



# Network and Information Security in the Finance Sector

*Regulatory landscape and Industry priorities*

December 2014





## About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at [www.enisa.europa.eu](http://www.enisa.europa.eu).

## Authors

Lionel Dupré, CISA, CISM, NIS Expert at ENISA.

## Contact

For contacting the authors please use [resilience@enisa.europa.eu](mailto:resilience@enisa.europa.eu)

For media enquires about this paper, please use [press@enisa.europa.eu](mailto:press@enisa.europa.eu).

## Acknowledgements

The research, interviews and reporting related to this stocktaking was carried out by FORMIT Foundation. The research was performed by Simona Cavallini, Margherita Volpe and Anthony Cecil Wright. The National Association of Security Specialists in Financial Intermediary (ANSSAIF) provided also some support during the research process.

Maps were drawn from statistical data by Anna Sarri and Christina Skouloudi, ENISA.

### Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 526/2013. This publication does not necessarily represent state-of-the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

### Copyright Notice

© European Union Agency for Network and Information Security (ENISA), 2014

Reproduction is authorised provided the source is acknowledged.

ISBN: 978-92-9204-118-2

DOI: 10.2824/654601

## **Executive summary**

Securing cyberspace and e-communications has become both a governmental and an Industry priority worldwide. The growing relevance of information and communication technologies in the essential functions of the economy has reinforced the necessity of prevention and protection measures in all sectors, naturally including the finance sector.

This research aimed at understanding and comparing the obligations relevant to Information Security within the finance sector in most of the EU28 Member States, to compare them with the Industry's prospects, and to draw a clear vision of important priorities for the future.

In order to understand the differences between the regulatory approaches and the priorities of the Industry, a combined data stock taking approach was elaborated, including:

- A Desktop research, that was used to discover national requirements related to ICT security;
- Interviews of national financial supervisory authorities (NFSA) and information security related obligations and standards;
- An online questionnaire, was used for collecting information from Industry representatives.

The analysis performed revealed the following key aspects:

- Convergence of regulations appear to be a desirable objective in order to reduce both the heterogeneity of security levels as well as the overlapping of prescriptions in the field;
- Compliance costs for Companies established in several countries can be cumbersome;
- The definition of operative standards would be more effective for enhancing security levels than issuing new high level prescriptions;
- International cooperation on security issues in the field might be the most feasible solution in order to define common and appropriate guidelines.

Based on information collected, further research will be required to comparatively assess costs and benefits of different potential scenarios for the improvement of information security baselines in the finance sector.

This report issues four main recommendations:

- EBA and ENISA should consolidate scattered NIS obligations in supervisory guidelines;
- ENISA should establish guidelines on how NIS supervision practices in the Finance-sector apply by extension to their supply chain, including Cloud providers that operate financial services;
- ENISA should establish guidelines which summarise the key conditions for the adoption of Cloud-based applications or services in the Finance sector;
- ENISA should support the ECB and the ESFS (EBA, ESMA, EIOPA) to organise regular and voluntary NIS stress tests in the Finance sector: the purpose is to identify where possible black swan risks and uncover to the greatest extent possible "unknown unknowns".

## **Table of Contents**

<b>1</b>	<b>Introduction</b>	<b>5</b>
1.1	Objective	5
1.2	Policy Context	5
1.3	Target audience	6
1.4	Methodology	6
1.5	Scope	6
1.6	Document structure	7
<b>2</b>	<b>E-communications in the Finance sector</b>	<b>8</b>
2.1	Sector structure	8
2.2	Communications flows	10
2.3	Network infrastructures	11
2.3.1	Infrastructure types	12
2.3.2	IT service providers	13
2.4	Network and Information Security (NIS) drivers in Finance	14
2.4.1	About the influence of foreign regulations	14
2.4.2	Standards and Supervision	15
<b>3</b>	<b>European Regulatory Landscape</b>	<b>17</b>
3.1	Regulations' provisioning for NIS	17
3.1.1	European level	17
3.1.2	Member States' approaches and cultural differences	19
3.2	Domains coverage	22
3.2.1	Lack of coverage and emerging trends	23
<b>4</b>	<b>Industry's prospect</b>	<b>25</b>
4.1	Risks and Challenges	25
4.1.1	Mitigation limitations	27
4.2	Desirable features	28
<b>5</b>	<b>Recommendations</b>	<b>31</b>

## 1 Introduction

Finance networks are increasingly operating at an international level and many Finance companies function in two or more European countries. They interact with National Central Banks, European platforms (e.g. STEP2, TARGET2), and private networks operated by specialised managed providers.

Financial IT systems are exposed to a number of hazards which require consistent efforts to operate securely. In recent years, NIS risks have become more complex and their impact can range from low to very high, including domino effects. Such impacts will not be confined to the “virtual” world; a major attack outreach would most certainly impact the assets in safekeeping or in transit.

### 1.1 Objective

As the finance sector overall is a complex aggregation of several players regulated from several different angles, our aim was to understand both the coverage of Network and Information Security (NIS) obligations in the European regulatory landscape (both at EU and Member State level), and compare it with the Industry’s prospects. This comparison has led to a high-level overview of the situation and to recommendations on the alignment of policies and needs where possible.

### 1.2 Policy Context

The analysis retained three major policies which have a direct or indirect impact on Finance sector’s ICT. The reader can find all references in Annex:

- MiFID 2004/39/EC - Commission Directive 2006/73/EC of 10 August 2006 of the European Parliament and of the Council as regards organisational requirements and operating conditions for investment firms and defined terms for the purposes of that Directive;
- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;
- Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union - COM(2013) 48 final.

The “Payments Services Directives (PSD) Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on Payment Services in the internal market” is also noteworthy as the scope extent of its current revision (PSD2) is currently debated.

Information Security measures are dispersed overall across many European and National regulations. Such fragmentation increases the need for common and shared guidelines as Companies operate more and more at pan-European level.

In Europe, the proposal for a new NIS Directive and the discussions documentation [COM(2013) 48 final - 2013/0027 (COD)] state that an “insufficient level of protection against network and information security incidents, risks and threats across the EU [...], may undermine, ed.] the proper functioning of the Internal market”<sup>1</sup>. This statement is particularly relevant in the finance sector, where a failure of critical IT infrastructure can lead to major damages in the financial market.

---

<sup>1</sup> COMMISSION STAFF WORKING DOCUMENT, EXECUTIVE SUMMARY OF THE IMPACT ASSESSMENT, Accompanying the document “Proposal for a Directive of the European Parliament and of the Council Concerning measures to ensure a high level of network and information security across the Union”, [COM(2013) 48 final].

Overall, three key regulatory categories and one catch-all category were identified, which refer to policies that could indirectly affect finance sector professionals:

- the *Data Protection* category refers to regulation and standards which is relevant to the protection of personal and sensitive data and information;
- *ICT security* category includes regulations and guidelines impacting ICT infrastructures' security Governance and Management, regardless of the sector considered;
- *Finance Sector Security* refers to regulation and standards specific to the security of the finance sector as a whole;
- *Other to be defined, which refers* to categorising all remaining references bearing a possible indirect impact.

Beyond Europe, several other countries have already taken political decisions to reinforce the security of the finance sector which have impact on foreign companies present in European Countries: e.g. the U.S. the Homeland Security Department and the Department of the Treasury elaborated in 2010 the "Banking and Finance Sector-specific plan" as an Annex to the National Infrastructure Protection Plan<sup>2</sup>.

### 1.3 Target audience

This document provides relevant information both at a strategic and governance level.

It is primarily intended to CISOs/CIOs/CTOs of the Finance sector, NIS Experts in National Financial Supervisory Authorities, NIS Experts in the ESFS (EBA, ESMA, EIOPA), and Professional Associations.

### 1.4 Methodology

The stock taking process used a three-angles approach:

- The *Desk research* allowed to collect a consistent stock of publicly available regulations and standards or relevant to Information security / Information assurance in the finance sector.
- An *Online questionnaire* was used to investigate private operators' security management approach.
- *Interviews* aimed at bridging the knowledge gaps between the Desktop research and the questionnaire, while collecting further respondents' spontaneous considerations and context about the issue in object.

### 1.5 Scope

The interviews were elaborated based on the preliminary results of the desktop research and the questionnaire. Their purpose was to drive in an efficient way the interaction with the National Financial Supervisory Authorities and the Industry respondents.

Overall, a number of key questions were used as entry points for obtaining more detailed information:

1. *What security measures are relevant to your business activities ?*
2. *How are security measures implemented?*
3. *Which security measures are considered "best practices" ?*
4. *Which of these measures are voluntary and which are obligatory ?*

---

<sup>2</sup> US. Homeland and Security Department, and US. Department of Treasury, *Banking and Finance Sector-Specific Plan, Annex to the National Infrastructure Protection Plan, 2010*

5. How are threats and vulnerabilities considered within the existing regulatory landscape ?

6. How incidents are detected, managed and addressed ?

The questionnaire collected information and refined the understanding about organisations, regulation and guidelines in place at national level which may impact directly or not the information security in the finance sector. It also revealed how private operators approach security management practically. The questionnaire was structured in three sections, which addresses issues related to a macro-area in the field of information security:

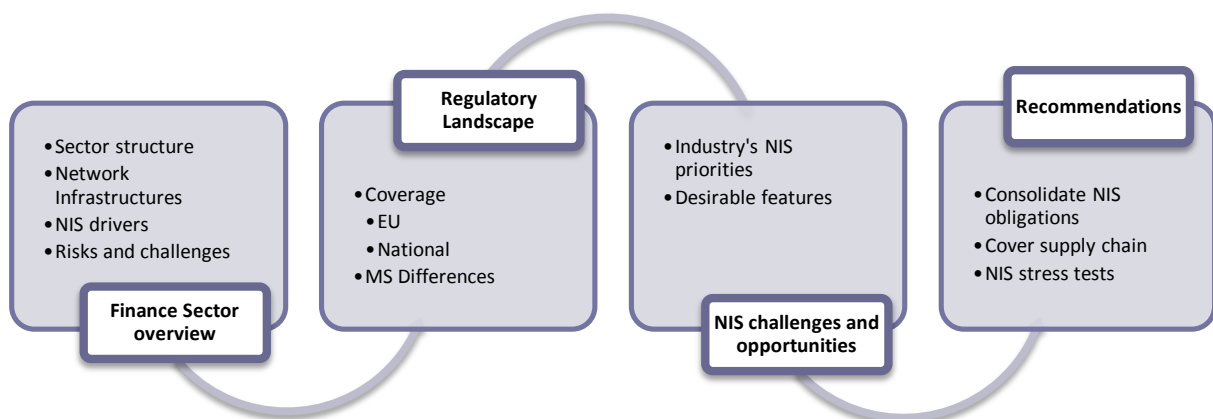
- Section 1 addresses the approach and the competences in the field of security;
- Section 2 addresses private operators management approach to security concerns;
- Section 3 had been left for additional considerations.

A short report with the main findings of each questionnaire has been elaborated and reported in integral form in the Annex.

## 1.6 Document structure

The following pages present the key features of the investigation performed and the relevant conclusions that emerged. In particular:

- Chapter 2 provides high-level background information related to the specifics of the European Finance System.
- Chapter 3 presents a general view of information security related regulations in Europe, and describes other frameworks considered as Security Baselines through the Industry.
- Chapter 4 presents an analysis of the feedback collected among Security Professionals of the Finance sector.
- Chapter 5 proposes a number of recommendations for the future of NIS in the Finance sector.



## 2 E-communications in the Finance sector

The denomination “finance sector” describes a complex mesh of different actors who achieve different missions and goals. Their interaction is also complex and is better understood when adopting an high-level view of the sector and exploring specific areas when required.

### 2.1 Sector structure

A taxonomy of relevant stakeholders was identified including associations and regulation institutions. This taxonomy aims to identify where information security concerns could be of relevance. Figure 1 – Taxonomy of stakeholders presents a high-level view of the European Finance sector main actors, including the relevant authorities.

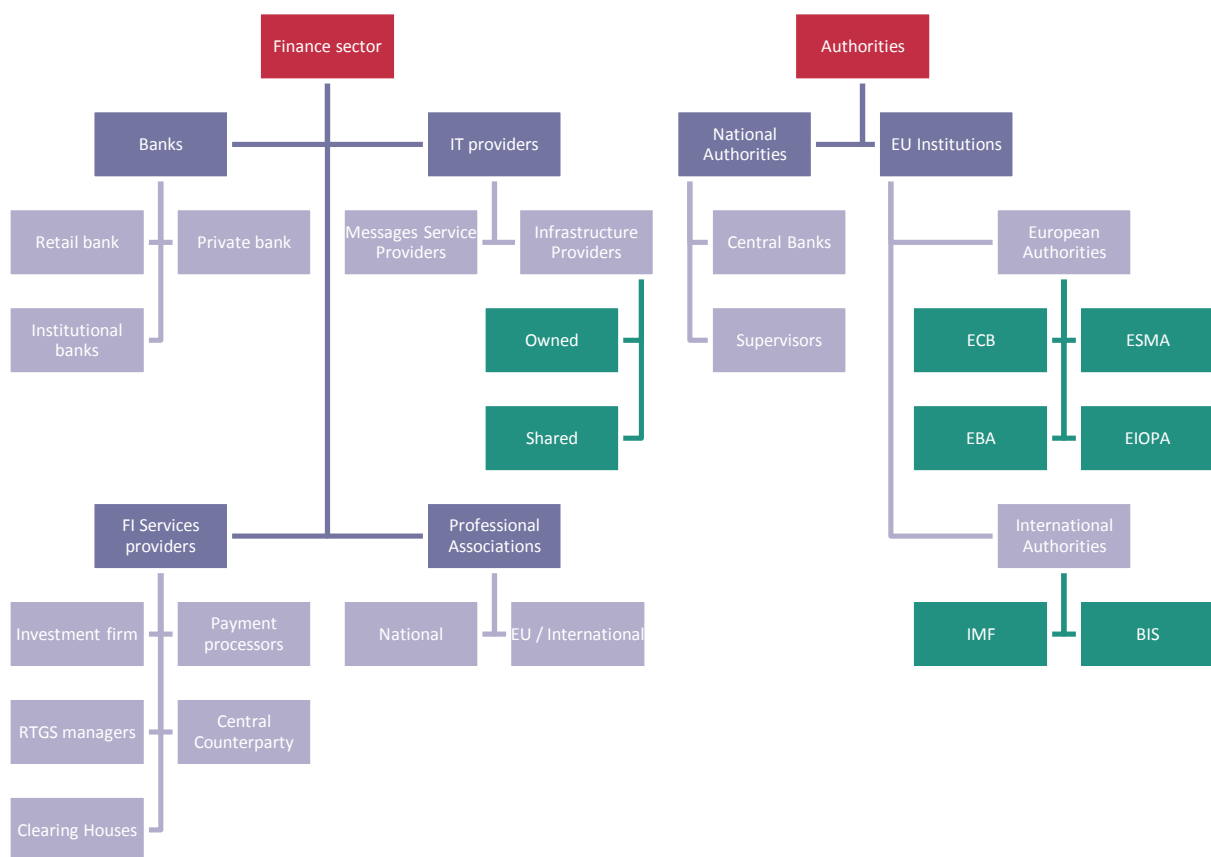


Figure 1 – Taxonomy of stakeholders

The resulting taxonomy considered categorises stakeholders according to four main categories, namely:

- Banks,
- Service Providers,
- Professional Associations
- Authorities.

In the area of Financial Authorities, we can distinguish two different levels:

- **National Supervisory Authorities** are in charge of financial institutions supervision.



- **European Supervisory Authorities** work to improve the functioning of the internal market by ensuring appropriate and harmonised European regulation.

The term **Financial Service activities** encompasses the “**Banks**” and “**FI Service Providers**” categories. These non IT/ICT activities can be considered as “core business” and consist overall in redistributing funds other than insurance, pension funding or compulsory social security. The following activities are considered:

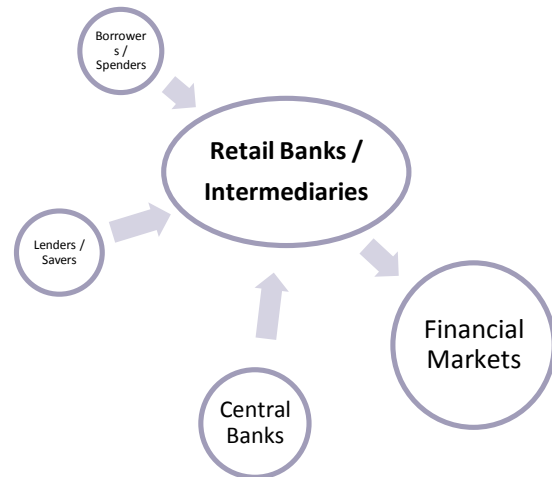
- Monetary Intermediation (Central banking, other monetary intermediation): this group includes transferable deposits (i.e. funds, obtained on a day-to-day basis not only from central banking, but from other non-financial sources);
- Holding companies: this class includes the units that hold the assets (owning controlling-levels of equity) of a group of subsidiary corporations which own the group; the holding companies in this class do not provide any other service to the businesses in which the equity is held (i.e. they do not administer or manage other units);
- Trust, funds and similar financial entities: this class includes legal entities organized to pool without managing securities or other financial assets on behalf of shareholders or beneficiaries; the portfolios are customised to achieve specific investment characteristics such as diversification, risk, rate of return and price volatility. These entities earn interest, dividends and other property income, but have little or no employment and no revenue from the sale of services;
- Other financial service activities, except insurance and pension funding: this group includes financial service activities except those conducted by monetary institutions.

## 2.2 Communications flows

The historical purpose of the finance sector is to provide three types of services:

- Safe storage for financial assets;
- Financial assets movements capabilities (and transactional support);
- Access to financial instruments (Payments, Funds, Securities, Trade).

Overall, financial institutions (e.g. Banks, Corporate and Investment companies) act as brokers to borrowers on one side and lenders on the other side. They rely on several intermediaries, who provide services ranging from depositaries to communications activities.



The key function of the finance sector is therefore the safe storage and communications of assets (cash, gold, securities, etc.). This implies that financial institutions must be able to:

- Store those assets in a secure fashion;
- Communicate with comparable security levels with their counterparts, i.e. their customers, their providers, their central banks, etc.

The protection of stored assets is comparable to a medieval fortress: for ages, banks have built vaults, safes, and those were protected by safeguards. Nowadays, ledger books are entirely digital; physical assets are rarely moved, but banks keep track records of each account statements and transactions in their books.

The protection of assets in transit (i.e. transactions) require specific dedicated protection measures to avoid crime, theft or fraud. The usual technologies are used (cryptography, tunnels, etc.), over a variety of infrastructures that are detailed at a later stage.

The finance sector is actually a mesh of smaller, very specific functions which need permanent communication channels with their counterparts. For example, Banks need to be able to communicate on request with:

- Clearing Houses, both at National and European levels;
- Settlement platforms (e.g. TARGET2, national platforms now provide a bridge to the central bank since the adoption of the Euro).
- Stock Markets;
- Payments processors.
- Etc.

Some of these smaller functions may be grouped within a larger holding company, and therefore communications may happen internally in those finance groups. Indeed, over the past 30 years a consolidation of several Banks or other financial functions through mergers and acquisitions was observed. In such large groups, all communications happen on entirely private networks.

Banks and Payment processors need to relate themselves to National and European reserves, and therefore use their settlement platforms when a movement of funds is operated (after it is cleared). Depending on their size, they either have a direct connection to these platforms, or they may use “service providers” who can register them as participants.

In Europe, an international dimension is present in addition to the national dimension in many cases; high volumes of transactions are processed cross-border.

Figure 2 below pictures information flows between Banks, Clearing Houses and Settlement platforms (European and National).

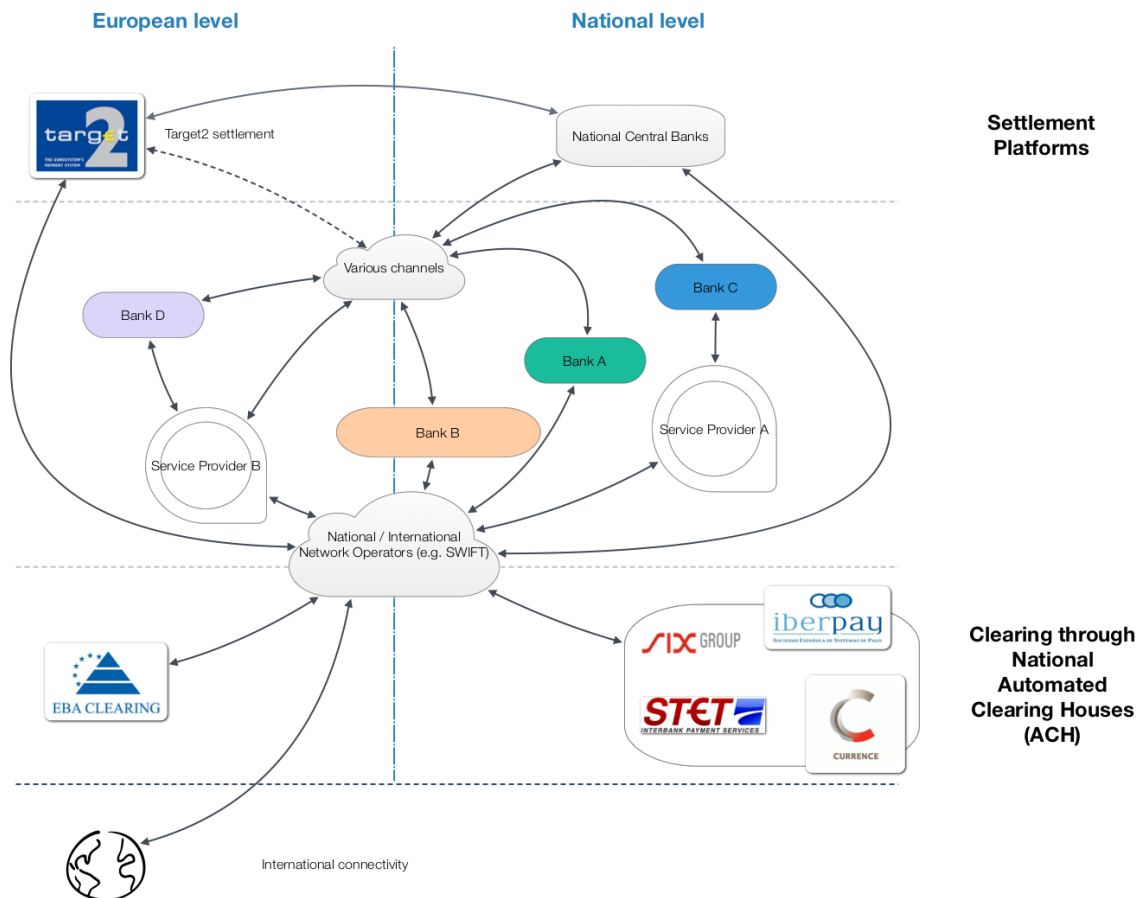


Figure 2 - European Finance communications overview

### 2.3 Network infrastructures

Overall, the means for communications that financial institutions use are numerous. They tend to make equal use of public and private networks, for which they can either be fully in control or be totally dependent on their providers' security and resilience features and operations.

### 2.3.1 Infrastructure types

Four main categories of networks are used in the finance sector:

- Public (i.e. telephone networks, internet, etc.), which are used mostly for customer interaction. In this case, Resilience is managed by the ICT provider, and Security by the financial institution.
- Shared Leased / Owned (information networks e.g. Reuters and some Trade Markets) which are used to access “business” networks. Resilience and Security are both managed mostly by the service provider.
- Leased / Owned (private) lines usually connect headquarters to local branches or to datacentres, or to their worldwide branches. They are provided by ICT Operators and financial institutions use those lines for all internal connectivity (voice, data, multimedia). Resilience is managed by the ICT provider (although financial institutions may choose to establish redundant connectivity), and security is fully managed by the financial institution.
- Provided lines come with the subscription to a service or a platform, and are completely out of the financial institutions’ control, except at the moment of deciding which type of installation is contracted (e.g. SWIFT).

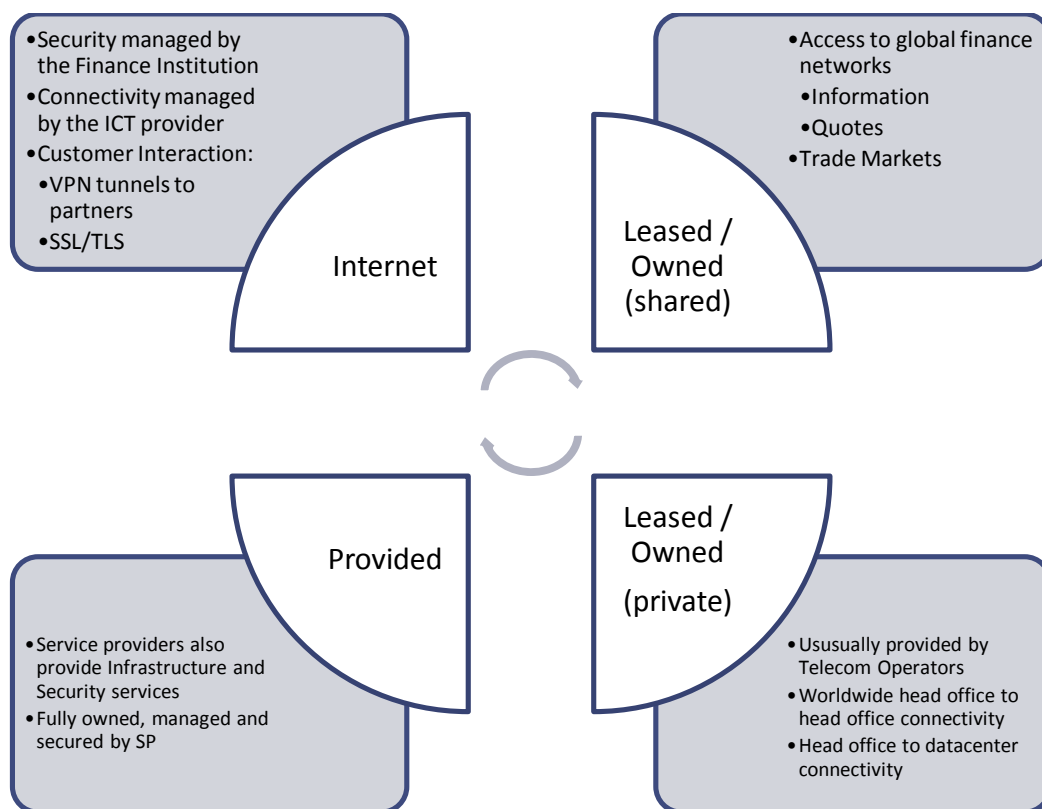


Figure 3 - Network types

### *International Networks*

Banks may often establish one to one private links with counterparts to cut costs and avoid the fees imposed by IT service providers. Many respondents however prefer to use IT service providers for such purpose.

Many respondents referred to SWIFTnet as an IT service provider: SWIFT (The Society for Worldwide Interbank Financial Telecommunication) provides a proprietary information network enabling financial institutions to communicate financial messages in a standardised, secure and trustworthy environment. SWIFT operates in 200+ countries and therefore provides an access point to many types of international markets and counterparts. SWIFT provides the infrastructure, the software, standardised message formats, input validation and many associated services to their customers. SWIFT participants have however no control on the security and resilience measures of the software or the network; they have to trust that both their main and backup gateways will operate and that messages flow is never interrupted.

### *National and European Networks*

At National and European levels, the same scenario may occur as described above. However, the access to Euro settlement platforms (and therefore to the European Central Bank) is a specific service to the TARGET2 platform.

European countries have implemented national gateways to the TARGET2 SSP (Single Shared Platform), which is operated by the Central Banks of Germany, France and Italy<sup>3</sup>. For a few years now, participants are required to interact through the SSP, and no longer through their National Central Bank. The SSP includes a SWIFT gateway, however “Each TARGET2 participant has to subscribe to the relevant SWIFT service according to its own participation profile”.

In Italy, SIANET<sup>4</sup> is a private network provider, which can also route all national interbank commercial payments (commercial payments, credit card transactions, check truncation, etc.) according to the standards defined for RNI (Rete Nazionale Interbancaria). In Interbanking communications taking place through SIANET, all messages are authenticated and depending on the use, encrypted.

### **2.3.2 IT service providers**

The primary function of the Finance sector is traditionally far from information technology preoccupations, and the Finance sector’s IT Banks and financial institutions faced major challenges in automating their business processing. They built entire internal IT functions to address the arising needs. These daughter companies are often however legally separated from their parent company, and obtain a specific status (e.g. PSF “professionnels du secteur financier” in Luxembourg) and therefore a specific regulation.

Those IT Service Providers are often fully dedicated to provide their mother company with internal services. In some cases, they also externalise some services to other companies. Their status remains however the same as regards to the law as they need to demonstrate compliance to their mother company’s regulatory requirements by extension. They however are usually ahead of regulations as they apply a risk-based security governance which is driven by the security of their assets.

In some cases also, these companies have been established as joint-ventures.

### *Service Gateways*

---

<sup>3</sup> <https://www.ecb.europa.eu/pub/pdf/other/ANNEX4TARGET24thprogress.pdf>

<sup>4</sup> <http://www.sia.eu/Engine/RAServePG.php/P/294510011600/M/256010011617>

Many service providers offer gateway services to SWIFTnet, and their customers are typically smaller participants. Communication between such players usually takes place over the Internet, analogous to companies connecting to their banks to make payment instructions or to retrieve account information<sup>5,6,7,8</sup>. Many of these providers have a European presence, but can also operate from non-European countries.

## 2.4 Network and Information Security (NIS) drivers in Finance

Overall, the Industry uses three main layers for their information systems' security governance:

- External oversight describes both the impact of standards and regulations which impact networks and information security directly or not.
- Internal governance describes the strategic alignment to business objectives, depending on which types of NIS architecture are necessary to support the business model.
- NIS operations describe the managed activities that allows the actual security to operate on a daily basis.

According to Industry participants, international standards usually serve as a reference, but some national standards also exist in larger European countries which are taken into account when regulation is high-level.

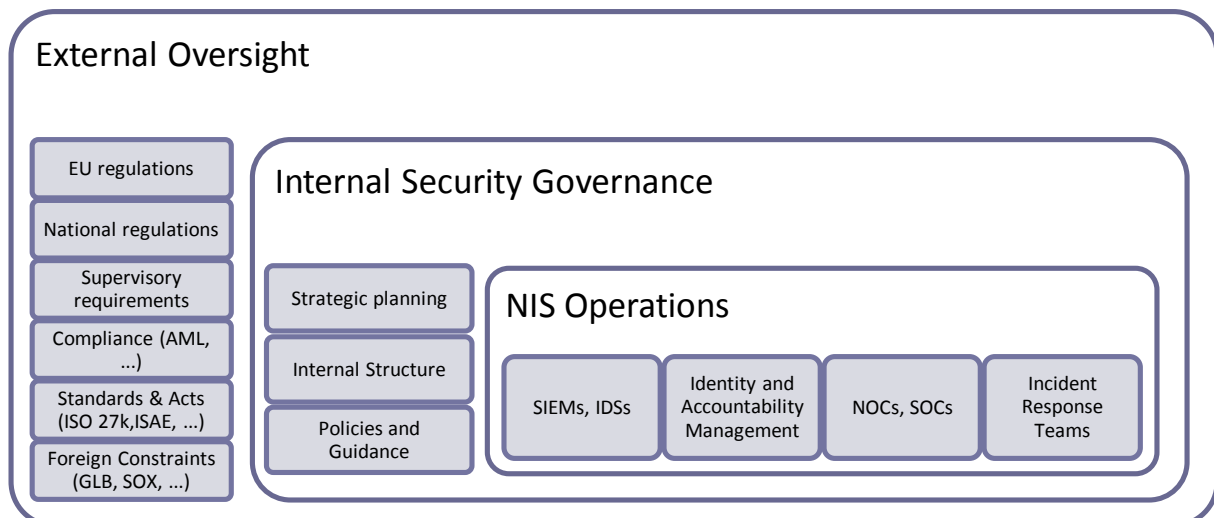


Figure 4 - NIS drivers

### 2.4.1 About the influence of foreign regulations

The influence of international regulations and standards is significant for several reasons. Two influential examples are significant:

- Basel III requires better liquidity provisioning; this will lead to a need for banks to be able to reconstitute liquidity stocks at the end of day on the Interbanking market. Banks tend to develop such provisioning with a trusted counterpart (i.e. call "operational intimacy"). A secure communication link is therefore critical for such type of communications;

<sup>5</sup> <http://www.ingcb.com/media/296564/ingserviceforswiftnet.pdf>

<sup>6</sup> <http://www.bbp.ch/en/home.html>

<sup>7</sup> <http://financialsystems.sungard.com/solutions/corporate-liquidity/syntesys-swift-services>

<sup>8</sup> <http://www.tieto.com/services/business-process-services/business-information-exchange/bank-connectivity>

- SOX requires the control of the “internal control systems” (sections 302 and 404, namely “Corporate responsibility for financial reports”, and “Management assessment of internal controls”). Both sections do not list which internal controls are required, which lead in the finance sector to largely adopt COSO or CoBIT as control frameworks. As a consequence, Security is covered as voluntary measures under the following pillars: Security policy, standards, access and authentication, network security, monitoring, and segregation of duties, physical security<sup>9</sup>. Companies regulated under SOX which have a European presence are therefore required to follow SOX requirements.

#### 2.4.2 Standards and Supervision

International and National Standards are also often used as a mechanism to further define some specific, non-regulatory guidance on NIS matters. Several voluntary standards [such as the German *IT-Grundschutz Manual*, the *UNI CEI ISO/IEC 27001:2006 Standard* and the *Industrial Standard PCI Data Security Standard (PCI DSS)*] are frequently highlighted by the involved respondents.

This approach appears to provide a double benefit: it improves security measures’ technical adequacy (while regulations’ requirements remain at a general/service level) and provides Supervisory Authorities with a clear and immediate understanding of the approach adopted: Supervisory authorities prefer to understand whether or not the operator adopted sound security controls instead of providing evidences of a specific technical measures in place.

The implementation of commonly recognised standards serves this purpose. For instance, the *Industrial Standard PCI Data Security Standard (PCI DSS)* was designed by the association of several payment providers (American Express, Discover Financial Services, JCB, MasterCard and Visa International) in order to improve the security baselines of major payment channels. This standard was mentioned by many respondents as a key point of reference in the field, besides regulations, and extended beyond the payment industry.

At Member State level, Regulations for Finance’s Technology vary widely both in depth and scope coverage. National central banks and National Financial Supervisory Authorities<sup>10</sup> form the National regulatory foundation.

Banks are responsible for ensuring that their systems pass their supervision audits, and also that they contractually provision adequate security levels from their service providers. Typically, supervisors analyse and challenge the security specifications and practices (whether the implementing party will be the banks themselves or external system and service providers).

Typically, Supervisors analyse and challenge the security specifications and practices (whether the implementing party will be the banks themselves or external system and service providers).

The typical mechanisms observed therefore are:

- Regulations define high-level obligations;
- Supervisory Authorities use Standards (national or international) to assess the application of regulation.

<sup>9</sup> <http://www.sans.org/reading-room/whitepapers/legal/overview-sarbanes-oxley-information-security-professional-1426>

<sup>10</sup> Typically there is one or two supervisory authority in addition to the national central bank. Eg., for UK they are Prudential Regulatory Authority (PRA) and Financial Conduct Authority (FCA).

Beyond the international standards cited by all, Member States have developed standards that address more specifically their own needs, e.g.:

- *Minimum Requirements for Risk Management (Mindestanforderungen an das Risikomanagement – The German Federal Financial Supervisory Authority)*

The German Federal Financial Supervisory Authority (BaFin) provides a framework for risk management for German financial institutes. It is based on EU Directive 2004/39/EC.

This framework relates to Senior Management's responsibilities, general requirements for risk management and resources including personnel, systems, technical facilities and related processes as well as contingency plans. It includes references to the IT-Grundschutz Catalogues of the Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik – BSI) and the ISO/IEC 27002.

- *Banking Act (Gesetz über das Kreditwesen): The German Federal Financial Supervisory Authority:*

The German Federal Financial Supervisory Authority (BaFin) refers to the Banking Act (Kreditwesengesetz – KWG) in banking supervision. The Banking Act lays down rules for banks which they have to observe when they are being established and when they are carrying on their business. Rules are designed to enable smooth functioning of the banking system, and it includes top-level description of very basic requirements. For example, the Banking Act states that:

- The credit institution and BaFin shall put in place state-of-the-art measures to safeguard data protection and data security.
- They shall guarantee the confidentiality and integrity of the retrieved and transmitted data.

This state of the art is defined by BaFin in consultation with the Federal Office for Information Security; actual measures are not described in the Banking Act.

- *Swiss National Bank: The National Banking Act 3/2004*

The Swiss National Banking Act obliges the National Bank to oversee systems operating clearing, settlement and other financial instruments. The text applies also to operators that are domiciled abroad, provided that substantial parts of the operation or leading participants are located in Switzerland. The Banking Act states that the National Bank may demand that minimum security requirements are fulfilled.

- *The Finnish Financial Supervisory Authority: Management of operational risk, standard 4.4b*

The supervision standard establishes an obligation for operational risk management in financial organisations. It provides detailed instructions on special subjects such as process management, staff, information and payment systems, information security, continuity planning, and legal risks.

Chapter 6.8 covers payment systems and payment services. There are eight (8) controls that banks "shall adopt". These include payment systems characterisation, means of payment, stating principles for fund transfers in payment systems, ensuring internal control for efficient and secure payment services.



### 3 European Regulatory Landscape

The regulations and standards identified as relevant to the Finance Sector’s Security of IT assets were categorised under a meta-framework for security measures developed during the implementation phase of the telecom package’s Art.13a.<sup>11</sup> The benefits of using this framework are numerous:

- The framework in substance covers most of the security measures and domains already used in worldwide standards and can easily be mapped with them (e.g. ISO, CoBIT, ...);
- It covers most of the areas of concern at this stage;
- It provides a sound and measurable means of comparison between different regulatory models.

The framework is organised in domains and sub-domains. The figure below provides the framework’s skeleton:

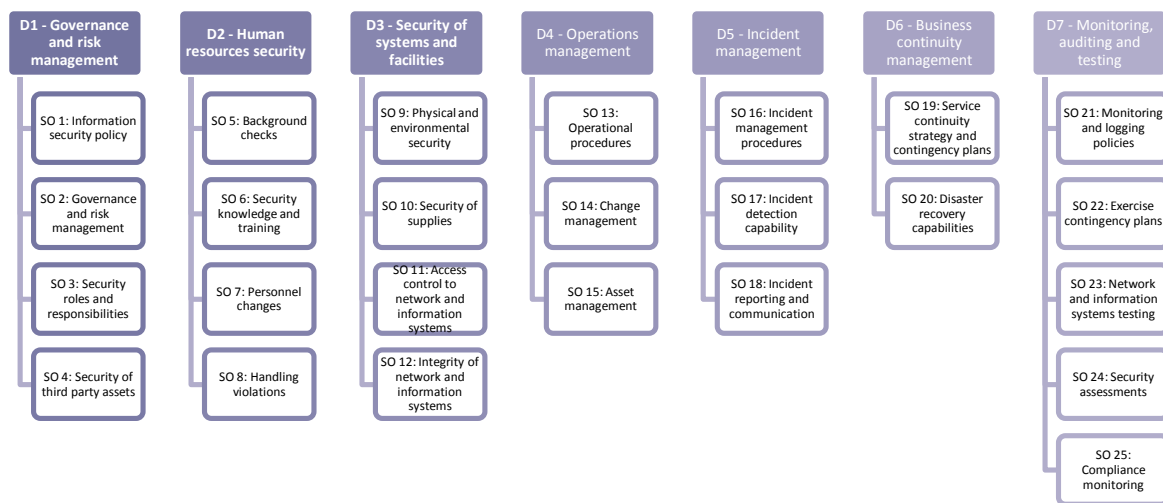


Figure 5: security measures meta-framework

Based on the above framework, several different security strategies were horizontally compared. This revealed which categories are covered by binding regulations and which ones are delegated to voluntary measures or commonly recognised standards.

The information obtained was further merged to identify possible gaps and attract the attention of decision makers.

#### 3.1 Regulations’ provisioning for NIS

Based on the information collected during the initial phase, a representative sample of 8 EU countries was defined and a preliminary analysis was performed in order to understand which category of security measures are typically covered by regulations.

##### 3.1.1 European level

At the European level, the financial supervision is still relatively recent (2011 for EBA, ESMA and EIOPA); it was established as a response to the financial crisis and covers mostly the regulation of financial instruments and practices. These are part of the European System for Financial Supervision

<sup>11</sup> ENISA – Minimum Security Measures – Art.13a of the eComms package

(ESFS), and typically are instruments to equalise national regulations so a financial institution would not competitively benefit from less stringent regulations in one member state or another. Their role in the supervision of the finance sector’s information technology domain is however not their main focus.<sup>12</sup>

*EU Directives overview*

The preliminary identified set of EU regulations had also been analysed in order to identify the topic addressed by EU prescriptions. Regulations are usually rather high level; our analysis attempted to identify both direct references to NIS-related obligations, or obligations which indirectly impact NIS measures and organisations. In cases of indirect impact, the precise reference of the regulatory text in the directive is referenced.

The information analysed is reported in the following table:

Reference	Contents
<i>Proposal for a Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) - COM(2012) 11 final</i>	<ul style="list-style-type: none"> <li>• <b>D1-SO1 Information security policy</b> (Chapter III)</li> <li>• <b>D1-SO3 Security roles and responsibilities</b> (Chapter IV Section 4)</li> <li>• <b>D3-SO12 Integrity of network and information security</b> (Chapter IV Section 1 and 2)</li> <li>• <b>D7-SO24 Security assessment</b> (Chapter IV Section 3)</li> </ul>
<i>Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union - COM(2013) 48 final</i>	<ul style="list-style-type: none"> <li>• <b>D5-SO18 Incident reporting and communication</b></li> <li>• <b>D4-SO13 Operational procedures</b></li> </ul>
<i>Opinion 03/2014 on Personal Data Breach Notification - 693/14/EN WP 213 - Adopted on 25 March 2014 - Article 29 Data Protection Working Party</i>	<ul style="list-style-type: none"> <li>• <b>D5-SO18 Incident reporting and communication</b> (Article 2)</li> </ul>
<i>Financial and Compliance Audit Manual, European Court of Auditors, 2012</i>	<ul style="list-style-type: none"> <li>• <b>D7-SO24 Compliance monitoring</b></li> </ul>
<i>Directive 2004/39/EC on market on financial instruments, 2004</i>	<ul style="list-style-type: none"> <li>• <b>D1-SO1 Information security policy</b></li> </ul>
<i>Directive 2002/58/CE concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communication), 2002</i>	<ul style="list-style-type: none"> <li>• <b>D3-SO11 Access control to network and information systems</b></li> </ul>
<i>Directive 2000/12/EC relating to the taking up and pursuit of the business of credit institutions</i>	<ul style="list-style-type: none"> <li>• <b>D1-SO1 Information security policy</b> (Article 30)</li> </ul>

**Table 1 - European Regulations mapping**

*SecuRePay recommendations*

In October 2013, the European Central Bank (ECB) published the “Recommendations for the security of internet payments”, often referred to as “Secure Pay recommendations”<sup>13</sup>. These requirements directly impact Payment Processors and ecommerce companies.

These include the obligation to ensure:

- regular risk assessments, gap analyses;
- breach/incident monitoring and reporting;
- risk control and mitigation;
- transaction traceability;

<sup>12</sup>

[http://europa.eu/legislation\\_summaries/internal\\_market/single\\_market\\_services/financial\\_services\\_general\\_framework/index\\_en.htm](http://europa.eu/legislation_summaries/internal_market/single_market_services/financial_services_general_framework/index_en.htm)

<sup>13</sup> <https://www.ecb.europa.eu/pub/pdf/other/recommendationssecurityinternetpaymentsoutcomeofpcfinalversionafterpc201301en.pdf>

- customer identification and strong authentication;
- adoption of strong authentication tools delivered to the customer;
- transaction monitoring;
- protection of sensitive transaction data;
- customer/end-user education.

These recommendations are focused on systems security; they impact directly the security governance of payments processors and merchants. Indirectly, they influence the specifications and engineering of future payments means (3D secure, mobile payments, etc.) and increase the criticality of network communications.

#### *Impact of MiFID II / MiFIR*

MiFID II / MiFIR (Directive 2014/65/EU on markets in financial instruments) does not contain any NIS specific measures to be implemented. However, the obligation of transactions reporting have an indirect impact that has been cited by a few respondents: the obligation of traceability for transactions leads, in terms of security, to the requirements that all transactions must be non-repudiable<sup>14</sup>, which also introduce integrity assurance. As a result, stronger authentication mechanisms and complete transaction history is an obligation for all players in the Securities market. Typically, Transaction Reporting and Recordkeeping (MiFIR, recitals 32-36, Articles 24-27; MiFID, Article 66; MiFID II, recitals 52, 57, 71, Article 16) are the main drivers for improved NIS<sup>15</sup>.

Several central banks and supervisors require that financial institutions report the incidents which affect their operations. For example in the UK, the financial institutions are required to report to the relevant authority (BoE, FCA) about operational interruptions of a payment system provider (regardless of the cause of this interruption, which could be, e.g. a cyber-incident). According to respondents, the communication channels used between banks and authorities are “of course adequately secured” but no further details were provided.

The incidence of national regulations on Finance NIS is therefore scattered across many different regulations also at National level.

### **3.1.2 Member States’ approaches and cultural differences**

Following the analysis of the European regulations, the objective was to understand if Member States implemented those directives together with additional requirements.

In the selected countries, the differences are based in the nature of obligations (either Regulatory or Legal). In several Member States, financial institutions are required to report to national authorities many different aspects of their operations (such as operational risks, issues in payment processing or transfers, outsourcing, and so on). This reporting is often specified in detail and leads to recommendations issued by the supervisor to the financial institution. The scope consists of the types of communication channels and the methods of securing them. Also, it is of interest whether financial institutions are required to report various cyber incidents and similar issues to the national authorities.

Based on the information collected, the topics covered during the supervision exercises vary widely in nature and in depth.

<sup>14</sup> [www.linklaters.com/pdfs/mkt/london/MiFID2-Fact-sheet.pdf](http://www.linklaters.com/pdfs/mkt/london/MiFID2-Fact-sheet.pdf)

<sup>15</sup> [http://ec.europa.eu/finance/securities/isd/mifid/index\\_en.htm](http://ec.europa.eu/finance/securities/isd/mifid/index_en.htm)

			BE	FR	DE	IT	NL	PT	ES	UK	EU
D1: Governance and risk management	SO 1	Information security policy		•					•	•	•
	SO 2	Governance and risk management			•	•	•		•		
	SO 3	Security roles and responsibilities			•	•					•
	SO 4	Security of third party assets			•	•	•		•	•	
D2: Human resources security	SO 5	Background checks			•						
	SO 6	Security knowledge and training			•					•	
	SO 7	Personnel changes			•					•	
	SO 8	Handling violations									
D3: Security of systems and facilities	SO 9	Physical and environmental security			•					•	
	SO 10	Security of supplies									
	SO 11	Access control to network and information systems			•	•					•
	SO 12	Integrity of network and information systems			•	•		•	•	•	•
D4: Operations management	SO 13	Operational procedures	•			•				•	•
	SO 14	Change management				•					
	SO 15	Asset management									
D5: Incident management	SO 16	Incident management procedures			•	•			•		
	SO 17	Incident detection capability									
	SO 18	Incident reporting and communication				•			•		•
D6: Business continuity management	SO 19	Service continuity strategy and contingency plans			•	•			•	•	
	SO 20	Disaster recovery capabilities								•	
D7: Monitoring, auditing and testing	SO 21	Monitoring and logging policies			•	•	•	•		•	
	SO 22	Exercise contingency plans									
	SO 23	Network and information systems testing									
	SO 24	Security assessments			•	•	•			•	•
	SO 25	Compliance monitoring									•

Table 2 - Comparative overview of the Information security-related topic addressed at national level

In order to complete the overall landscape, the data was enriched with a column to visually compare the delta of National regulation with EU directives. Typically, Member States should have implemented those directives in National regulations; in other cases, the regulations remain high level and the control that the obligation is fulfilled is performed at the supervisory level.

In addition to the security measures found in the meta-framework we used, we noticed that National regulations frequently addressed additional topics. Those topics are either sub-sector specific (i.e. payments or Finance IS professionals) or they are an extension of financial supervisory rules. The following are noteworthy:

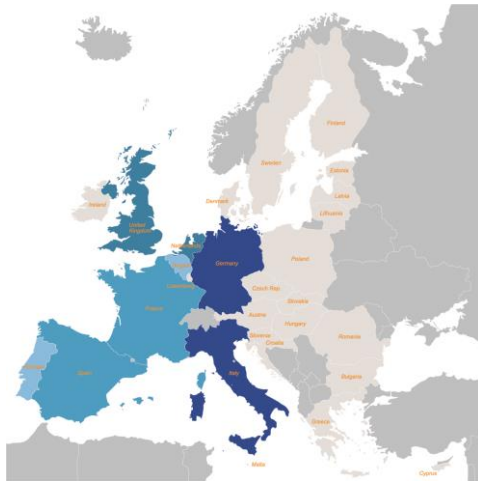
- **Third parties and outsourcing** [e.g. Danish *Executive Order in outsourcing significant areas of activity*, or the Spanish *CIRCULAR 3/2008, de 22 de mayo, del Banco de España, a entidades*

*de crédito, sobre determinación y control de los recursos propios mínimos*]; Various situations concerning the requirements imposed to third parties. For example in Spain no additional contractual requirements were imposed on third parties on information security levels. In Germany, third parties are bound by contract to allow finance sector supervisory authority to audit their activities.

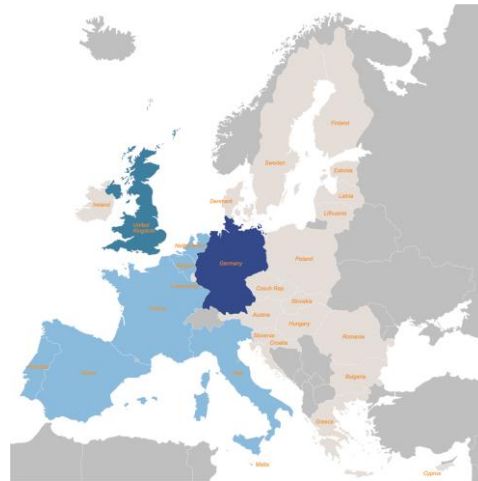
- **Contingency plan and data recovery requirements** [egg. *Mindestanforderungen an das Risikomanagement (MaRisk, Minimum Requirements for Risk Management)*];
- **E-payments security.**

The data collected reveals differences in terms of regulatory coverage depending on the Member States. Darker colours mean that one or several regulation(s)/standards cover from different angles a given domain. In essence, those regulations may cover the same topic, but in different parts of the industry (Retail, Corporate, Payments ...).

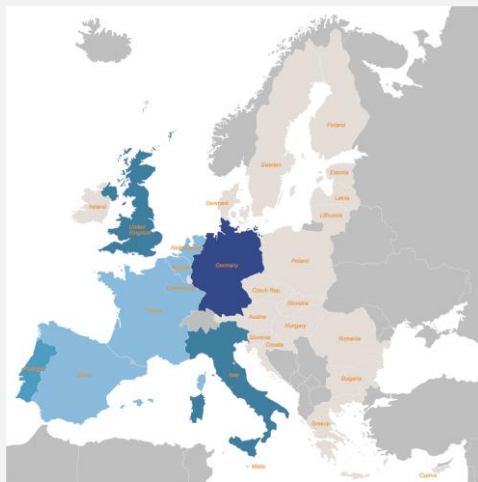
Only the countries in scope are coloured. The others are greyed out.



**Figure 6: D1 - Governance and risk management**



**Figure 7: D2 - Human resources security**



**Figure 8: D3 - Security of systems and facilities**



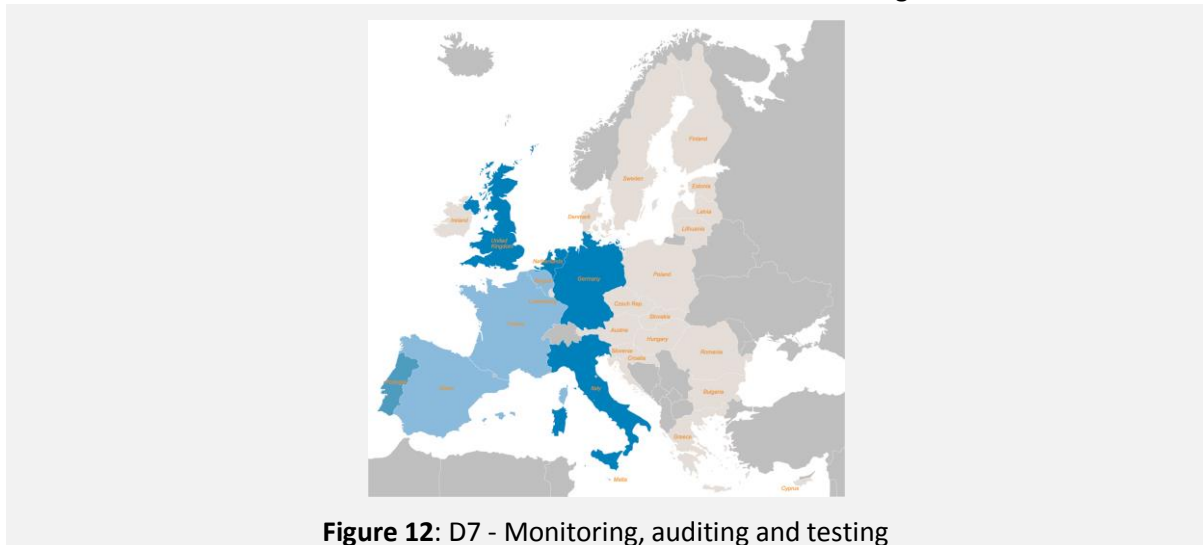
**Figure 9: D4 - Operations management**



**Figure 10:** D5 - Incident management



**Figure 11:** D6 - Business continuity management



**Figure 12:** D7 - Monitoring, auditing and testing

### 3.2 Domains coverage

Based on this preliminary review of ICT security-related regulation and standards for the above described sample of countries, the most recurrent security measures covered at national level appeared to be:

- D1 SO2 Governance and risk management
- D7 SO21 Monitoring and logging policies.

The distribution of the most frequently covered domains in different regulations is reported in the following graph. The Y-axis shows the percentage of Member States from our sample that refer to a given domain.

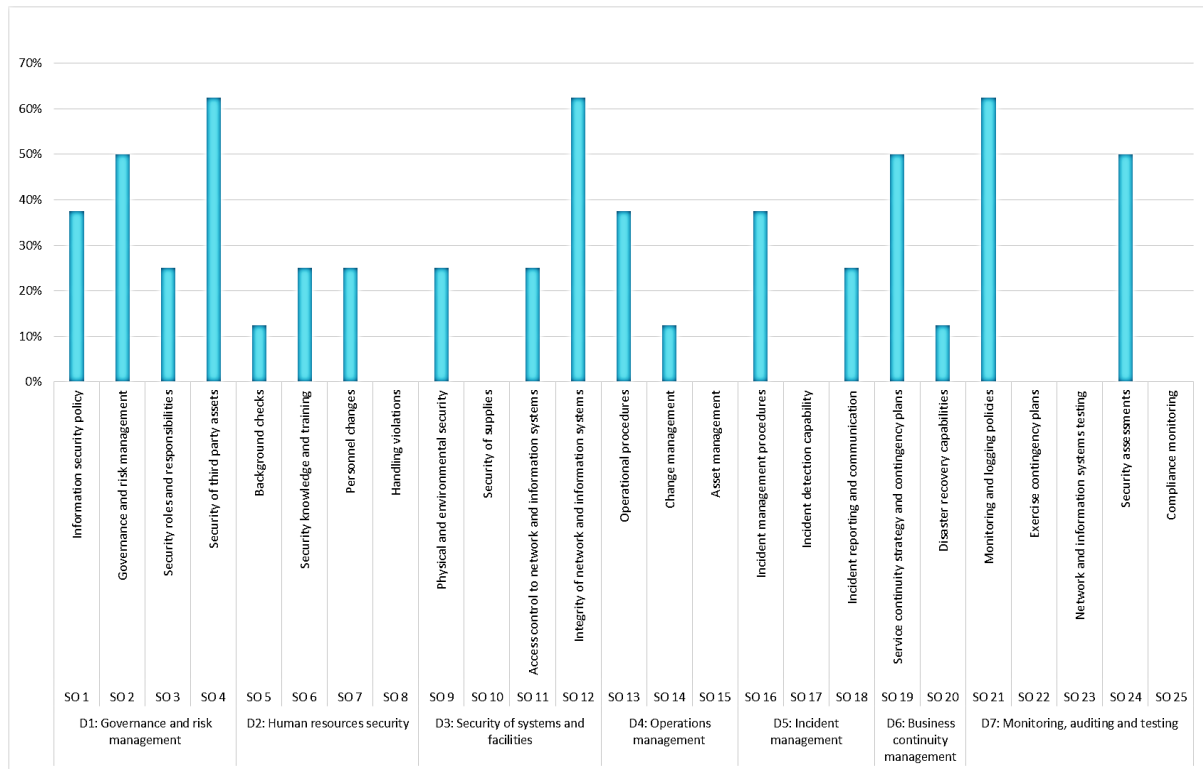


Figure 13 – Security measures recurrence

### 3.2.1 Lack of coverage and emerging trends

Several topics defined remain out of the scope of the regulations. The topics not covered relate to topics which can be qualified as “how” to comply with proper security measures, e.g.:

- Handling Violations [D2.SO8]
- Assets Management [D4.SO15];
- Incident Detection Capability [D5.SO17];
- Exercise Contingency plans [D7.SO22];
- Network and Information Systems testing [D7.SO23];
- Compliance monitoring [D7.SO25].

From this standpoint, the absence of such specifications make sense in the regulatory foundation; laws and implementing laws typically remain at a level of abstraction which provides freedom of action within boundaries.

One aspect, however, is on the verge of becoming more regulated, as the trends indicate: the topic “security of supplies” [D3.SO10] is now on the radar of several member states: this is the case of the Danish *Executive order on IT audit in datacentres owned by financial institutions*. Besides a few major banks which manage IT internally the majority of smaller banks rely on datacentres which are jointly owned and managed by the banks. The regulations dedicated to such shared data centres pertain to requirements and procedures for supervision practices almost exclusively.

This situation might be considered under two different perspectives:

- On one hand, the auditing process is facilitated by having one single service provider to control the information security of all the financial operators. All operators which rely on the same data centre will have a standardised level of security;

- On the other hand, the collection of data and information on a single provider might be a vulnerability for the system; an attack to a single datacentre might impact a number or even all finance operators relying on that single service provider.

Security of supplies is however to be considered as a much broader topic than simply the provisioning of supplies **for** financial institutions; each point of the financial mesh is both receiving and supplying. In this respect, such regulations' scope will be under scrutiny to understand whether new texts adopted address both upwards and downwards Supply Chain Management (SCM).



## 4 Industry's prospect

Often, Industry perceives regulations as yet an additional constraint that they have to comply with; this is a strong dichotomy with the original intent of regulations and standards. The natural step after assessing the regulatory landscape is not intended to increase the depth or scope of such regulations, but to better understand which mechanisms can help the sector altogether to improve their security baseline.

The Industry's concerns are usually orthogonal to the usual scope covered in the Regulatory landscape. This can be easily explained:

- Mature companies already comply with regulatory requirements, and their maturity level allows them to consider further risks;
- Less mature companies are essentially driven by threats and risks and address these in a less proactive manner.

The purpose of studying this dimension is to better understand where the needs are, to define recommendations for future support to industry beyond their usual compliance exercise.

### 4.1 Risks and Challenges

**In general, large international banking groups** demonstrated a good understanding of the Risk Landscape and the available Security schemes. Many companies follow a clear Information Security Management System (ISMS), and adopt Standards and Control frameworks as part of their Security Governance.

Many banks have introduced further good practices especially in the area of IT governance (e.g.: roles and responsibilities; certification to the International Standards like ISO27001 and 22301) and demonstrate a clear information security strategic vision. Security related prescriptions are mostly reported in national regulations or are defined by sector-internal strategies. In some Member States, industry stakeholders publish high-level security and compliance strategies and participate in exercises planned by their Central Bank.

**Medium-sized stakeholders** demonstrate limited top management involvement, limited capacity to be certified against current international standards, and a de-prioritisation of security investments.

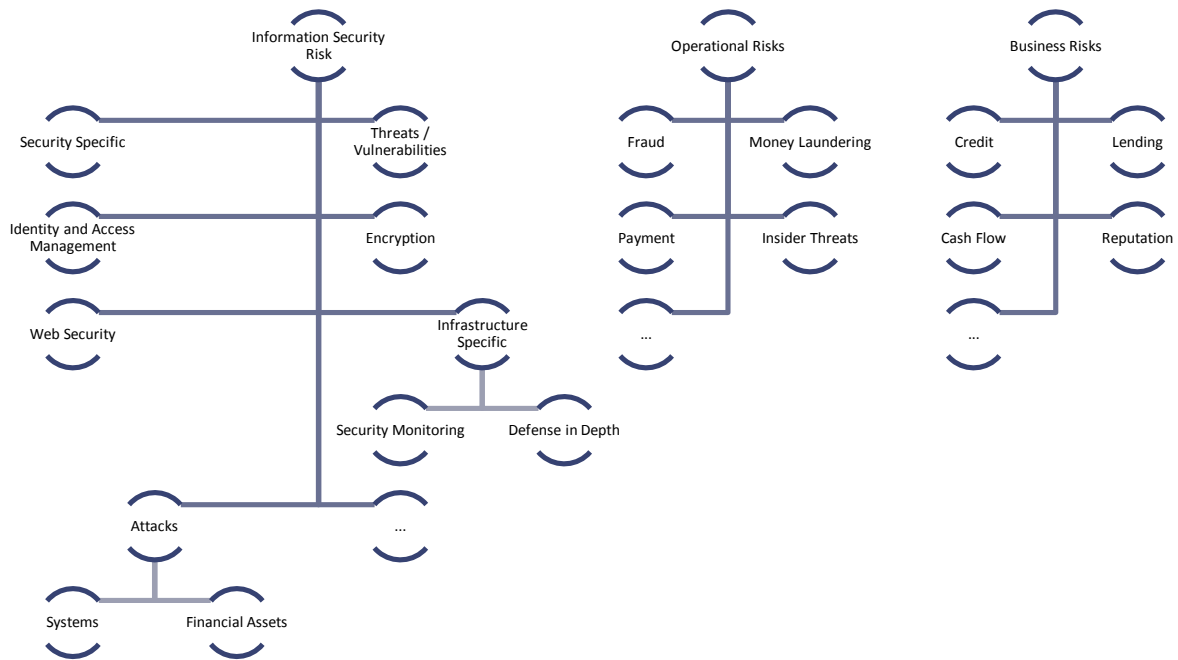
Such difference of situation is not new, it is also not specific to the Finance sector. The aim is to understand where such prospects could impair Financial resilience altogether.

#### *Risk Management Domains*

Typical risk management practices and threats are well known and understood by respondents.

Respondents especially mentioned that "Risk Management" was not NIS-specific, which was later confirmed by literature review. The finance sector manages mainly risk in "sectors", and they make a clear distinction between Financial, Operational and IT risks.

Figure 14 sets the Information Security risk domain in the overall perspective; it expands broadly across all categories.



**Figure 14 – Information security risks in Financial risks landscape**

Typically, NIS therefore belongs to the information risk area despite having a potential impact on the three pillars above mentioned. In the opinion of several respondents, NIS risk is a horizontal risk that pertains to all the others:

- Poor input controls may lead to fraud risks;
- Insider threats were reported by many as a “hot topic” in several member states, which could be both categorised under “Finance risk” or “Information Security Risk”;
- Payment being almost entirely digital nowadays also relates more to an Information security risk than a purely financial risk;
- Etc.

### *Security governance*

At present, the Security Governance and the NIS Risk management are therefore typically part of the Technology divisions.

Interviews revealed that in many cases, top management is only formally involved once a year, as this constitutes in many Member States a binding prescription. Respondents underlined that, as the CISO often reports to the CIO, both budget lines conflict in times of ICT budget restrictions. In particular, CISOs suggested that the **Security budget (Safety, ICT Security, and Security Continuity) should be separated from all other budgets** and be approved directly by the Board of Directors. In addition, the Board of Directors should appoint one of its members as a delegate for the company’s security.

In light of these considerations, this topic should possibly be further discussed and pragmatic solutions be presented in the light of the upcoming directives (NIS and PSD2).

### *Security assessments*

The replies collected concerning the usual security assessment practices were in line with the requirements usually found in international standards. Several statements support this observation, e.g.: «CISO defines policies, structures and techniques ...», « Vulnerability analysis is carried out every year...»; «Risk Assessment and Business Impact Analysis at least annually»; «all security incidents are

logged, classified, analysed, and discussed with internal audit and at the periodical management's review meeting».

The answers collected on the "systematic security assessments" topic suggest that most actors operate in an adequate way fulfilling all regulatory and standards requirements. Other aspects of the feedback received also suggest that the approaches implemented, the binding prescriptions, the voluntary measures / strategies aim at enhancing information security both globally and in-depth.

#### 4.1.1 Mitigation limitations

##### *Three dimensions of complexity*

The structure of the finance sector is complex overall. Threats and potential weaknesses vary according to the business type and the security model adopted: for instance, Investment banks or high frequency trading (HFT) might face difficulty in ensuring the continuous and balanced provision of information security in their activities.

Customer-facing operators might be more exposed to risks related with the rapidly evolving technological environment. On the other hand, while the technological environment is rapidly changing, the business and financial services landscape is also rapidly evolving (e.g. new competitors, emerging market models, etc.). The combination of these trends influence the degree of complexity of the financial sector itself and of the information security management requirements.

##### *Supply chain in security measures*

The key issue reported by participants during our interview process relates to the dichotomy between the security objectives / obligations of their company, and the fact that many aspects are totally under 3rd party control: this remark applies both to messages / networks service providers. Likewise this issue seems to extend to other supply areas: Banks are responsible for instance for the protection against data leaks, but cannot always configure entirely the devices they purchase (mobile phones, tablets, laptops, servers, operating systems, etc.).

Another issue was reported several times and is noteworthy: the need for including the entire **supply chain as part of principle security measures**. Respondents mentioned several outsourcing contracts with major providers (e.g. Telecom Operators, SWIFT, IBM, Microsoft, ...). They perceived that such world-class providers implement and maintain satisfactory security levels on their services.

Smaller providers are also used, and respondents felt that these might be more subject to breaches; such attacks might be aimed those weaker links as a way to enter the target victim.

Last but not least, when required, respondents mentioned many international standards (ISO 27001, 31000, 22301) but none cited ISO 28000, confirming that supply chain security requires more attention.

##### *Privacy considerations*

Current technology allows both private companies and public authorities to use personal data on an unprecedented scale in order to pursue their activities. Individuals increasingly make personal information available publicly and globally. Because of the close relation between information

technology's evolution and economic development<sup>16</sup>, personal data protection play a central role in the Digital Agenda for Europe, and more generally in the Europe 2020 Strategy. A “*personal data breach*” is defined by Directive 2002/58/EC in Article 2 as “*a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service in the Community*”<sup>17</sup>.

#### *Skills shortage*

Finally, although risk and security issues are very well understood among operators, many issues still remain. The finance sector operators manifest a positive tendency to invest in IT security, with a growth in the amounts invested varying from +6% to +10% in the past years. Nevertheless, a lack of skilled and competence staffing persists in the field of IT security in the finance sector, which leads many finance operators to contract external experts or consultancy companies to secure their infrastructures and communications. Such security functions should however be considered more critical since those experts are requested to sign non-disclosure agreements (NDAs).

## **4.2 Desirable features**

The NIS management instruments mentioned are numerous in the sector, and many of them expressed limited concerns related to their ability to manage an adequate security level. In some cases, a few of them hoped for:

- Company cultural change to integrate more future security insights;
- Improved corporate NIS awareness and involvement;
- Consolidated standards and guidelines for implementing sustainable security strategies;
- Voluntary NIS exercises both at national or European level, with the inclusion of their supply chain.

The first topics may be addressed by additional supervisory requirements, in the member states where NIS governance is covered by the law. In the others, raising the awareness on such issues may be a possible alternative.

The two following topics (NIS guidance and cooperation) are further detailed below:

- *From Compliance to Sustainable Security Objectives*

The finance sector, overall, is perceived as being a “state of the art” implementation of sustainable security measures in almost all areas (e.g. Web Banking security, internal security procedures). In most cases, the compliance to Supervisors’ requirements comes usually as an addition to high-level regulations and is a compliance exercise.

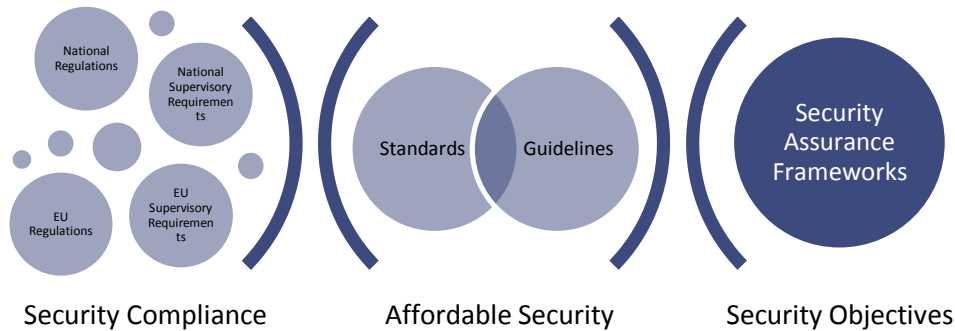
However, Supervisory requirements on Information Security differ widely from one country to another and the compliance exercise can become extremely complex. Unlike business areas –where finance instruments are already supervised under the Single Supervisory Mechanism (SSM)- the supervision convergence for network and information security is still a work in progress. Additionally, Financial Services that operate worldwide are also bound by foreign legislation. This compliance overhaul is increased when IT Infrastructures are either outsourced or physically reside under remote

---

<sup>16</sup> DORANTES C., KO M., “Impact of Information security breaches on financial performances of the breached firm: an empirical investigation”, in *Journal of Information Technology Management*, Vol. XVII, n.2, 2006; PONEMON INSTITUTE, *Ponemon Study Shows the Cost of a Data Breach Continues to Increase*, 2012.

<sup>17</sup> Opinion 693/14/EN WP 213

legislations: the use of Cloud Computing creates much supervisory and compliance concerns. Many respondents also related that they are rarely fully aware of all the implications and impact of regulatory requirements; they felt these were scattered across several different texts, and that a single implementation guideline would be precious (See *Figure 15*).



**Figure 15 - from compliance to security objectives**

Furthermore, current regulations were criticised for considering mostly the prevention of “Financial Incidents”. The risks arising from information security, data confidentiality or business continuity could be encompassed as critical component of the financial stability. This reveals a demand for assessing the financial system’s resilience globally; a combined Business/IT stress-testing was also advocated at large scale.

- *Cross Sector / Cross Border Cooperation opportunity*

The extra-mile to enhanced security and resilience was recommended to be approached using self-commitment and cooperation, possibly supported by the guidance of National IT Supervisors. Furthermore, since Regulation should establish principles rather than specific measures, Interviewees felt that recommendations should not lead to strengthen regulation as a result. Self-commitment to guidelines and standards is perceived as a practical and pragmatic method. Such guidance would benefit greatly to smaller institutions which do not face the same challenges as larger ones.

Global European cooperation and Good Practices sharing could allow a better understanding of the Risks and Security challenges faced by the Finance Sector. Any means of cooperation should include the relevant stakeholders from regulators, banks, system and service providers, clearing houses, and other relevant parties.

- *Contingency planning and exercises*

A majority of respondents stressed the importance of contingency plans’ testing recurrence. Besides being able to demonstrate that information security is managed, and that contingency plans are established, there is a need to demonstrate its periodical testing and update. Respondents suggested that an optimal recurrence for such exercises would need to follow a two-fold principle:

1. contingency plans testing is requested at least once a year, although for very critical components and infrastructures it would be even most appropriate to having it test twice a year;
2. contingency plans testing is necessary each time major changes occur in the management structure or in the physical infrastructure: this helps to ensure that the plan is consistent to the changed conditions are eventually appropriately updated.

In a few Member States, operators are required to periodically test their contingency plans, and also to develop scenarios in cooperation with their partners and service providers to guarantee that the entire supply chain is appropriately tested.

Respondents mentioned the fact that finance sector operators might be required to comply to regulations related to critical infrastructure security (egg. in the case of Spain, where selected major financial operator are requested to comply with the requirements of the *Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas*).

This approach, while it improves practical security levels, demands additional compliance efforts from finance sector operators. These efforts might required guidance by specialised Government bodies or CERTs.

## 5 Recommendations

Based on the information collected and reported a number of desirable measures, tools and objectives can be formulated in the field of Information Security in the finance sector:

- A European Security Guidebook: the **definition of a common set of guidelines** would represent a possible solution for the implementation of common operative security standards rather than defining service-level regulations. Among finance sector operators, standards appear to be frequently used to ensure both prevention, detection and response to security concerns. In addition, common guidelines on how to assess the cost-benefits of Information Security investments and how to effectively involve top management in security investment decisions is key;
- Supply Chain Security: Operators could find several benefits in implementing **risk transparency** between them and their immediate operational circle.
- Security Intelligence: **International cooperation of finance sector operators** might be the most effective approach in defining a common set of indications. It could ensure both a consistent level of technicality on the elaborated guidelines and an appropriate “operator-friendly” approach to realistic security measures. Moreover, cooperative occasions could potentially include regular NIS stress-tests in the finance-sector;

The figure below summarises this three pillars approach and their desired effect:

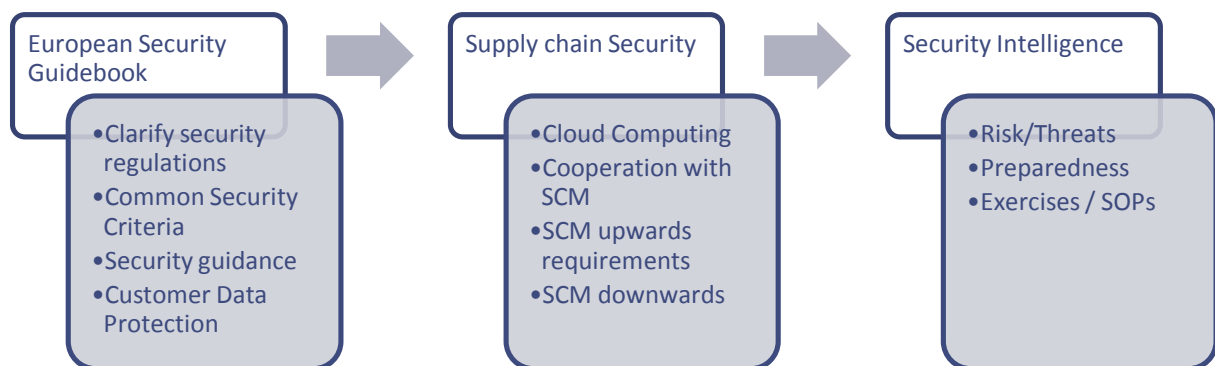


Figure 16 - Recommendations structure

Those objectives are translated into recommendations below.

*1. Establish a European NIS guidebook*

This guidebook should contain useful guidance for CISOs of the Finance sector, independent from the size of their company, which comprehends:

- A clear set of security measures, aligned with National standards used by Supervisors;
- An evaluation framework.

Recommendation: ENISA will support EBA in building a guidebook on horizontal, pan-European security measures.

This guidebook would by no means need to be mandatory; it should however be an authoritative source for good practices and recommendations. For instance, it would cast in stone the need for a separate executive management line between CISO and CTO/CIOs, in order to secure funding for NIS matters, as suggested by many respondents.

ENISA proposes to consider the Security domains used in Chapter 3 to evaluate the scope of regulations in the Member States. Those seven domains can be studied and discussed, and measures be defined only if there is a rationale to do so.

*2. Enable systematic cooperation between the Finance Sector and their supply chain*

In many cases, respondents mentioned that they were liable for several security aspects that were outsourced and outside of their control. While contractually they are allowed to perform security assessments for these outsourced contracts, they felt that the inclusion of their supply chain in supervision frameworks could address several issues. However, these aspects need to be defined comprehensively.

Recommendation: ENISA should develop a Good Practice Guide based on Industry's input on:

- Extension of NIS Guidebook to Supply Chain (upwards and downwards);
- Existing NIS standards and baselines.

ENISA will support the identification of specific issues in the supply chain's NIS.

*3. The case for Cloud Computing*

As the European Commission encourages the European companies to use Cloud Computing to increase their mobility and resilience, the Finance sector will be likely to request that extra security guarantees are given so their data and processing remain safe (or even safer).

Recommendation: EBA and ENISA should define the conditions for adoption of Cloud-based services and applications in the Finance sector. The special case of services already used by the Finance sector which are cloud-based are identified and that they can apply by extension the measures contained in existing supervisory frameworks.

*4. Stress tests and global security intelligence*

The objective and scope of security intelligence is to provision for extreme NIS issues, or even issues qualified as "Unknown unknowns".

Those stress tests' purpose would be to evaluate the maturity level of the Finance-Sector when compared against the NIS Guidebook; instead of performing a checklist audit, the stress test would be based on a realistic incident scenario to which participants would be able to voluntarily participate. ENISA would support extensively those tests.





The objective is therefore to improve the efficiency of security measures by testing them in fictitious scenarios (i.e. exercises).

Recommendation: ENISA should support the ECB and the ESFS (EBA, ESMA, EIOPA) to organise regular and voluntary NIS stress tests in the Finance sector.

The results of the stress tests will help to identify global and structural NIS weaknesses. They will be anonymised and key conclusions circulated after the test among participants.

## References

1. Deloitte, Financial Sector Professionals (PSF) in Luxembourg. At the heart of regulatory and tax environments, 2012
2. BISOGNI F., CAVALLINI S., TROCCHIO S., "Cybersecurity at European Level: The Role of Information Availability", The Economics of Cybersecurity, First quarter 2001, No. 81, edited by Communications & Strategies, March 2011
3. CAMP, L. J., "The state of economics of information security", I/S A journal of law and policy, 2(2), Pag. 189 - 205. 2006
4. GLAESSNER T., KELLERMANN T., MC NEVIN VALERIE, "Electronic Security: Risk Mitigation in Financial Transactions", Public Policy Issues
5. Verizon, 2012 Data Breaches Investigation Report, 2012
6. European Central Bank, The Payment System, 2010
7. ICAEW Corporate Finance Faculty, HM Government, Cybersecurity in Corporate Finance, 2014
8. Oxera, Methodology for monitoring prices, costs and volumes of trading and post trading activities, MARKT/2006/14/G, 2007
9. FSA, Data Security in Financial Services. Firms control to prevent data loss by their employees and third-party suppliers, 2008
10. GARG A., CURTIS J., HALPER H., "Quantifying the financial impact of IT security breaches", in Information Management & Computer Security, Vol. 11 Iss: 2, 2003AIZOMAI M., AIFAYYADH B., JØSANG A., McCULLAGH A. "An experimental investigation of the usability of transaction authorization in online bank security systems", in AISC '08 Proceedings of the sixth Australasian conference on Information security, Volume 81, 2008
11. KESAR S., "Knowledge management within information security: the case of Barings Bank", in International Journal of Business Information Systems, Vol.3, n.6, 2008
12. MACCARTHY M., "Information Security Policy in the U.S. Retail Payments Industry", in Stanford Technology Law Review, 2011
13. VATANASOMBUTA B., IGBARIAB M., STYLIANOUC A.C., RODGERSD W., "Information systems continuance intention of web-based applications customers: The case of online banking", in Information & Management, Vol. 45, Issue 7, November 2008

## Related ENISA papers

1. Proposal for One Security Framework for Articles 4 and 13a, 2013
2. Recommendations for a methodology of the assessment of severity of personal data breaches, 2013
3. Eid Authentication methods in e-Finance and e-Payment services – Current practices and Recommendations, 2013
4. Securing personal data in the context of data retention, 2013
5. Schemes for auditing security measures, 2013

## Legislation

1. EU – Data Protection Directive 95/46/EC <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML>
2. EU – Regulation 260/2012 (Business requirements for credit transfers and direct debits) <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:094:0022:0037:En:PDF>
3. EU – Investment Services Directive – Markets in Financial Instruments Directive (MiFID) 10/2010 [http://ec.europa.eu/internal\\_market/securities/isd/mifid/index\\_en.htm](http://ec.europa.eu/internal_market/securities/isd/mifid/index_en.htm)

4. European Central Bank: TARGET2-Securities User Requirements 6/2012  
[http://www.bde.es/f/webbde/SPA/sispago/t2/URD\\_v5.2.pdf](http://www.bde.es/f/webbde/SPA/sispago/t2/URD_v5.2.pdf)
5. German Federal Financial Supervisory Authority: Banking Act  
[http://www.bafin.de/SharedDocs/Downloads/EN/Aufsichtsrecht/dl\\_kwg\\_en.pdf?blob=publicationFile](http://www.bafin.de/SharedDocs/Downloads/EN/Aufsichtsrecht/dl_kwg_en.pdf?blob=publicationFile)
6. German Federal Financial Supervisory Authority: Minimum Requirements for Risk Management  
[http://www.bafin.de/SharedDocs/Downloads/EN/Rundschreiben/dl\\_rs\\_0915\\_ba\\_marisk.pdf?blob=publicationFile](http://www.bafin.de/SharedDocs/Downloads/EN/Rundschreiben/dl_rs_0915_ba_marisk.pdf?blob=publicationFile)
7. The Swiss National Bank: Federal Act on the Swiss National Bank.  
<http://www.admin.ch/ch/e/rs/9/951.11.en.pdf>
8. Finland – Management of operational risk, standard 4.4b *Finnish Financial Supervisory Authority*, 3/2004  
[http://www.finanssivalvonta.fi/en/Regulation/Regulations/Financial\\_sector/4\\_Capital\\_adequacy\\_and\\_risk\\_management/Documents/4.4b.std4.pdf](http://www.finanssivalvonta.fi/en/Regulation/Regulations/Financial_sector/4_Capital_adequacy_and_risk_management/Documents/4.4b.std4.pdf)
9. Finland – The Credit Institutions Act (LLL 121/2007) [Finnish]  
<http://www.finlex.fi/fi/laki/ajantasa/2007/20070121>
10. Finland – Law for monitoring Financial and Insurance operators (699/2004) [Finnish]  
<http://finlex.fi/fi/laki/ajantasa/2004/20040699>
11. Finland – Corporate governance and business activity Finnish Financial Supervisory Authority, 9/2013  
[http://www.finanssivalvonta.fi/en/Regulation/Regulations/Financial\\_sector/1\\_Corporate\\_governance\\_and\\_business\\_activity/Pages/Default.aspx](http://www.finanssivalvonta.fi/en/Regulation/Regulations/Financial_sector/1_Corporate_governance_and_business_activity/Pages/Default.aspx)
12. Finland – Financial Supervisory Authority’s regulation and guidelines: 1/2012 Outsourcing [Finnish]  
[http://www.finanssivalvonta.fi/fi/Saantely/Maarayskokoelma/Uusi/Documents/01\\_2012.M2.pdf](http://www.finanssivalvonta.fi/fi/Saantely/Maarayskokoelma/Uusi/Documents/01_2012.M2.pdf)
13. Finland – Guidelines for acting in national emergency 9/002/2005 [Finnish] 3.10.2005 Donor 9/002/2005 <http://www.finlex.fi/data/normit/23938-VVVpaatosyhtio.pdf>
14. Information Guide for TARGET2 users Version 4.0. 11/2010.  
[http://www.ecb.europa.eu/paym/t2/shared/pdf/infoguide\\_V4\\_0.pdf](http://www.ecb.europa.eu/paym/t2/shared/pdf/infoguide_V4_0.pdf)

## Standards

1. ISO/IEC 20 000
2. ISO27001:2005
3. Information Technology Infrastructure Library (ITIL)
4. International Standard for Assurance Engagements (ISAE) No. 3402
5. Payment Card Industry Data Security Standard (PCI DSS)

**Annex A: Figures**

Figure 1 – Taxonomy of stakeholders.....8

Figure 2 - European Finance communications overview .....11

Figure 3 - Network types .....12

Figure 4 - NIS drivers .....14

Figure 5: security measures meta-framework .....17

Figure 6: D1 - Governance and risk management .....21

Figure 7: D2 - Human resources security .....21

Figure 8: D3 - Security of systems and facilities .....21

**Figure 9:** D4 - Operations management .....21

Figure 10: D5 - Incident management .....22

**Figure 11:** D6 - Business continuity management.....22

Figure 12: D7 - Monitoring, auditing and testing .....22

Figure 13 – Security measures recurrence.....23

Figure 14 – Information security risks in Financial risks landscape .....26

Figure 15 - from compliance to security objectives.....29

Figure 16 - Recommendations structure .....31

Figure 17 – Workflow overview .....43

Figure 18 –Interview - Section 1.....44

**Annex B: Tables**

Table 1 - European Regulations mapping .....18

Table 2 - Comparative overview of the Information security-related topic addressed at national level .....20

Table 3 - EU regulators .....37

## Annex C: Regulators

### C.1 European Authorities

At European level, Authorities cover the areas of the Finance System. The table below summarises the scope of each of them:

ESFS (European System of Financial Supervision)	Competences and functions
<b>ECB</b> <i>European Central Bank</i>	The central bank for Europe's single currency is mainly committed to maintain price stability in the euro area. The ECB is expected to have an active role concerning banking supervision under the upcoming <i>Single Supervisory Mechanism</i> .
<b>EBA</b> <i>European Banking Authority</i>	It is an independent EU Authority responsible for prudential regulation and supervisor of the European banking sector. Its main aim is to provide a single set of harmonised prudential rules for financial institutions throughout the EU.
<b>EIOPA</b> <i>European Insurance and Occupational Pensions Authority</i>	<i>"EIOPA is part of the European System of Financial Supervision consisting of three European Supervisory Authorities and the European Systemic Risk Board. It is an independent advisory body to the European Parliament, the Council of the European Union and the European Commission".</i>  <i>"EIOPA's core responsibilities are to support the stability of the financial system, transparency of markets and financial products as well as the protection of insurance policyholders, pension scheme members and beneficiaries."</i>
<b>ESMA</b> <i>European Security and Markets Authority</i>	ESMA is an independent EU Authority committed to contribute to ensure the integrity, transparency, efficiency and functioning of the securities markets, particularly enhancing investor protection and by fostering supervision convergence at EU level.

Table 3 - EU regulators

The supervision of the IT is typically a national competence. European authorities however influence the national practices: a single market requires a single rule book adoption which EBA typically supports. NIS Supervisory rules are also considered and discussed during EBA's IT supervisory boards.

### C.2 National Authorities

Based on the information preliminary collected at national level, regulators' mission is typically twofold: regulation and supervision. In some cases, they support the implementation of specific, one-off regulations. In the EU28, the following is generally observed:

- National Central Banks (NCB) are usually in charge of regulations. They are supported by the relevant ministries or technical committees.
- Supervision is often the responsibility of a specific branch of the NCB or may be delegated to other institutions.

Such setup however depends greatly on the size of the Member State. In some Member States, some functions may be merged or organised differently. The initial interviews performed confirmed the preliminary hypothesised scheme of roles and competences: Supervisors and Regulators are often hosted within the same entity. Three different models exist, and their function can either be:

- Part of a dedicated department of the National Central Bank, as in the case of Banco de Span Directorate General Banking Supervision, or in the case of Banca d'Italia;
- A shared responsibility between the National Central Bank and an Agency, which is the case for BaFin (*Bundesanstalt für Finanzdienstleistungsaufsicht*) working in close cooperation with the Deutsche Bundesbank.

- Be performed autonomously by a dedicated institution, as in the case of the Danish Finanstilsynet.

The organisation within one country does however not affect the principle: both Regulation and Supervision are typically covered in every Member State.

### C.3 Other Relevant Publications

Text	Mapping
<b>Target2 Securities - User Requirements Chapter 18 Information Security Requirements</b> , European Central Bank, 2007	<ul style="list-style-type: none"> <li>• <b>D1-SO1 Information security policy (18.2)</b></li> <li>• <b>D1-SO3 Security roles and responsibilities (18.3.1.3)</b></li> <li>• <b>D3-SO11 Access control to network and information systems (18.3.1.4 and 18.8)</b></li> <li>• <b>D7-SO24 Security assessment (18.3.1.8)</b></li> <li>• <b>D1-SO4 Security of third party assets (18.3.2)</b></li> <li>• <b>D2 Human resources security (18.5)</b></li> <li>• <b>D3-SO9 Physical and environmental security (18.6)</b></li> <li>• <b>D5 Incident management (18.10)</b></li> <li>• <b>D6 Business continuity management (18.11)</b></li> <li>• <b>D7-SO25 Compliance monitoring (18.12)</b></li> </ul>
<b>Basel II - International Convergence of Capital Measurements and Capital Standards</b> , Basel Committee on Banking Supervision, 2006	<ul style="list-style-type: none"> <li>• <b>D4-SO13 Operational procedure (V. Operational risks)</b></li> </ul>

### C.4 Professional Associations

Professional Associations are worth mentioning as they often constitute a representation of the European Finance Sector to the Authorities. They are therefore typically within the network reach of public decision makers, they voice the interests of the Industry on the verge of new discussions on legislation matters.

Beyond this type of activities, associations are also setup with other objectives: Information Sharing, Security Awareness Raising, Education, Professional Training, Conferences, Analytics, etc.

Many European-based associations exist; a number of associations or non-profit organisations have also arrived from other continents and develop similar activities both with European and non-European members.

To complete the overview of the framework of organizations operating in the finance sector, some of the European and international professional associations deserved to be mentioned:

Association	Profile
<b>EACB</b> <i>European Association of Co-operative Banks</i>	This association commits to “represent, promote and defend the common interest of its member institutions concerning banking and co-operative legislation. It acts as official spokesperson for its members toward European institutions”.
<b>EACH</b> <i>European Association of Central Counterparty Clearing Houses</i>	Established as a Belgian not-for-profit organization, it “represents central counterparty clearing houses in Europe. Its representatives actively participates in European public discussions and consultations, and help member CCPs to agree appropriate standards and guidelines”.
<b>EBF</b> <i>European Banking Federation</i>	Represents “the interest of European banks in front of European institutions. It constitutes for its members a forum where best practices are exchanged, legislative proposals are debated and common positions adopted.”

Association	Profile
<b>EPC</b> <i>European Central Securities Depositories Association</i>	<p>“Supports and promotes the Single Euro Payments Area (SEPA). The EPC develops payment schemes and frameworks which help to realise the integrated euro payments market. In particular, the EPC defines common positions for the cooperative space of payment services.”</p>
<b>ECSDA</b> <i>European Central Securities Depositories Association</i>	<p>Represents “central securities depositories (CSDs) across 37 European countries. It aims at promoting the dialogue between the CSD community, European public authorities and all other stakeholders with the final aim to improve the regulatory framework for clearing and settlement”.</p>
<b>EFAMA</b> <i>European Fund and Asset Management Association</i>	<p>EFAMA represents the European investment management industry. It “promotes governance standards, enhances the smooth functioning of the European single market for investment management, strengthens the competitiveness of the industry and promotes industry visibility at international level.”</p>
<b>ESBG</b> <i>European Saving Banks Group</i>	<p>It is a European banking association that “represents the industry interests in front of EU institutions, with a specific focus on retail banking issues. It works as a research centre on legislative issues, and cooperation forum among participants members.”</p>
<b>FESE</b> <i>Federation of European Securities Exchanges</i>	<p>A trade association representing 41 public regulated markets at European level. Its objectives are to “foster the competitiveness of European exchanges, to promote the public recognition of the exchanges and their contribution to the European and global economy, and to allow the debate on capital markets.”</p>

## Annex D: Terminology

Following terms and definitions are used throughout this report.

Term / Abbreviation	Definition / Description
Clearing	Term used for all activities from the time a commitment is made for a transaction until it is settled. E.g., the payment instruction is sent between banks but no money is exchanged yet.
Settlement	Process of finishing the transaction, i.e., delivering securities. E.g. moving money to balance out the payment instruction.
ACH	Automated Clearing House
ABE-EBA	EURO BANKING ASSOCIATION ( <a href="https://www.abe-eba.eu/">https://www.abe-eba.eu/</a> )
EBA	European Banking Authority ( <a href="http://www.eba.europa.eu/">http://www.eba.europa.eu/</a> )  EBA's main aims are to ensure that the rules applicable to credit institutions and the competent authorities that supervise them, as set out in the specific legislation establishing our scope of action, are adequately implemented and applied to preserve financial stability and to ensure confidence in the financial system as well as sufficient protection for consumers of financial services. Payment issues are only relevant insofar as they are not covered by existing legislation but serve to ensure "the effective and consistent application of those acts" (see Article 1 of the Regulation 716/2009 establish the EBA).
EBA CLEARING	Covers 63 shareholder banks and, through its EURO1, STEP1 and STEP2 systems, offers both high-value and low-value clearing and settlement services to a wide community of banks in the European Union. ( <a href="https://www.ebaclearing.eu/">https://www.ebaclearing.eu/</a> )
EBF-FBE	European Banking Federation ( <a href="http://www.ebf-fbe.eu/">http://www.ebf-fbe.eu/</a> )
EBICS	Electronic Banking Internet Communication Standard ( <a href="http://www.ebics.org/">http://www.ebics.org/</a> )
EPC	European Payments Council ( <a href="http://www.europeanpaymentscouncil.eu/">http://www.europeanpaymentscouncil.eu/</a> ) The EPC represents the industry to the EU Institutions, and coordinates the European banking industry in relation to payments. The EPC supports the development of the payment schemes and frameworks helping to promote SEPA
EU	European Union



Term / Abbreviation	Definition / Description
Finance Pine	<p>A communications service provided by SIX.</p> <p>It enables access to the payment, transaction and financial information of SIX companies separately from the Internet through Managed MPLS-VPN (Multiprotocol Label Switching-Virtual Private Network) and represents an alternative to the Internet through guaranteed Service Level Agreements, bandwidth and privacy. Finance IPNet facilitates single or redundant communications connections with guaranteed availability (end-customer connections), optionally through one or more carriers.</p>
FIRST	<p>Forum of Incident Response and Security Teams (<a href="http://www.first.org/">http://www.first.org/</a>)</p>
IBASEC	<p>Interbank security system</p> <p>IBASEC is used for the SIC and euroSIC payment systems as well as for the securities clearing and settlement system SECOM at SIX. Within the framework of the Swiss financial centre infrastructure, the Swiss Value Chain, it guarantees the unadulterated transmission of messages, ensures their unambiguousness as well as the indisputable dispatch and receipt thereof. It is thereby impossible to read messages during their transmission.</p>
NIS	<p>Network and Information Security</p>
PCI DSS	<p>Payment Card Industry Data Security Standard  (<a href="https://www.pcisecuritystandards.org/security_standards/">https://www.pcisecuritystandards.org/security_standards/</a>)</p>
RTGS	<p>Real-time Gross Settlement (system)</p> <p>indicates a specific type of payment transfer system, in which processing and payment settlement are continuously handled in real-time on a gross basis – thus, primarily in individual transactions.</p>
SEPA	<p>Single European Payment Area</p> <p>SEPA is a European Union (EU) integration initiative in the area of payments</p>

Term / Abbreviation	Definition / Description
SIC	<p>SIX Interbank Clearing is a SIX Group company. It is in charge of the RTGS operational aspects in assignment from the system manager and the financial institution. In this function it contributes to monitoring and controlling. Computer centre activities are assigned to SIX Group Services, also a SIX Group company.</p> <p>SIC (RTGS)</p> <p>Refers to the autonomous instance of the payment transfer system conducted in the currency CHF. SIC is a registered trademark.</p> <p>euroSIC (RTGS)</p> <p>Refers to the autonomous instance of the payment transfer system conducted in the currency EUR (domestic as well as cross border. Cross border as SEPA Credit Transfer). euroSIC is a registered trademark.</p> <p>A System manager Controls and monitors the (payment) traffic of its RTGS instance. Currently, this is the Swiss National Bank (SNB) for the instance SIC and the SECB Swiss Euro Clearing Bank GmbH in Frankfurt am Main (SECB) for the instance euroSIC.</p>
SWIFT	<p>Society for Worldwide Interbank Financial Telecommunication (<a href="http://www.swift.com/index.page?lang=en">http://www.swift.com/index.page?lang=en</a>)</p>
SWIFTnet	<p>An advanced IP-based messaging platform, operated by SWIFT. SWIFTnet comprises services and products that enable customers to communicate mission-critical financial information and transactional data securely and reliably.</p>
TARGET2	<p>Trans-European Automated Real-time Gross Settlement Express Transfer System (2<sup>nd</sup> generation)</p>
UN/EDIFACT	<p>United Nations rules for Electronic Data Interchange for Administration, Commerce and Transport <a href="http://www.unece.org/trade/untdid/welcome.html">http://www.unece.org/trade/untdid/welcome.html</a></p> <p><i>comprise a set of internationally agreed standards, directories, and guidelines for the electronic interchange of structured data, between independent computerized information systems.</i></p>

## Annex E: Research Methodology

The figure below summarises the approach used to collect data, assess its relevance, and structure it accordingly.

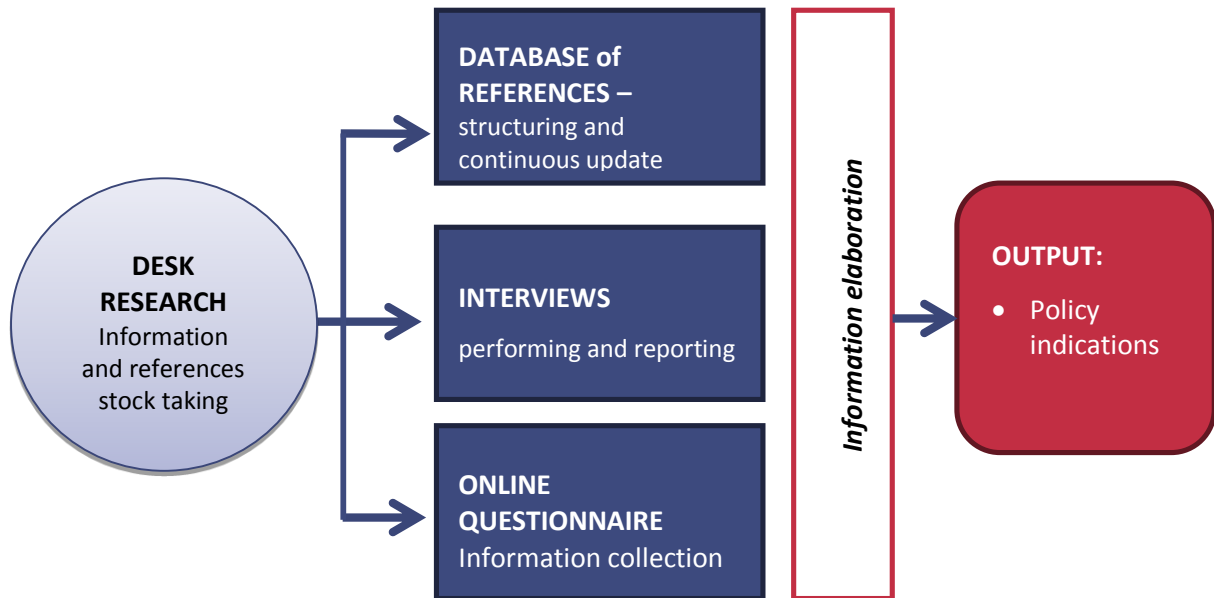


Figure 17 – Workflow overview

### E.1 Interviews

The interviews were elaborated based on the preliminary results of the desktop research and the questionnaire. Their purpose was to drive in an efficient way the interaction with the National Financial Supervisory Authorities and the Industry respondents.

This interview approach was selected for two reasons:

1. It allows the collection of relevant qualitative information: respondents have the opportunity to stress their points of major interests, best practices and relevant qualitative information they are willing to share. On the other hand, and in order to avoid bias or missing answers, a set of indications on the objectives of each open question were provided to respondents, in order to structure answers.
2. It provides means of comparison for the evaluation of the information collected.

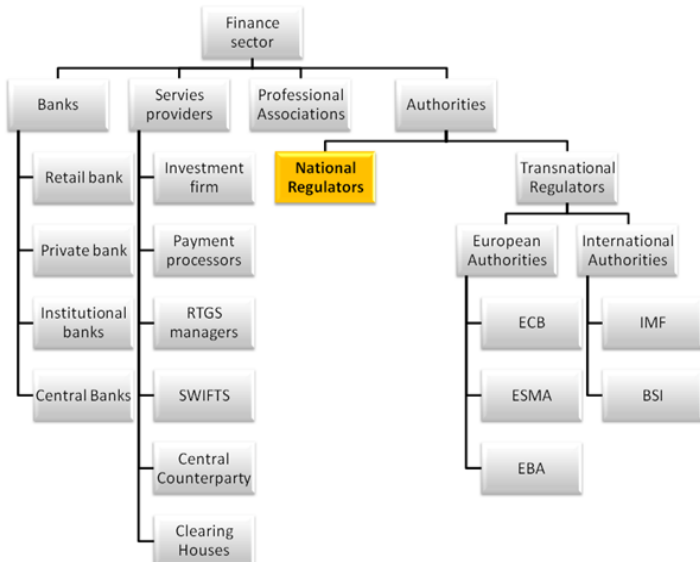
European Union Agency for Network and Information Security
www.enisa.europa.eu

*Finally,*

Please consider the following proposed taxonomy of Finance Sector key players and Stakeholders.

3.01 May You please list below the National bodies which in Your country are concerned with Finance Sector ICT security and resilience?

- (  )
- (  )
- (  )
- (  )
- (  )
- (  )
- (  )
- (  )



```

graph TD
    FS[Finance sector] --> B[Banks]
    FS --> SP[Services providers]
    FS --> PA[Professional Associations]
    FS --> A[Authorities]
    
    B --> RB[Retail bank]
    B --> PB[Private bank]
    B --> IB[Institutional banks]
    B --> CB[Central Banks]
    
    SP --> IF[Investment firm]
    SP --> PP[Payment processors]
    SP --> RTGS[RTGS managers]
    SP --> SW[SWIFTS]
    SP --> CCP[Central Counterparty]
    SP --> CH[Clearing Houses]
    
    PA --> NR[National Regulators]
    
    A --> TR[Transnational Regulators]
    TR --> EA[European Authorities]
    TR --> IA[International Authorities]
    
    EA --> ECB[ECB]
    EA --> ESMA[ESMA]
    EA --> EBA[EBA]
    
    IA --> IMF[IMF]
    IA --> BSI[BSI]
    
    style NR fill:#ffff00
            
```

Figure 18 –Interview - Section 1

## Annex F: Relevant European Directives and Regulations

Authority	DATA PROTECTION	INFORMATION SECURITY	FINANCIAL Markets Supervision	other (tbd)	
European and International	European Parliament	<p>Proposal for a Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) - COM(2012) 11 final</p> <p>Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data</p>	Budapest Convention on Cybercrime	Directive 2013/36/EU on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms	Directive 2002/58/CE concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communication)
	European Commission		<i>Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union - <b>COM(2013) 48 final</b></i>	COMMISSION DIRECTIVE 2006/73/EC of 10 August 2006 implementing Directive 2004/39/EC of the European Parliament and of the Council as regards organisational requirements and operating conditions for investment firms and defined terms for the purposes of that Directive (Text with EEA relevance).	
	ECB		Target2 Securities - User Requirements Chapter 18 Information Security Requirements	SSM Framework Regulation - ECB/2014/17	



## Network and Information Security in the Finance Sector

Regulatory landscape and Industry priorities

December 2014

Authority	DATA PROTECTION	INFORMATION SECURITY	FINANCIAL Markets Supervision	other (tbd)
other	Opinion 03/2014 of the Article 29 Data Protection Working Party on Personal Data Breach Notification - 693/14/EN WP 213 - Adopted on 25 March 2014	COBIT 5 (Control Objective for Information and related Technologies)	Basel II - International Convergence of Capital Measurements and Capital Standards	Financial and Compliance Audit Manual

**Annex G: Relevant National Laws**

	Issuing authority	DATA PROTECTION	INFORMATION SECURITY	FINANCIAL Markets Supervision	other (tbd)
<b>National</b>	AT	Federal Act concerning the Protection of Personal Data (DSG 2000)		Finanzmarktaufsichtsbehördengesetz	
	BE			Loi établissant les mécanismes d'une politique macroprudentielle et précisant les missions spécifiques dévolues à la Banque nationale de Belgique dans le cadre de sa mission visant à contribuer à la stabilité du système financier	
	BU			Ordinance n°10 on the Internal Control in Banks	
	HR				
	CY	Directive for the Operation of a System or a Mechanism for the Exchange, Collection and Provision of data between the Authorized Credit Institutions and the credit institutions that operate in the Republic under section 10A of the Law			-
<b>National</b>	CZ			Financial Market Supervision	
	DK			Danish Financial Business Act	
				Executive Order on outsourcing significant areas of activity	



Issuing authority	DATA PROTECTION	INFORMATION SECURITY	FINANCIAL Markets Supervision	other (tbd)
			Executive Order on Management and Control of Banks etc.	
			Executive order on IT audit in datacentres owned by financial institutions	
EE			Financial Supervision Authority Act - Finantsinspektsiooni seadus	
FI			Standard RA4.2 - Reporting of operational risk events	
FR	Loi 78-17 du 6 Janvier 1978 modifiée - Loi informatique et Libertés			
DE			Gesetz über das Kreditwesen (Banking Act)	
			Mindestanforderungen an das Risikomanagement (MaRisk) - Minimum Requirements for Risk Management	
			IT-Grundschutz Manual	
GR			Governor's Act 2597/31 - Annex 2	
HU				
IE				



	Issuing authority	DATA PROTECTION	INFORMATION SECURITY	FINANCIAL Markets Supervision	other (tbd)
<b>National</b>	IT			Nuove disposizioni di vigilanza prudenziale per le banche - Circolare 263/2006 Banca d'Italia	
	LT	-	-	-	
	LU	Traitement des données a caractèr personnelle	Circulaire CSSF 13/554	Circulaire CSSF 12/552	
	LV		Regulation on Information Security Systems	Regulation n.94 for Electronic Information Exchange with the Bank of Latvia	
	MT				
	NL			Financial Supervision Act (Wet op het financieel toezicht / Wft)	
	PL				
	PT	Lei 32/2008 - transpõe a Diretiva da Retenção de Dados, relativa à conservação de dados das comunicações eletrónicas	Lei 109/ 2009 - Lei do cibercrime	Decreto Lei 104/2007	Resolução do Conselho de Ministros nº 12/2012
	Lei46/2012 de Alteração à Lei n.º 41/2004		Modelo de Avaliação dos riscos		
<b>National</b>	RO	ORDONANȚĂ DE URGENȚĂ nr. 13 din 24 aprilie 2012 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice	Hotărârea nr. 271/2013 pentru aprobarea Strategiei de securitate cibernetică		
		DECIZIE privind stabilirea unui model de autorizație pentru			

Issuing authority	DATA PROTECTION	INFORMATION SECURITY	FINANCIAL Markets Supervision	other (tbd)
	transferul în străinătate al datelor cu caracter personal în baza regulilor corporatiste obligatorii (Binding Corporate Rules — BCR)			
SI			Regulation on Risk Management and Implementation of the Internal Capital Adequacy Assessment Process for Banks and Savings Banks	-
SK			Methodological Instruction of the Banking Supervision Division No. 7/2004 on the audit of information systems security of banks and branch offices of foreign banks	DECREE of Národná banka Slovenska of 31 August 2010
National	ES	Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal	Orden Ministerial 76/2006, de 19 de mayo, por la que se aprueba la política de seguridad de la información del Ministerio de Defensa	
		Real Decreto 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual	Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos	
		Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones	Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica	

Issuing authority		DATA PROTECTION	INFORMATION SECURITY	FINANCIAL Markets Supervision	other (tbd)
			Real Decreto 4/2010 de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica		
			Ley 59/2003, de 19 de diciembre, de firma electrónica		
			Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico		
<b>National</b>	SE				
	UK		Telecommunication Resilience Good Practices Guide	Business Continuity Management Practical Guide	
		The privacy and Electronic Communications (EC Directive) Amendment Regulation 2011	British Standard for Information Security - ISO/IEC 27002	Banking Act	
		Data Protection Act - 1998	Technology and Cyber Resilience Benchmarking Report 2012	The Bank of England's supervision of financial market infrastructure - Annual report	
other (tbd)	-	US. Department of Defence Strategy for Operating in Cyberspace	Liechtenstein - Gesetz über Finanzmarktaufsichts		

## Annex H: National Cards

Nine country have been studied in depth and key information is gathered under the form of “country fiches”. These fiches are attached in [Annex H: National Cards](#). The countries which are part of the sample for this exercise are Belgium [BE], France [FR], Germany [DE], Italy [IT], Netherlands [NL], Portugal [PT], Spain [ES], and United Kingdom [UK].

For every country of the sample, the organisations responsible for regulation, supervision or other supportive functions are described.

Each Organisation is categorised either as:

- Government/Minister [GM]
- Specific Commission [SC]
- National Central Bank [NCB]
- Specific Authority concerned with cybersecurity issues [SA-cybersecurity],
- Specific finance market supervision Authority [SA-fms]
- Specific data protection Authority [SA-data]
- Other to be defined [Other tbd].

Then, the content of the regulation and standards was sorted out according to ENISA’s information security measures meta-framework. Codes reported are formulated in this report as follows:

*Domain – sub-domain*

e.g. Governance and risk management – Information security policy = **D1-SO1**



## BELGIUM

### Context information

*Major credit banks:* ING Belgium, KBC, AXA Bank Europe, Dexia

*Finance-intensive locations:* Brussels

### Reference organization for information security in the Finance sector

**[NCB]** *National Bank of Belgium* – It is in charge of prudential supervision of financial institutions from both the micro-prudential and the macro-prudential angles, and the prompt detection of systemic risk (according to the Law of July 2<sup>nd</sup>, 2010); the bank is responsible for the prudential supervision of credit institutions, insurance companies and investment firms.

**[SC]** *Financial Services and Markets Authority* – It is responsible for financial market supervision in terms of confidence and consumer protection, authorising and supervising certain categories of financial institutions, overseeing compliance by financial intermediaries with codes of conduct and supervising the marketing of investment products to the general public. The FSMA has substituted the *Banking, Financial and Insurance Commission* (CBFA), which was formerly in charge of supervision activities.

**[SA-fms]** *Belgian Financial Intelligence Processing Unit (CTIF-CFI)* – It is an independent administrative authority, supervised by the Ministries of Justice and Finance, concerned with suspicious financial facts and transactions linked to money laundering and terrorism financing, reported by institutions and individuals (according to the Royal Decree of 11 June 1993).

### Preliminary identified regulation and standards

- *Loi établissant les mécanismes d'une politique macroprudentielle et précisant les missions spécifiques dévolues à la Banque nationale de Belgique dans le cadre de sa mission visant à contribuer à la stabilité du système financier, Belgium National Central Bank 2014 – D4-SO13 Operational procedures*



## FRANCE

### Context information

*Major credit banks:* BNP Paribas, Crédit Agricole, Société Générale, BPCE

*Finance-intensive locations:* Paris

### Reference organization for information

#### security in the Finance sector

[NCB] Banque de France (*French National Central Bank*) – Its main functions include the formulation and implementation of monetary and credit policies, the maintenance of financial stability and the monitoring of the country's financial market. The French NCB oversight tasks are concerned with financial market infrastructures (payment systems, clearing systems and financial instrument settlement systems) and cashless means of payment. In particular, according to both national and European legal framework, the French NCB oversight mission consist in ensuring the security of cashless means of payment and the relevance of the standards applicable in this area, ensuring the smooth operation and security of payment systems, and the security of financial instrument clearing and settlement systems.

[SC] Commission National de l'Informatique et des Libertés (*National Commission for informatics and liberties*) – It is an independent administrative regulatory body (established by the *Loi 78-17 du 6 Janvier 1978*) whose mission is to monitor the application of data privacy law. Besides communication and education activities, the CNIL also monitors the security of information systems by checking that all precautions are taken to prevent the data from being distorted or disclosed to unauthorised parties.

#### Preliminary identified regulation and standards

- *Loi 78-17 du 6 Janvier 1978 modifiée - Loi informatique et Libertés, 1978* [ed. 2013] - **D1-SO1 Information security policy** (ChapitreV: Obligations incombant aux responsables de traitements et droits des personnes)



## GERMANY

### Context information

*Major credit banks:* Deutsche Bank, Commerzbank, Deutsche Postbank, UniCredit Bank

*Finance-intensive locations:* Frankfurt, Berlin, Munich

### Reference organization for information security in the Finance sector

**[NCB]** Deutsche Bundesbank (*German National Central Bank*) – It shares the responsibility of finance sector supervision with BaFin, being specifically responsible for the supervision of credit institutions and financial services, monitoring their solvency and liquidity (according to the Banking Act, 1998, Division 2 Section 7).

**[SA-fms]** BaFin, Bundesanstalt für Finanzdienstleistungsaufsicht (*Federal Financial Supervisory Authority*) – It is an autonomous public-law institution committed with both solvency and market supervision of banks and financial services providers, insurance undertakings and securities trading; it shares the supervision responsibility with the Deutsche Bundesbank (according to the Banking Act, 1998, Division 2 Section 6).

**[SA-data]** Bundesamt für Sicherheit in der Informationstechnik (*Federal Office for Information Security*) – It is a national security agency aimed at promoting information security in Germany; it investigates security risks and develops preventive security measures.

**[Other tbd]** Deutsche Kreditwirtschaft (*German Banking Industry Committee*) – It is the national banking industry association; it takes normative decisions for the sector either by interbank treaties or indirectly by preparing draft regulation for national authorities.

### Preliminary identified regulation and standards

- *Gesetz über das Kreditwesen (Banking Act), 1998* - **D1-SO2 Governance and risk management** (Section 25a), **D1-SO3 Security roles and responsibilities** (Division 1), **D3-SO11 Access control to network and information systems** (Sect. 24c)
- *Mindestanforderungen an das Risikomanagement (MaRisk, Minimum Requirements for Risk Management), 2012* - **D1-SO2 Governance and risk management** (BTR 4 Operational risk), **D7-SO21 Monitoring and logging policies** (AT 4, and BT 2.4), **D3-SO12 Integrity of network and information systems** (AT 7.2), **D6-SO19 Service continuity strategy and contingency plans** (AT 7.3), **D7-SO24 Security assessment** (BTO 1.4)
- *IT-Grundschutz Manual, 2005* - **D1-SO2 Governance and risk management** (B 1.0), **D2 Human resources security** (B1.2), **D6-SO19 Service continuity strategy and contingency plans** (B1.3), **D5-SO16 Incident management procedures** (B 1.8), **D2-SO4 Security of third party assets** (B1.11), **D2-SO6 Security knowledge and training** (B1.13), **D3-SO9 Physical and environmental security** (Layer 2), **D3-SO12 Integrity of network and information system** (Layer 3)



## ITALY

### Context information

*Major credit banks:* UniCredit, Inters Sanpaolo, Mediobanca, Monte dei Paschi di Siena

*Finance-intensive locations:* Milan

### Reference organization for information security in the Finance sector

[NCB] Banca d'Italia (*Italian National Central Bank*) – It is a public law institution committed to ensure price stability and the stability and efficiency of the financial system; the Bank of Italy had been entrusted by public law to supervise banks and financial intermediaries: it monitors that activities are managed soundly and prudently, as well as the transparency and correctness of the services provided. To this end the Bank of Italy 1) issues technical regulations and ensures that they are applied, 2) fosters the sound and prudent management of intermediaries by examining documentation and carrying out inspections at their premises, and 3) sanctions incorrect and opaque conduct vis-à-vis customer.

### Preliminary identified regulation and standards

- *Nuove disposizioni di vigilanza prudenziale per le banche - Circolare 263/2006 Banca d'Italia, 15° update, July 2013 – Title V, Chapter 8: D1-SO2 Governance and risk management* (Section II 5., Section IV 2. and Annex A), **D1-SO4 Security of third party assets** (Section VI), **D7-SO21 Monitoring and logging policies** (Section V), **D7-SO24 Security assessment** (Section II 6. and Section III), **D1-SO3 Security roles and responsibilities** (Section II 3. and 4.), **D3-SO11 Access control to network and information systems** (Section IV 3.), **D4-SO13 Operational procedures** (Section IV 4.), **D4-SO14 Change management** (Section IV 5.), **D5-SO16 Incident management procedures** (Section IV 6.), **D6-SO19 Service continuity strategy and contingency plans** (Section IV 7.), **D3-SO12 Integrity of network and information systems** (Section V); *Title V, Chapter 9: D6-SO19 Service continuity strategy and contingency plans*





## NETHERLANDS

### Context information

*Major credit banks:* ING Group, NIBC bank, Rabobank, SNS bank

*Finance-intensive locations:* Amsterdam

### Reference organization for information security in the Finance sector

[**NCB**] De Nederlandsche Bank (*Nederlandaise National Central Bank*) – It is a public limited company committed to safeguard financial stability of the national system; it independently operates as both a central bank and a national supervisor, ensuring the price stability and a balanced macroeconomic development, the shock-resilient attitude of financial system and the security of the payment system. DNB is responsible for the prudential supervision of banks, pension funds, insurance companies and other similar institution.

[**SA-fms**] Autoriteit Financiële Markten (*Netherlands Authority for the Financial Markets, AFM*) – It supervises the way financial institutions (savings, investment, insurance and loans) deal with their customers, according to the 2002 Ministry of Finance policy document 'Review of the supervision of the financial market sector'; it focuses on the question of whether the participants in the financial markets are handled properly and whether they have accurate information.

### Preliminary identified regulation and standards

- *Financial Supervision Act (Wet op het financieel toezicht / Wft)* – **D5-SO18 Incident reporting and communication** (Chapter 3.3 Article 3.10)
- *DNB Supervisory Strategy 2010-2014, 2010* - **D7-SO24 Security assessments**
- *DNB Supervisory Strategy 2010-2014 and themes 2010, 2010* - **D1-SO2 Governance and risk management, D1-SO4 Security of third party assets, D7-SO21 Monitoring and logging policies**



## PORTUGAL

### Context information

*Major credit banks:* Millennium BCP, Banco Espírito Santo, Caixa Geral de Depósitos, Banco Santander Totta

*Finance-intensive locations:* Lisbon

### Reference organization for information security in the Finance sector

**[NCB]** Banco de Portugal (*Portugal National Bank*) - According to its Organic Law, Banco de Portugal is a public-law legal person with administrative and financial autonomy and own property; its main activities are concerned with monetary policy, asset and reserve management, supervision of money and foreign exchange markets, prudential and banking conduct supervision, regulation of payment systems and other decision-making supportive activities. In particular, it performs prudential and market conduct supervision of credit institutions, financial companies and payment institutions with a view to ensuring the stability, efficiency and soundness of the financial system.

**[Other tbd]** Conselho Nacional de Supervisores Financeiros (*National Council of Financial Supervisors, CNSF*) – It is in charge of the coordination among authorities as well as of the monitoring and assessment of developments regarding the stability of the financial system; it also conducts public consultations on initiatives within its fields of competence.

### Preliminary identified regulation and standards

- *Decreto Lei 104/2007 - D7-SO21 Monitoring and logging policies.*
- *Lei 109/ 2009 - Lei do cybercrime – D3-SO12 Integrity of network and information security*



## SPAIN

### Context information

*Major credit banks:* CaixaBank, Bancaha, BBVA, Banco Santander

*Finance-intensive locations:* Madrid

### Reference organization for information security in the Finance sector

[**NCB**] Banco de Espana (*Spanish National Bank*) – It is the national central bank and supervisor of the Spanish banking system (according to the Ley 13/1994, de 1 de junio, de autonomía del Banco de España). It is concerned with the promotion of the stability of the financial system and with the supervision of the solvency and compliance of credit institutions and financial entities.

[**Other tbd**] Instituto Nacional de Tecnologías de la Comunicacion (*ICT National Institute*) – It performs activities related with the provision of services in the field of cybersecurity, research activities and the coordination of partnership networks in the field.

### Preliminary identified regulation and standards

- *Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal* – **D1-SO1 Information security policy**



## UNITED KINGDOM

### Context information

*Major credit banks:* Barclays, HSBC, Lloyds Banking Group, The Royal Bank of Scotland Group.

*Finance-intensive locations:* London

### Reference organization for information security in the Finance sector

[NCB] Bank of England – It is the central bank of England, established as a privately owned institution, it had been nationalized after the Second World War; it is committed to ensure the financial stability of the systems.

[SA-fms] Financial Service Authority (FSA) – It is the national financial regulator (according to the Financial Services and Market Act, 2000); besides regulatory tasks, it promotes efficient and fair financial markets behaviours.

[SA-fms] Prudential Regulation Authority – It is responsible for the supervision of banks, building societies and credit unions, insurers and major investment firms; its role is defined by its statutory objectives which refer to the promotion of the safety and soundness of these firms.

[SA-fms] Information Commissioner's Office - It is an independent authority concerned with the uphold of information rights in the public interest; data controllers should notify the ICO of their processing of personal data, so that these activities can be mapped and maintained in a public register.

### Preliminary identified regulation and standards

- *Banking Act, 2009 - D4-SO13 Operational procedures* (Part V)
- *The privacy and Electronic Communications (EC Directive) Amendment Regulation 2011, 2011 – D1-SO4 Security of third party assets* (31A.), **D3-SO12 Integrity of network and information systems** (5A. and followings)
- *Telecommunication Resilience Good Practices Guide, 2006 – D7-SO24 Security assessments*
- *Business Continuity Management Practical Guide, 2006 – D6-SO19 Service continuity strategy and contingency plans, D6-SO20 Disaster recovery capabilities*
- *Data Protection Act, 1998 – D1-SO1 Information security policy*
- *FSA Data Security in Financial Services, 2008 - D1-SO1 Information security policy* (3.1), **D2-SO6 Security knowledge and training** (3.2), **D2-SO7 Personnel changes** (3.3), **D7-SO21 Monitoring and logging policies** (3.4), **D3-SO9 Physical and environmental security** (3.5), **D4-SO13 Operational procedures** (3.6), **D1-SO4 Security of third party assets** (3.7)



TP-05-14-150-EN-N

**ENISA**

European Union Agency for Network and Information Security  
Science and Technology Park of Crete (ITE)  
Vassilika Vouton, 700 13, Heraklion, Greece

ISBN: 978-92-9204-118-2

doi: 10.2824/654601

**Athens Office**

1 Vass. Sofias & Meg. Alexandrou  
Marousi 151 24, Athens, Greece



PO Box 1309, 710 01 Heraklion, Greece

Tel: +30 28 14 40 9710

[info@enisa.europa.eu](mailto:info@enisa.europa.eu)

[www.enisa.europa.eu](http://www.enisa.europa.eu)