.2. The case of a Spanish bank (Liberbank)

Partner Liberbank involved in this Pilot, is regulated by the Spanish the national central bank, Banco de España, which transposes the European regulation of European Banking Authority (EBA) to Spain without adding additional considerations.

In relation to the regulations involved, there are two important aspects to consider in this Pilot, i.e. monitoring and response to incidents:

Monitoring. In this sense, all the regulations to comply with in relation with the process of information.

- Importantly, GDPR because it highlights accountability which implies having a record of the activities and knowledge of what is happening in your network. Particularly, monitor the access to system components.
- PCI DSS which impacts the card information handling, on how to handle the monitoring of this information, identifying what is the access to system components and deploying audit systems to link this access to particular users.
- PSD2, which impacts on how you provide an API, monitor what is happening and offers this information to third parties. It must be established and implemented continuous monitoring processes to detect anomalous activities in the provision of payment services. Also, procedures that guarantee the traceability of all payment transactions and other interactions with the user of the payment services and with other entities, in the context of the provision of the payment service.

Special mention to monitor the information described in the "Law on the prevention of money laundering" which requires to comply with the highest level of Organic Law of Protection of Personal Data (LOPD).

Response to incidents. In this sense, all the regulations to comply with in relation with the response to an incident and how and to whom this must be reported. In particular:

- Report to European Central Bank (ECB): which establishes how to evaluate an incident depending on the criteria ECB defines and how to report it.
- PSD2: which establishes that in case of serious security incidents, the payment service providers must notify the competent authority, in this case the EBA, defining a criteria of what is consider a serious security incident and how to report it.
- GDPR: which requires that the Data Protection Officer (DPO) must inform the control authority, in this case the Spanish Agency for Data Protection (AEPD), whenever the incident constitutes a high risk for the rights and freedoms of the people, defining what a high risk is and how to report it.
- Report to VISA: which requires an immediate notification and response to the suspicion or confirmation of the loss, theft or compromise of Visa accounts to maintain the security of cardholder data and avoid financial and reputational damage.
- Report to MasterCard: which requires a rapid identification of an ADC event (Account Data Compromise) that compromises the data of MasterCard card holders to reduce exposure and risk of financial loss.

The research leading to these results has received funding from the European Union's Horizon 2020 Research and Innovation Programme, under grant agreement no 700071.

5.6. Insurance Risk Assessment

The scope of the pilot will cover the underwritings core system and applications which is the most critical and complex framework of the company. The purpose is to build a reference approach (based on FINSEC) about security in the insurance sector.

5.6.1. Mapping between security objectives and compliance requirements

The objectives defined by HDI in the Cybersecurity field and their instantiation within a framework based on what is proposed by NIST (Framework for Improving Critical Infrastructures Cybersecurity) allow HDI to efficiently address the management of Cybersecurity, also ensuring the compliance with the internal and external requirements that HDI must meet, because they derive from applicable industry regulations and / or policies / guidelines defined internally within the Talanx group.

The following are the main internal and external regulations, impacting in the Cybersecurity area, to which HDI must ensure compliance:

- External regulations:
    - European Regulations on the protection of personal data (EU Regulation 2016/679) - GDPR
    - IVASS - Regulation n. 38 IVASS of 3 July 2018;
    - IVASS - Letter to the Market on 29 December 2017.
- Internal regulations:
    - Talanx Group Information Security Policy.

European Regulation on the protection of personal data (EU Regulation 2016/679) – GDPR

In the context of this regulations and standard framework for HDI's Cybersecurity area, the activities related to FINSEC deployment on the Insurance Risk Assessment Pilot have to be compliant with the same rules. Of course, a number of different aspects of the aforementioned regulations have direct impacts on the design and operations of the pilot itself. The following table defines and maps the design and functional requirements for the pilot with the relevant GDPR articles, giving a global overview of how this regulation will drive the personal data management in Task 6.6.

Table 1: Requirements from GDPR for Insurance Risk Assessment Pilot

ID	Requirement	Reference
GDPR_1	Definition of the data retention period	GDPR, Art. 13, subsection 2.a
GDPR_2	Adoption of technological solutions for the protection of the right of access to data.	GDPR, Art. 15
GDPR_3	Adoption of technological solutions for the protection of data correction rights.	GDPR, Art. 16
GDPR_4	Adoption of technological solutions for the protection of data cancellation rights.	GDPR, Art. 17
GDPR_5	Adoption of technological solutions for the protection of the right to limit the treatment.	GDPR, Art. 18
GDPR_6	Adoption of technological solutions for the protection of data portability rights.	GDPR, Art. 20
GDPR_7	Privacy by design e privacy by default	GDPR, Art. 25
GDPR_8	Pseudonymisation and data encryption	GDPR, Art. 32, subsection 1.a
GDPR_9	Security measures to ensure confidentiality, integrity, availability and resilience of systems and services	GDPR, Art. 32, subsection 1.b
GDPR_10	Incident management - Recovery capability	GDPR, Art. 32, subsection 1.c
GDPR_11	Verification and testing of the effectiveness of technical and organizational security measures	GDPR, Art. 32, subsection 1.d
GDPR_12	Definition of security measures based on risk assessments	GDPR, Art. 32, subsection 1.d
GDPR_13	Data Breach Notification	GDPR, Art. 33
GDPR_14	Data protection impact assessments	GDPR, Art. 35

The main Cybersecurity requirements defined by the reference standards are appropriately addressed through the definition of the HDI Cybersecurity objectives, declined within the framework, according to a precise mapping declined by HDI itself and illustrated in this chapter. The following paragraphs summarize the Cybersecurity requirements defined by the reference standards and, for each of these, the diagram illustrating the mapping between these requirements and the HDI Cybersecurity objectives defined within its framework is reported.

Among the provisions introduced by the GDPR, some IT security measures are defined that organizations must implement to ensure the correct protection of the rights of the data subject.

The GDPR requirements with an impact on the Cybersecurity that, therefore, HDI must incorporate within its Cybersecurity framework the requirements summarized in the following table.

The Cybersecurity requirements defined within the GDPR are appropriately addressed by HDI within its framework according to the mapping with the relative objectives shown below.

Table 2: Identified GDPR requirements mapped on HDI's measures

GDPR		Framework Cybersecurity HDI	
ID	**Requirement**	**ID Categ.**	**Category**
GDPR_1	Definition of the data retention period	PR.IP	Information Protection Processes and Procedures
GDPR_2	Adoption of technological solutions for the protection of the right of access to data.	PR.IP	Information Protection Processes and Procedures
GDPR_3	Adoption of technological solutions for the protection of data correction rights.	PR.IP	Information Protection Processes and Procedures
GDPR_4	Adoption of technological solutions for the protection of data correction rights.	PR.IP	Information Protection Processes and Procedures
GDPR_5	Adoption of technological solutions for the protection of the right to limit the treatment.	PR.IP	Information Protection Processes and Procedures
GDPR_6	Adoption of technological solutions for the protection of data portability rights.	PR.IP	Information Protection Processes and Procedures
GDPR_7	Privacy by design e privacy by default	PR.IP	Information Protection Processes and Procedures
GDPR_8	Pseudonymisation and data encryption	PR.DS	Data Security
GDPR_9	Security measures to ensure confidentiality, integrity, availability and resilience of systems and services	PR.DS	Data Security
GDPR_10	Incident management - Recovery capability	RC.RP	Recovery Planning
GDPR_11	Verification and testing of the effectiveness of technical and organizational security measures	ID.GV	Governance
GDPR_12	Definition of security measures based on risk assessments	ID.RA	Risk Assessment
GDPR_12	Definition of security measures based on risk assessments	PR.AC	Identity Management Authentication and Access Control
GDPR_13	Data Breach Notification	RC.CO	Communications
GDPR_14	Data protection impact assessments	ID.AM	Asset Management
GDPR_14	Data protection impact assessments	ID.RA	Risk Assessment

IVASS - Regulation n. 38 IVASS of 3 July 2018

HDI, through the objectives set out within the Cybersecurity framework, intends to satisfy the IT security guidelines dictated by the sector regulations issued by IVASS and, in particular, defined within the art. 16 of Regulation no. 38 of 3 July 2018, which establishes a series of requirements for IT systems and Cybersecurity that italian insurance companies must meet.

Further addresses for the management of information and the prevention of IT risks to insurance companies had already been suggested by IVASS with a Letter to the Market issued on 29 December 2017, within which a series of interventions to insurance companies were suggested to raise the level of data protection. These addresses are also incorporated into the HDI framework.

The Cybersecurity requirements defined and suggested by IVASS in the two documents mentioned above are summarized below.

Table 3: Requirements from IVASS for Insurance Risk Assessment Pilot

ID	Address	Reference
IVASS_1	Definition of the ICT Strategic Plan	IVASS – Regulation n. 38, art. 16, 2.a
IVASS_2	Definition of roles and responsibilities	IVASS – Regulation n. 38, art. 16, 2.b.i
IVASS_3	Evaluation of the ICT security risk	IVASS - Regulation n. 38, art. 16, 2.b.ii
IVASS_4	Systematic monitoring for the identification of security incidents	IVASS - Regulation n. 38, art. 16, 2.b.iii
IVASS_5	Identification of resource vulnerabilities	IVASS - Regulation n. 38, art. 16, 2.b.iii
IVASS_6	Cybersecurity incident management	IVASS - Regulation n. 38, art. 16, 2.b.iv – 2.b.vii
IVASS_7	Access management (IAM)	IVASS - Regolamento n. 38, art. 16, 2.c
IVASS_8	Management of outsourced services	IVASS - Regulation n. 38, art. 16, 2.d
IVASS_9	Hardware and software acquisition	IVASS – Regulation n.38, art. 16, 2.d
IVASS_10	Business continuity management	IVASS - Regulation n. 38, art. 16, 2.e
IVASS_11	Change management (computer systems integration and migration)	IVASS - Regulation n. 38, art. 16, 3
IVASS_12	Communications to IVASS	IVASS - Regulation n. 38, art. 16, 4
IVASS_13	Definition of Cyber Security policy	IVASS – Letter to the Market 29/12/2017
IVASS_14	Semi-annual checks of compliance of company operations with policies	IVASS – Letter to the Market 29/12/2017
IVASS_15	Training	IVASS – Letter to the Market 29/12/2017
IVASS_16	System configuration	IVASS – Letter to the Market 29/12/2017
IVASS_17	Backup management (daily)	IVASS – Letter to the Market 29/12/2017

Through its objectives set within the framework of Cybersecurity, HDI responds to the guidelines dictated and suggested by IVASS according to the mapping summarized in the following table.

Table 4: Identified IVASS requirements mapped on HDI's measures

IVASS		Framework Cybersecurity HDI	
ID	Address	ID Categ.	Category
IVASS_1	Definition of the ICT Strategic Plan	ID.GV	Governance
IVASS_2	Definition of roles and responsibilities	ID.GV	Governance

IVASS		Framework Cybersecurity HDI	
ID	Address	ID Categ.	Category
IVASS_3	Evaluation of the ICT security risk	ID.RA	Risk Assessment
IVASS_4	Systematic monitoring for the identification of security incidents	DE.CM	Security Continuous Monitoring
IVASS_5	Identification of resource vulnerabilities (VA / PT)	DE.CM	Security Continuous Monitoring
IVASS_6	Cybersecurity incident management	RS.RP	Response Planning
IVASS_6	Cybersecurity incident management	RS.CO	Communications
IVASS_6	Cybersecurity incident management	RS.AN	Analysis
IVASS_6	Cybersecurity incident management	RS.MI	Mitigation
IVASS_6	Cybersecurity incident management	RS.IM	Improvements
IVASS_7	Access management (IAM)	PR.AC	Identity Management Authentication and Access Control
IVASS_8	Management of outsourced services	ID.SC	Supply Chain Risk Management
IVASS_9	Hardware and software acquisition	ID.SC	Supply Chain Risk Management
IVASS_10	Business continuity management	PR.IP	Information Protection Processes and Procedures
IVASS_11	Change management (computer systems integration and migration)	PR.IP	Information Protection Processes and Procedures
IVASS_12	Communications to IVASS	RC.CO	Communications
IVASS_13	Definition of Cyber Security policy	ID.GV	Governance
IVASS_14	Semi-annual checks of compliance of company operations with policies	DE.CM	Security Continuous Monitoring
IVASS_15	Training	PR.AT	Awareness and Training
IVASS_16	System configuration	PR.IP	Information Protection Processes and Procedures
IVASS_17	Backup management (daily)	PR.IP	Information Protection Processes and Procedures

Talanx Group Information Security Policy

The Talanx Group's Information Security Policy, which suggests good practices to the Group's international companies, including therefore HDI, defines the security strategy of the Talanx Group which, in order to be pursued, is translated into safety objectives articulated according to the control defined by the ISO / IEC 27001: 2013 reference standard.

Table 5: Requirements from Talanx Group Information Security Policy for Insurance Risk Assessment Pilot

ID	Requirement	Reference
TAL_1	Information security policies	ISO27001, Annex A, A.5
TAL_2	Organization of information security	ISO27001, Annex A, A.6

ID	Requirement	Reference
TAL_3	Security of human resources	ISO27001, Annex A, A.7
TAL_4	Heritage management	ISO27001, Annex A, A.8
TAL_5	Access control	ISO27001, Annex A, A.9
TAL_6	Encryption	ISO27001, Annex A, A.10
TAL_7	Physical and environmental security	ISO27001, Annex A, A.11
TAL_8	Safety of activities	ISO27001, Annex A, A.12
TAL_9	Security of communications	ISO27001, Annex A, A.13
TAL_10	Acquisition, development and maintenance of the system	ISO27001, Annex A, A.14
TAL_11	Relations with suppliers	ISO27001, Annex A, A.15
TAL_12	Information security incident management	ISO27001, Annex A, A.16
TAL_13	Aspects on information security in business continuity management	ISO27001, Annex A, A.17
TAL_14	Compliance	ISO27001, Annex A, A.18

Through its objectives set within the framework of Cybersecurity, HDI intends to address and meet the security objectives defined within the Group Policy, according to a mapping of the requirements summarized in the following table.

Table 6: Identified Talanx Group Information Security Policy requirements mapped on HDI's measures

ID	Requirements	ID Categ.	Category
TAL_1	Information security policies	ID.GV	Governance
TAL_2	Organization of information security	ID.GV	Governance
TAL_3	Security of human resources	PR.AT	Awareness and Training
TAL_4	Heritage management	ID.AM	Asset Management
TAL_5	Access control	PR.AC	Identity Management Authentication and Access Control
TAL_6	Encryption	PR.DS	Data Security
TAL_7	Physical and environmental security	PR.AC	Identity Management Authentication and Access Control
TAL_7	Physical and environmental security	PR.IP	Information Protection Processes and Procedures
TAL_7	Physical and environmental security	DE.CM	Security Continuous Monitoring
TAL_8	Safety of activities	PR.IP	Information Protection Processes and Procedures
TAL_8	Safety of activities	PR.DS	Data Security

ID	Requirements	ID Categ.	Category
TAL_8	Safety of activities	DE.CM	Security Continuous Monitoring
TAL_8	Safety of activities	PR.PT	Protective Technology
TAL_8	Safety of activities	DE.DP	Detection Processes
TAL_9	Security of communications	PR.DS	Data Security
TAL_9	Security of communications	DE.CM	Security Continuous Monitoring
TAL_9	Security of communications	PR.AC	Identity Management Authentication and Access Control
TAL_10	Acquisition, development and maintenance of the system	PR.DS	Data Security
TAL_10	Acquisition, development and maintenance of the system	PR.IP	Information Protection Processes and Procedures
TAL_11	Relations with suppliers	ID.AM	Asset Management
TAL_11	Relations with suppliers	ID.SC	Supply Chain Risk Management
TAL_11	Relations with suppliers	PR.AT	Awareness and Training
TAL_12	Information security incident management	RS.RP	Response Planning
TAL_12	Information security incident management	RS.CO	Communications
TAL_12	Information security incident management	RS.AN	Analysis
TAL_12	Information security incident management	RS.MI	Mitigation
TAL_12	Information security incident management	RS.IM	Improvements
TAL_13	Aspects on information security in business continuity management	PR.IP	Information Protection Processes and Procedures
TAL_14	Compliance	ID.GV	Governance

6. Impact of regulations and standards on FINSEC components

The regulations and directives reviewed in the previous sections prompt a number of implications for the components of the FINSEC project and the design of the project's architecture.

The following is a preliminary logical view of the FINSEC platform architecture, which is currently under development in WP2 and will be documented in D2.4.

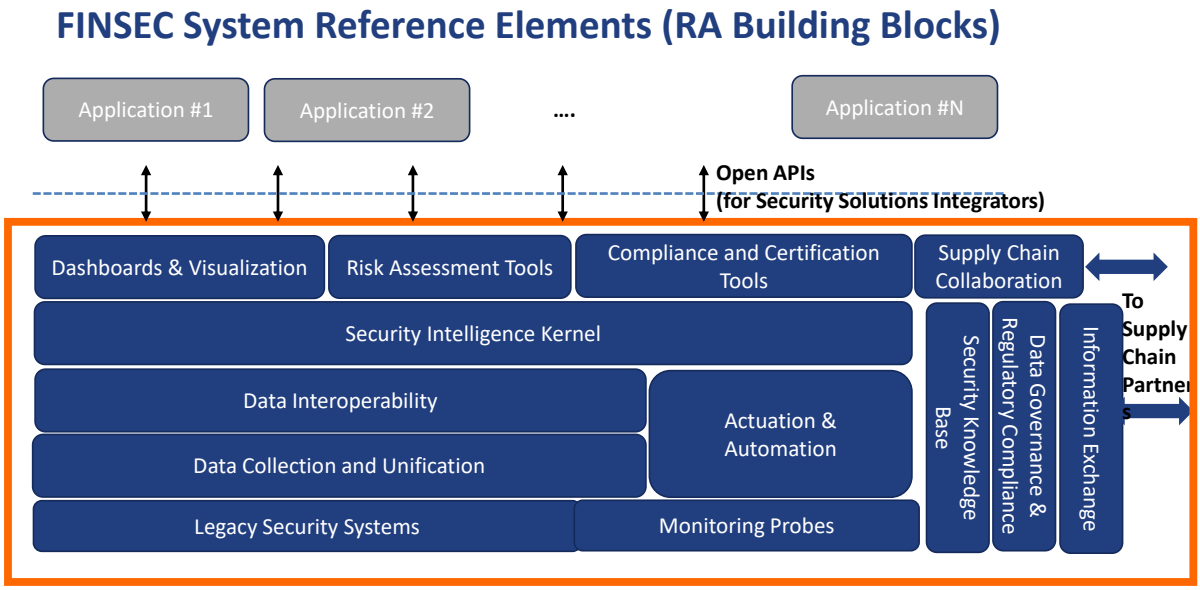

Figure 2: FINSEC System Reference Elements

The FINSEC RA defines a set of building blocks for building data-intensive security monitoring systems including:

(i) Monitoring probes, which interface to cyber and physical security systems towards collecting security-related information

(ii) Data Collection mechanisms will ensure data quality, data filtering, as well as adaptive selection of the needed data sources based on dynamic changes to the configuration of the critical infrastructures

(iii) Actuation and Automation module, builds on predictive security and machine learning to achieve the identification and correlation of events

(iv) Security Intelligence Kernel, which identifies known and potential new security attack patterns by means of advanced data analytics and matching of identified evens against the security knowledge base

(v) Risk Assessment Tools include a range of background security technologies, including a risk assessment engine, Security Information and Event Management (SIEM) technologies, anomaly detection technologies, predictive CCTV analytics, a Risk Assessment Engine (RAE), vulnerability assessment services and more

(vi) Supply Chain Collaboration, are tools facilitating the collaborative assessment and mitigation of risks by participants in the financial sector supply chain.

(vii) Security Knowledge Base that holds Information gathered a-priori (databases, etc.) on known attacks against critical infrastructures

(viii) Open APIs are Open programming interfaces dedicated to each single service within the RA

Table 2 summarizes the main impacts of each regulation or directive with respect to the building block being affected.

Table 2 - Building block and impact by regulation

Building Block	Role within the RA	Regulations	Main Impacts
Data collection – CCTV	Monitoring for physical security level – raw data extraction	GDPR	• Minimisation: not exceeding needed amount of acquired data; • Impact Assessment on Data Protection; • Control Authority consultation
Data collection - Access control	Monitoring for physical security level – raw data extraction	GDPR NIS	• Minimisation: not exceeding needed amount of acquired data; • Transparency in the use of personal data; • Privacy by design; • Personal data usage acceptance; • Right of deletion; • Need for mechanisms such as Multi-Factor Authentication, Single Sign-On, User Behaviour Analysis, etc.
		ISO 27001	• Physical security perimeter with physical barriers; • Physical entry controls; • Removal of access rights at the end of employment; • Isolation between delivery/loading areas and information processing facilities; • Written access control policy according to business and security requirements
Logs control	Monitoring for logical security level – raw data extraction	GDPR	• Minimisation: not exceeding needed amount of acquired data • Pseudonymisation • Personal Data encryption; • Need for role-based access controls
		NIS	• Notification of significant security incidents to authorities
		ISO 27001	• Event records shall be synchronized with an agreed accurate time source
Risk Assessment Tools: SIEM	Existing security tools, which collects, analyses and correlates security events within a critical infrastructure, with generation of alarms and reports	GDPR	• Need for automated reporting, ensuring that data handling is in compliance with security by design (pseudonymisation, encryption, minimization of data); • Automated measure inside the SIEM to correct activities violating GDPR-compliance controls; • Flexibility to quickly process any kind of data generated by different applications; • Need for data destruction policies; • Need for role-based access controls

		NIS	• Need for traceability and communicability of number of users affected by an incident and its duration;
		ISO 27001	• Third party service must be in compliance with the service delivery agreement; reports of service to be periodically reviewed
Data collection module	Ensures that data from different data sources (security monitoring data, assets monitoring data, user behaviours, customer interaction data, publicly available security threat knowledge bases, vulnerabilities knowledge bases, sensor data) are correctly gathered together	GDPR	• Minimisation: not exceeding needed amount of acquired data; • Accountability (e.g. control logs as evidence of compliance of data usage); • Data Security test procedure; • Need for network firewall/antivirus; • Need for Data Leakage Protection measures • Automatization to avoid human errors in data management
		ISO 27001	• Classify collected data in terms of their value, sensitivity and criticality
Data Storage module	Big data infrastructure where FINSEC data are saved	GDPR	• Storage time no longer than needed; • Privacy by design; • Accountability (e.g. control logs as evidence of compliance of data usage); • Resilience-based design against physical and logical damages; • Data Security test procedure; • Need for Data Leakage Protection measures
		ISO 27001	• Classify stored data in terms of their value, sensitivity and criticality; • System resource in terms of data storage must be constantly monitored; • Back-up of data; • Written procedures for the management of removable media
Data interoperability module	Ensures that data are unified and compliant with data formats selected for FINSEC purposes	GDPR	• Automation to avoid human errors in data management
Actuation & automation module	Semi-automated intelligence module to interact with data collection settings	GDPR	• Avoid the use of data collected to extract intelligence that may be used for personalised behavior analysis
Security Intelligence Kernel	Analytics tool, extracting information about abnormal or suspicious behaviours	GDPR NIS	• Minimisation: not exceeding needed amount of acquired data; • Storage time should not be longer than required;
		ISO 27001	• System resource in terms of information extraction must be constantly monitored

Security Knowledge Base	Information gathered a-priori (databases, etc.) on known attacks against cyber critical infrastructures	GDPR	• Minimisation: not exceeding needed amount of acquired data; • Storage time no longer than required.
		NIS	• Ensure a network security level adequate to the estimated level of risk.
Dashboard & visualization	Visualization and interaction between the user and the applications (Risk Assessment tools, Compliance and Certification tools)	GDPR	• Minimisation: the required amount of visualized data should not exceed purpose;
		ISO 27001	• Implement measures to ensure responsibilities of users are clear, to reduce the risk of misuse of the services • Removal of access rights at the end of employment
Risk Assessment Tools	Application delivered as a service for risk prediction and mitigation	GDPR	• Need for prediction of economic and reputational impacts of cyber and physical attacks
		NIS	• Ensure a network security level adequate to the estimated level of risk
		ISO 22301	• Resilience, include business continuity management aspects
Supply Chain Collaboration module	Ensures Security data sharing and information exchange between different end-user organizations	GDPR	• Accountability (e.g. control logs as evidence of compliance of data usage); • Pseudonymisation; • Personal Data encryption; • Need for network firewall/antivirus; • Need for Data Leakage Protection measures
		ISO 27001	• System resource in terms of data exchange (network resources) must be constantly monitored; • Information exchange agreements have to be foreseen between different parties
APIs	Open programming interfaces dedicated to each single service within the RA	ISO 27001	• Implement measures to ensure responsibilities of users are clear, to reduce the risk of misuse of the services • Removal of access rights at the end of employment

6.1. CCTV systems

Video monitoring systems constitute one of the main physical security tools within the FINSEC architecture. Such systems are subject to both general European regulations and national laws about privacy and data usage. In particular, the CCTV systems are significantly affected by the GDPR regulation. Although GDPR was discussed earlier in this deliverable (section 4.1), this section discusses its impact on the use of CCTV systems. Annex 1 includes more information on national regulations relevant to this topic.

The new GDPR regulation impacts on some aspects of a CCTV system design and usage. In particular, the following principles have to be taken into account:

Minimization: CCTV devices have to be installed in order to ensure the amount of data processed is the minimum needed for the purposes of monitoring. For instance, CCTV cameras are supposed to monitor only the portion of space which is strictly correlated to the physical access to the monitored area, avoiding to register the surrounding zones.

Right to be forgotten: A data subject has the right to obtain from the data controller the deletion of their personal information from the system as soon as the data is no longer necessary for the purpose it was collected for.

Data portability: the CCTV system should allow the data subject to receive its own data in a portable and standard format

Data Protection Impact Assessment: this can be undertaken before installing a new CCTV system; it is aimed at identifying the most effective way to comply with GDPR requirements, thus reducing the risks of misuses of personal information. The DPIA can be needed for a CCTV system, as specified in Article 35 of GDPR, mentioning the "large scale, systematic monitoring of public areas (CCTV)".

6.2. Physical access controls – biometric measures

Use of biometric measures is another possible way to control physical access to sensitive areas of critical infrastructures within the scope of FINSEC. The following paragraphs discuss the main restrictions and recommendations to system designers for compliance with the current regulations and laws.

Any physical access control system must be designed in compliance with both the GDPR regulation, and the NIS, mainly under the following points of view:

Data Treatment Registry: the purpose for the use of biometric data has to be specified in a written registry. The registry should be available to the authorities for audit purposes.

Data Protection Impact Assessment: as explained for the CCTV case, this measure is aimed at identifying the most effective way to comply with GDPR requirements, thus reducing the risks of misuses of personal information. This assessment evaluates the effective need of all the foreseen biometric data treatments, and related risks.

Data Protection Officer: biometric data treatment forces the organization to appoint a Data Protection Officer, whose roles are ensuring the compliance of treatments to the GDPR, supporting the activities related to the Data Protection Impact Assessment and being a contact point for the control authorities.

Right to be forgotten: the data subject has the right to request from the data controller to delete all of his personal information - biometric data from the system, once the data is no longer necessary for the purpose it was collected for.

Data portability: the access monitoring system should allow the data subject to receive its own biometric data in a portable and standard format.

Information protection: Furthermore any information stored will need to be protected (application of the NIS directive as transposed to national laws), so that data breach may be avoided in the first place. Thus there is the need for mechanisms such as Multi-Factor Authentication that will protect the information.

6.3. Blockchain infrastructure

The Peer-to-Peer payment solution regulatory and law compliance requirements fall under several categories.

First, in terms of regulators, regulations and directives, the Smart Contracts need to be put under control either by a private company or consortium that must be, based on regulatory requirements, accepted as a "Trust", subject to relevant conditions, controls and inspections.

Second, effective controls need to be formulated for all encompassing prevention of risks (money laundering, terrorism, illegal activities, market manipulation, etc.), possibly granting CBs the same level of risk decision making they'd have in a "standard" payments scenario (for AML and other).

Third, end-to-end transactions tracking must be enabled. This could be achieved by leveraging on inherent CB KYC (Know Your Customer) provisions, granting them visibility on all CBs, on demand or automatically (for AML).

Finally, the GB and the Trust must accept being auditable by an independent and established audit firm.

Blockchain transactions ensure the privacy of end-users. Hence, end-users' transactions are inherently anonymously stored on the Blockchain. However, the privacy of end-users is protected as long as their CBs preserve separation of their network and real identities from other circuit participants or attackers. Along the same lines, cyber-security and in particular, the Digital Wallet (the mobile app) must be capable of safely storing end-user's credentials, leveraging on specific end-user's device features on platform provisions or on additional app components. The CB and GB must be able to adopt IT security best practices for their systems hosting dashboards. Similarly, peer-to-peer payment solution Smart Contract software should be protected, possibly by a continuous review by a third party that will be defined.

Finally, end-users must know about implications of using an easy and innovative, yet regulated, payment solution, where any DCASH and/or its equivalent flat currency may be forfeited or seized if illegal activities are performed using DCASH (also by other End-users) and unusable DCASH results in unusable or non/existing corresponding flat currency (however exchanged with it), and this possibly implies a new framework of usage terms and conditions.

6.4. Cloud technology

The FINSEC architecture foresees the use of a private cloud system to exchange data and information between the different security control centers. The cloud technology can be used in FINSEC in both the PaaS (Platform as a Service) and IaaS (Infrastructure as a Service) perspectives. The compliance with current GDPR regulation and NIS directive foresees the following measures:

- Clear definition of the cloud provider: who handles the infrastructures;
- Clear definition of data storage physical location;
- A priori definition of risks: assessment of how cloud deployment introduces data loss and data breach risks;
- Use of secure data transmission protocols;
- Store only encrypted data in the cloud; and
- Adequate logging procedures to monitor data access.

7. General recommendations for FINSEC

Based on the information presented above, we provide a digest of the regulatory (RR) and standardization requirements (SR) that impact the design of the FINSEC platform (including the individual components) and the execution of the pilots.

RR1. Minimization of data collected. Adding more layers of security and collecting more data than what is really required to face the existing challenges, is a temptation for system designers, especially in an environment exposed to a number of different and largely unknown threats; however, GDPR clearly states that the amount of data (personal data in this case) processed is "*adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed*".

- The data being collected in FINSEC should not exceed the minimum required. While this may put a limit to the further exploitation of the data collected, it does not prohibit a well-defined reason for collecting them in the first place (e.g. "extended CCTV coverage" may be justified for establishing a "soft" perimeter around ATMs, if the public is notified, privacy is respected and passers-by are not recorded).

RR2. Pseudonymisation. The processing of personal data should be performed in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately. Pseudonymisation is different from anonymization, as in the latter the detailed information about the owner of the data is lost (as in the USA and UK voting-influence crisis with Cambridge Analytics), while in the former the data can be traced back to their owners.

- The need for pseudonymisation will influence the way the FINSEC pilots are implemented.

RR3. Purpose limitation. Additionally the data collection goals should be consistent with the (initially defined) purpose set for the system and should be erased after that purpose is fulfilled.

- Purpose limitation means that "*They should be collected only for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes*" which limits the opportunities for exploiting data collected by one system for another (initially unforeseen) purpose, unless explicit notification is issued.

RR4. Increased incident reporting and notification needs. The NIS requires that "incidents having a significant impact on the continuity of the essential services they provide" are disclosed to the supervising authorities without undue delay. In determining the significance of security incidents operators of essential services will need to consider factors such as how many users are affected by disruptions to essential services, how long such an incident lasts and the "geographic spread" of the impact from such an incident. In contrast to GDPR, all incidents need to be reported including even the outages affecting availability that meet the stated threshold.

- The need for notification, required by NIS and GDPR, is thus a major driver for the selection of features that will need to be present in the FINSEC Knowledge Base.

RR5. User profiling. Controllers may continue to carry out profiling and automated decision-making if the processing doesn't produce legal or similar significant effect on the individuals, but always follow the GDPR principles.

- Any profiling activity implemented within FINSEC (e.g. analytics-based profiling on a CCTV stream) is prohibited, in case it leads to an individualized assessment and a recommendation about an individual.

RR6. Periodic Data Privacy Impact Assessment need to be foreseen. An obligation established by the GDPR is to carry out an impact assessment (Privacy Impact Assessment - PIA) for organizations that

perform data processing that may involve a high risk for the rights and freedoms of natural persons. The origin, nature, particularity and severity of such risk must be assessed (Recital 84 of the GDPR).

- A periodic assessment of the impact to user data privacy should be facilitated by the design of every FINSEC component. DPIA should precede any actual use of the component.

RR7. The design of FINSEC (input, data models, application logic) **should respect individual privacy rights.**

- The structure of the information should guarantee that the right to be informed about the information processed and stored as well as the right to be forgotten, are maintained by the users.

RR8. Data processing contracts are required. The contracts should state the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data to be processed and categories of data subjects and the obligations and rights of the controller.

- Data processing contracts need to be established between data owners (controllers) and data processors (technical partners). If vendors are involved in the execution of a pilot, vendor contracts need to be updated prior to the FINSEC pilots to comply with GDPR privacy requirements.

SR1. Collaboration is critical to assess emerging threats. The ISO28000 standard indicates the need for collaboration between peer organizations as well as partners in a supply chain (suppliers-customers) as a significant opportunity for an organization to be better informed and equipped for the threats emerging. This was vividly understood e.g. during the WannaCry crisis.

- Collaboration based on information exchange is an important consideration in FINSEC. The data model for information sharing should be based on the insights about threats and vulnerabilities that the financial institutions can offer.

SR2. Business Continuity, operational resilience. Financial services are mission-critical activities that should continue no matter how serious the threat it is exposed to. Anticipating failure and pursuing fault tolerance in the system design and implementation is a primary goal.

- Business continuity (itself a standard, ISO/IEC 22301) is a central element of the whole Information Security Management System and should be a key consideration for the FINSEC implementation.

SR3. Information about vulnerabilities needs to be obtained. ISO/IEC 27001 indicates in its A12.6 section "*Timely information about technical vulnerabilities of information systems being used shall be obtained, the organization's exposure to such vulnerabilities evaluated, and appropriate measures taken to address the associated risk*".

- Thus information exchange (as will be pursued by the FINSEC Collaboration Module) that will lead to timely assessment of vulnerabilities as new threats emerge is important to achieve compliance with the standard.

SR4. Proportionality is important. The security strategy should adapt to the magnitude and impact of the risks, considering the practical constraints imposed by the business needs and the environment in which the business operates. In terms of resources spent (time, money, effort) the amount to be spent on mitigating a risk should be proportional to the risk. Proportionality is thus an important design consideration for the Security-as-a-Service (SECaaS) product and service offering.

- The security requirements expected from a Fintech service provider (an SME) with a very specific business model, well-controlled service endpoints and a limited number of clients

should be less stringent than the ones expected from a bank which offers a multitude of services, web-based transactions including payments to millions of users.

8. Conclusions

This deliverable reviewed existing laws, regulations, standards and directives that apply for financial infrastructures, to provide a list of recommendations for the FINSEC project. These recommendations complement the insights delivered though T2.1 concerning the requirements arising from the need of financial organisations to comply with regulations and standards.

More specifically, D.2.2 provided a thorough list and an extensive description of the regulations relevant to financial institutions as defined by supervising authorities and regulatory bodies. In particular, Section 2 included reference to the Markets in Financial Instrument Directive MFID II, it also assessed the European Central Bank Cyber Incident Reporting Regime, providing directions for cyber incident reporting such that protection towards cyber-attacks and data breaches is enhanced. It also reviewed Payments Services Directive (PSD2), which introduces higher security standards for online payments and the Payment Card Industry Data Security Standard (PCI DSS), the latter being the worldwide information security standard for securing card payments. Among others, Section 2 also described the role of the European Banking Authority II to monitor new and existing financial activities, whereas it included reference on security requirements for outsourcing to cloud providers.

Then, the deliverable provided an overview of the standards associated to the financial sector. In particular, it emphasized on the ISO 27000 family of standards that are offering best practice recommendations on information security management, risk management and security controls within the context of an Information Security Management System (ISMS). It then emphasized on ISO 27001 which mainly focuses on information security management system domain.

This deliverable included an analysis of general regulations that have an Impact on banking and financial services. It extensively discussed GDPR and its impact on financial institutions with respect to the collection of customer information.

Moreover, D2.2 analysed the impact of these regulations, standards and directives on the pilots included in the FINSEC project as well as their implications for the components of the FINSEC project and the design of the project's architecture (e.g. APIs, CCTV etc.). As a result of this analysis, it was able to provide a list of recommendations (based on Regulatory Requirements, RRx, and Standardization Requirements, SRx) to be followed by the FINSEC project partners both in the design of the system components, as well as in the implementation of the pilots.

9. References

1. European Parliament and Council (2014a). "Directive 2014/65/EU on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU". *EUR-lex.* Accessed: 15th of September 2018. Retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014L0065

2. "Markets in Financial Instruments Directive (MiFID II): Frequently Asked Questions". *European Commission Press Release Database.* Accessed: 15th of September 2018. Retrieved from: http://europa.eu/rapid/press-release_MEMO-14-305_en.htm

3. European Parliament and Council (2015). "Directive 2015/2366/EU on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC". *European Commission.* Accessed: 20th of September 2018. Retrieved from: https://ec.europa.eu/info/law/payment-services-psd-2-directive-eu-2015-2366_en

4. European Payments Council (2017a). "PSD2 Infographic". Accessed: 30th of September 2018. Retrieved from: https://www.europeanpaymentscouncil.eu/sites/default/files/infographic/2017-06/EPC_Infographic_PSD2_March-2017_Updated%20June%202017.pdf

5. Papamichael. P.G., Evagorou, C., Antoniades, C (2017). "The early bird catches the worm": anticipating the challenges and opportunities of PSD2". *Payment Services Directive 2 | Challenges and Opportunities, Deloitte Cyprus*, pp.1-7. Accessed: 20th of September 2018. Retrieved from: https://www2.deloitte.com/content/dam/Deloitte/cy/Documents/financial-services/CY_FS_PaymentServicesDirective2_Noexp.pdf

6. European Commission (2017a). "Payment Services Directive (PSD2): Regulatory Technical Standards (RTS) enabling consumers to benefit from safer and more innovative electronic payments". *European Commission Press Release Database.* Accessed: 15th of September 2018. Retrieved from: http://europa.eu/rapid/press-release_MEMO-17-4961_en.htm?locale=en

7. European Payments Council (2017b)."Understanding the Final Regulatory Technical Standards for strong customer authentication and common and secure open standards of communication under PSD2". *European Payments Council AISBL.* Accessed: 30th of September 2018. Retrieved from: https://www.europeanpaymentscouncil.eu/sites/default/files/infographic/2018-02/EPC%20infographic%20on%20the%20RTS%20on%20strong%20customer%20authentication_February%202018.pdf

8. PCI Security Standards Council (2017). "Payment Card Industry 3-D Secure (PCI 3DS), Security Requirements and Assessment Procedures for EMV® 3-D Secure Core Components: ACS, DS, and 3DS Server". Accessed: 10th of September 2018. Retrieved from: https://www.pcisecuritystandards.org/documents/FAQs_for_PCI_3DS_Core_Security_Standard.pdf

9. Bankaufsichtliche Anforderungen an die IT (BAIT) (2018)."BaFin, Rundschreiben 10/2017 (BA) in der Fassung vom 14.09.2018". Accessed 28 September 2018. Retrieved from: https://www.bafin.de/SharedDocs/Downloads/DE/Rundschreiben/dl_rs_1710_ba_BAIT.pdf?__blob=publicationFile&v=9

10. Committee of European Banking Supervisors (2014). "Guidelines On Outsourcing". Accessed: 5th of September 2018. *European Banking Authority.* Accessed: 10th of September 2018. Retrieved from: https://www.eba.europa.eu/documents/10180/104404/GL02OutsourcingGuidelines.pdf.pdf

12. European banking authority (2018). "Guidelines on the security measures for operational and security risks of payment services under Directive (EU) 2015/2366(PSD2)". Accessed: 10th of September 2018. Retrieved from:

https://www.eba.europa.eu/documents/10180/2081899/Guidelines+on+the+security+measures+under+PSD2+%28EBA-GL-2017-17%29_EN.pdf

14. IVASS (2018). "Regulation laying down provisions on the system of governance", link to the regulation (in Italian)". Accessed: 4th of September 2018. Retrieved from: https://www.ivass.it/normativa/nazionale/secondaria-ivass/regolamenti/2018/n38/Regolamento_38_2018.pdf?language_id=3

15. International Organisation for Standardization (2018). "ISO/IEC 27000 family - Information security management systems".

16. European Commission (2018). "The Directive on security of network and information systems (NIS Directive)". *Digital Single Market.* Accessed: 8th of September 2018. Retrieved from: https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

17. European Commission (2017b). "Making the most of NIS – towards the effective implementation of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union". *EUR-lex.* Accessed: 11th of September 2018. Retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1505297631636&uri=COM:2017:476:FIN

19. National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity Version 1.1. Published April 16, 2018, Accessed: 24th of October 2018. Retrieved from: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

20. 2015 Italian Cyber Security Report, A National Cyber Security Framework, Accessed: 24th of October 2018. Retrieved from: http://www.cybersecurityframework.it/sites/default/files/CSR2015_ENG.pdf

21. Cyber Defense Methodology for an Organization, ver.1.0, published by the National Cyber Security Authority, Accessed: 24th of October 2018. Retrieved from: https://www.gov.il/BlobFolder/policy/cyber_security_methodology_for_organizations/he/Cyber1.0_english_617_A4.pdf

22. Federal Trade Commission (2015). "Gramm-Leach-Bliley Act". Accessed: 1st of September 2018. Retrieved from: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2017:0010:FIN

23. PwC (2017). "Is ePrivacy defining the future standard of data protection for the banking industry? The ePrivacy Regulation (ePR) and its impact on banks". *The ePrivacy Regulation and its impact on banks.* Accessed: 5th of September 2018. Retrieved from: https://news.pwc.ch/wp-content/uploads/2017/12/20171206_ePrivacy_POV_final.pdf

24. European Parliament and of the Council (2014b). "Electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC". Accessed: 5th of September 2018. Retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG

25. Woolfson, P., Terruso, D. (2015). The eIDAS Regulation: An Opportunity for Financial Services and Insurance?.Payments Compliance. Accessed: 6th of September 2018. Retrieved from:

https://www.steptoe.com/images/content/6/0/v1/6077/payments_compliance_-_the_eidas_regulation_an_opportunity_for_financial_services_and_insurance_-_2015-09-02.pdf

26. Tangen, S., Austin, D., (2012). "Business continuity - ISO 22301 when things go seriously wrong". *International Organisation for Standardization.* Accessed: 7th of September 2018. Retrieved from: https://www.iso.org/news/2012/06/Ref1602.html

27. Consultative Document, "Sound Practice: Implications of fintech developments for banks and bank supervisors", August 2017, Basel Committee on Banking Supervision

ANNEX A

Operation of CCTV systems under Italian legislation

Italian legislation, following the Video Monitoring Action of April 8th 2010, foresees the following restrictions on the design principles, installation and use of CCTV systems in areas accessible to the public:

- Information: people have to be clearly informed about the presence of video surveillance by means of signs well visible even in the dark. Moreover, special signs have to clearly state if the video surveillance is connected to police stations;
- Storage: video data have to be stored for a maximum period of 24 hours, with a possible derogation to 1 week in the case of threat-related activities, after a preliminary detailed evaluation of the effective need of this extra storage time;
- Image access rights: measures and procedures have to be implemented to allow the system owner to check the monitoring activities and video data usage by the operator;
- Data deletion: manual procedures or automatic processes have to be set up to ensure the deletion of data within the imposed maximum period;
- Maintenance: access to images to maintenance operators have to be allowed only in the case this is strictly needed for technical assessments, and in the presence of someone having the proper rights and credentials to access them;
- Authentication and authorization levels: different visibility and image treatment rights have to be configured for the different operators, according to their competences and roles. The subjects have to access the system via authentication credentials, allowing them to perform on the data only the operations foreseen by their own right level. Generally, the visualization, deletion or duplication rights have to be minimized;
- Network connection: in case CCTV devices (e.g., cameras) are connected to a network, they have to be protected against unauthorized accesses. Moreover, data encryption techniques have to be applied before image transmission via public networks or wireless connections.

Biometric measures in Italian legislation

Biometry Action of November 12th 2014 regulates the restrictions and recommendations to biometric measurement systems, summarized in the following:

- Data storage period: the access monitoring system has to foresee a limited period in which the presence of personal data are really necessary, according to their scope. After this period expiration, the data must be deleted;
- Consensus to biometric data for digital signature: informatics documentation can be signed in a digital way with the analysis of biometric data only with the explicit consensus of the user. Alternative methods must be foreseen in case the consensus is denied;
- Consensus to the use of other biometric data: fingerprint or other biometric data (e.g., hand topology) can be used in physical security procedure to monitor accesses to reserved areas,

only with the explicit consensus of the user. Alternative methods must be foreseen in case the consensus is denied;

- Use of biometric data without consensus: biometric data such as fingerprint, hand topology or voice recognition can be used as a security measure without the user's consensus in some applications, such as the authentication to informatics systems and the use of dangerous equipment;
- Minimization: physical access control system must foresee the minimum possible amount of biometric data acquisition, according to the sensitivity level of the monitored area/asset and to the scope of control procedure;
- Encryption of biometric data: biometric data must be encrypted before their storage.