CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

WORKING PAPER

MARCH 2021

Cyber Policy Initiative Working Paper Series | "Cybersecurity and the Financial System" #9

The European Union, Cybersecurity, and the Financial Sector: A Primer

Philipp S. Krüger and Jan-Philipp Brauchle

The European Union, Cybersecurity, and the Financial Sector: A Primer

Philipp S. Krüger and Jan-Philipp Brauchle

Carnegie Endowment for International Peace
Publications Department
1779 Massachusetts Avenue NW
Washington, DC 20036
P: + 1 202 483 7600
F: + 1 202 483 1840
CarnegieEndowment.org

This publication can be downloaded at no cost at CarnegieEndowment.org.

CONTENTS

Cybersecurity and the Financial System

Carnegie's working paper series 'Cybersecurity and the Financial System' is designed to be a platform for thought-provoking studies and in-depth research focusing on this increasingly important nexus. Bridging the gap between the finance policy and cyber policy communities and tracks, contributors to this paper series include government officials, industry representatives, and other relevant experts in addition to work produced by Carnegie scholars. In light of the emerging and nascent nature of this field, these working papers are not expected to offer any silver bullets but to stimulate the debate, inject fresh (occasionally controversial) ideas, and offer interesting data.

If you are interested in this topic, we also invite you to sign up for Carnegie's FinCyber newsletter providing you with a curated regular update on latest developments regarding cybersecurity and the financial system: CarnegieEndowment.org/subscribe/fincyber.

If you would like to learn more about this paper series and Carnegie's work in this area, please contact Arthur Nelson at arthur.nelson@ceip.org.

Papers in this Series:

- "Deepfakes and Synthetic Media in the Financial System: Assessing Threat Scenarios," Jon Bateman, July 2020
- "Cyber Mapping the Financial System," Jan-Philipp Brauchle, Matthias Göbel, Jens Seiler, and Christoph von Busekist, April 2020
- "Lessons Learned and Evolving Practices of the TIBER Framework for Resilience Testing in the Netherlands," Petra Hielkema, and Raymond Kleijmeer, October 2019
- "Cyber Risk Scenarios, the Financial System, and Systemic Risk Assessment," Lincoln Kaffenberger and Emanuel Kopp, September 2019
- "Cyber Resilience and Financial Organizations: A Capacity-building Tool Box," Tim Maurer and Kathryn Taylor, July 2019
- "The Cyber Threat Landscape: Confronting Challenges to the Financial System" Adrian Nish and Saher Naumaan, March 2019
- "Protecting Financial Institutions Against Cyber Threats: A National Security Issue" Erica D. Borghard, September 2018

Abbreviations

CCP	central counterparty
CIISI-EU	Cyber Information and Intelligence-Sharing Initiative
CRA	credit rating agency
CRAR	Credit Rating Agencies Regulation
CRD IV	Capital Requirements Directive IV
CROE	Cyber Resilience Oversight Expectations for Financial Market Infrastructures
CRR	Capital Requirements Regulation
CSD	central securities depository
CSDR	Central Securities Depositories Regulation
CTPPs	critical third-party service providers
DORA	Digital Operational Resilience Act
EBA	European Banking Authority
EC	European Commission
ECB	European Central Bank
EIOPA	European Insurance and Occupational Pensions Authority
EMIR	European Market Infrastructure Regulation
ENISA	European Union Agency for Cybersecurity
ESA	European Supervisory Agency
ESMA	European Securities and Markets Authority
EU	European Union
FMI	financial market infrastructure
GDPR	General Data Protection Regulation
ICT	information and communication technology
IT	information technology
MiFID II	Markets in Financial Instruments Directive II
NCA	national competent authority
NIS Directive	Directive on Security of Network and Information Systems
OES	operator(s) of essential services

Abbreviations Continued

PSD2	revised Payment Services Directive
PSP	payment service provider
RTS	Regulatory Technical Standard(s)
SCA	strong costumer authentication
SIPS	systemically important payment systems
SREP	Supervisory Review and Evaluation process
SSSs	securities settlement systems
TIBER-EU	the EU framework on threat intelligence-based ethical red teaming
TPP	third-party provider
TRs	trade repositories

Summary

In recent years Europe has put an intense focus on legislation concerning information and communication technology (ICT) and cybersecurity for the European financial sector. With compliance being one of the main drivers for cyber resilience, a prudent and consistent regulatory strategy can help to ensure the necessary baseline in security across the financial sector to mitigate institutional and systemic risk. This paper presents a comprehensive overview of the current European regulatory landscape for the financial sector concerning ICT risk and cybersecurity, evaluates the future plans of the European Commission (EC) in this field, and provides recommendations to advance and complement the planned initiatives with the objective to achieve a consistent, effective, and comprehensive legislative landscape for the European financial sector.

The current European regulatory landscape for ICT and cyber risk for the financial sector is multilayered and complex. There exists not one major European cybersecurity legislation for the financial services sector, but rather a multitude of different European and national regulations and sector-specific standards. Financial institutions must adhere to critical infrastructure regulations, general European legislation surrounding topics like data protection, and specific financial sector regulation and standards. These sector-specific standards are further divided into the different subsectors of the financial sector, such as banking and payments, insurance and reinsurance, and financial market infrastructures. Moreover, most European standards do not apply directly to all member states, but rather must be transposed into national legislation, creating further fragmentation and difference.

The two most important and far-reaching pieces of non-sector-specific legislation for financial institutions are the Directive on Security of Network and Information Systems (NIS Directive) and the General Data Protection Regulation (GDPR), both passed in 2016. Among other measures, the NIS Directive identifies the financial sector as one of seven critical infrastructure sectors for which the EU member states need to ensure an appropriate technical and organizational level of security through specific pieces of critical infrastructure legislation. This includes an incident response regime that financial institutions must adhere to. The GDPR was introduced to standardize data protection regulation across the European Union (EU) and applies to all organizations that control or process personal data and operate within or sell goods to the EU. Financial institutions control and process a large volume of data and are thus highly impacted by the GDPR. One of the main obligations by the GDPR is concrete requirements concerning privacy, security, and breach management.

Similar to the general European regulation on ICT and cybersecurity, currently there is no single sector-specific legislation for all financial institutions, but multiple standards applying to different subsectors and in different contexts. Out of the three subsectors, regulation in the banking and payment services sphere is quite detailed and specific—with the revised Payment Services Directive

(PSD2) and the European Banking Authority (EBA) Guidelines on ICT and Security Risk Management being the most far-reaching and explicit standards. The standards for insurances and reinsurances as well as for financial market infrastructures are, for the most part, still very high-level and address ICT and cybersecurity requirements rather implicitly as part of operational risk. The current regulatory landscape for financial institutions shows the significant progress that has been made during the past ten years in the area of ICT and cybersecurity legislation for the financial sector in Europe. However, although many financial institutions are subject to some sort of ICT and cybersecurity legislation, there are still gaps in the regulatory landscape, and the multitude of legislation and standards leaves room for confusion. This is most visible in the myriad of incident response regimes by multiple pieces of legislation that financial institutions fall under and that all differ in their conditions.

To improve on this situation and address inadequacies, the EC proposed in September 2020 new legislation on digital resilience for the European financial sector, called the Digital Operational Resilience Act (DORA). The proposal is part of the digital finance package to further enable and support the potential of digital finance in terms of innovation and competition while mitigating the risks arising from it. DORA aims to introduce a harmonized and comprehensive framework on digital operational resilience for European financial institutions spelling out explicit requirements to address and mitigate ICT and cyber risks. It is a direct response to the joint advice by the European Supervisory Agencies (ESAs). The ESAs identified four fields of action to concentrate on in regulatory developments in the near future: first, requirements on ICT security and risk management; second, sectoral cyber incident reporting requirements; third, direct oversight and supervision of third-party providers; and fourth, a cyber resilience testing framework. DORA addresses all of these areas and provides potential solutions for many current gaps.

The proposed measures by the EC do not only address the most urgent gaps and issues, but also go beyond current structures and set the framework for future innovation and security of the European financial sector.

To complement the commission's approach, resharpen certain aspects, and highlight new areas, this paper provides four recommendations:

Establish a single European legislation on ICT and cybersecurity for all financial institutions. The paper shows the regulatory fragmentation between financial subsectors concerning ICT and cyber risk. However, in order to achieve operational resilience from cyber risk, a harmonized level of cybersecurity across all financial institutions is crucial. This is further emphasized by the fact that a lack in

basic cybersecurity measures still underlines most successful cyber attacks. The proposed DORA regulation by the EC is a solution to this problem. As a common single legislation addressing most European financial subsectors, it can ensure harmonization and a baseline of requirements concerning ICT and cyber risks. To ensure this level of harmonization, the DORA proposal needs to be adopted and its core left unchanged by the upcoming review from the European Parliament and the European Council.

Shift to a risk-centric approach. Regulators need to incentivize larger financial institutions to shift from their currently predominant compliance-centric perspective to a risk-centric approach in order to achieve operational resilience. Systems such as the EU framework on threat intelligence-based ethical red teaming (TIBER-EU) and the requirements laid out in the proposed DORA regulation are a step in the right direction, improve the resilience of financial institutions, and therefore need to be incorporated into the supervisory toolkit.

Incorporate the systemic dimension of cyber risk into legislation and supervision. Current ICT and cyber risk legislation mainly focuses on the single institution. Although a harmonized level of cybersecurity of all financial institutions mitigates not only the risk for the single institution, but also for the system, it is still important to discuss further complementing macroprudential measures. These can be similar to existing systemic measures concerning capital and liquidity risk—such as additional security requirements for systemically important financial institutions—or they can be new measures altogether. The proposed DORA legislation acknowledges the systemic nature of cyber risks and comprises several initiatives to address it, including the fostering of information exchange from incident reporting regimes and an increased scrutiny on the role and interdependencies of third-party providers (TPPs).

Incorporate the systemic nature of cyber risk into regulators' actions. Cooperation in the sphere of cybersecurity is an important asset that can take many forms and that ranges from informal exchanges on best practices and indicators of compromise to the conduction of coordinated exercises. However, private institutions are often deterred from strong cooperation with cybersecurity regulators due to reasons of confidentiality and competition. Thus, there is a lack of European fora for cooperation. While there exist European initiatives such as the Cyber Information and Intelligence-Sharing Initiative (CIISI-EU), these initiatives should be expanded and enhanced to optimize the cooperation and information exchange in the European financial sector. Further, the European Union Agency for Cybersecurity (ENISA) could take up a crucial role as a central hub to foster and coordinate cross-sector cooperation and information sharing of public and private stakeholders across the EU.

Introduction

In the 2019 edition of its regulatory digest, the World Bank identified twenty-eight pieces of legislation, standards, guidelines, and supervisory documents that have been issued by EU standard-setting bodies on cybersecurity for the financial sector. Twenty-five out of the twenty-eight existing documents were introduced since 2016, demonstrating the EU's focus on this topic in recent years.[1] Financial institutions are highly dependable on their information technology (IT), and they increasingly place their trust in their networks and information systems to carry out daily operations. The financial sector has simultaneously been the main target of cyber attacks among all industries. Consequently, regulators and supervisory authorities have developed a high interest in the mitigation and management of ICT and cyber risks of financial institutions and have been working to improve the resilience and stability of the whole financial system.

Despite these intentions, the current European regulatory landscape is multilayered and complex. Lacking a holistic and overarching European legislation, standards are derived from the respective European and national financial subsector regulations (called Level 1 legislation) and therefore differ for banks, insurance companies, financial market infrastructures, and others.[2] The main focus of Level 1 legislation is on capital and liquidity risk, addressing ICT and cyber risk only implicitly as a subform of operational risk.[3] However, in the last two years, European regulators have started to implement standards and guidelines based on Level 1 legislation that explicitly address ICT and cyber risk. As part of a joint technical advice to the European Commission, ESAs emphasize four fields of action: first, requirements on ICT security and risk management; second, sectoral cyber incident reporting requirements; third, direct oversight and supervision of third-party providers; and fourth, a cyber resilience testing framework.[4] Based on these fields of action, in September 2020 the EC adopted a legislative proposal on digital resilience for the European financial sector, called DORA, as part of the EC's digital finance package. DORA aims to introduce a harmonized and comprehensive framework on digital operational resilience for European financial institutions, spelling out explicit requirements to address and mitigate ICT and cyber risks.

The paper presents a comprehensive overview of the European regulatory landscape for the financial sector concerning ICT risk and cybersecurity and provides recommendations on the future direction and missing pieces in the target view of the EC. To achieve this, it outlines and comments on the important regulations, guidelines, and standards, as well as the overall state of regulation in the three subsectors. Further, the paper evaluates the EC's plans on the future regulatory and supervisory development in the four fields of actions as well as the digital finance strategy and operational resilience. To conclude, the paper provides four recommendations to emphasize, improve, or complement the existing initiatives with the objective to achieve a consistent, effective, and comprehensive legislative landscape for the European financial sector.

Overview of Cybersecurity Regulation in the EU for the Financial Sector

The current situation of the financial services sector in the EU concerning cybersecurity legislation is multilayered and complex. Because financial institutions fall under the scope of different regulatory and supervisory areas, there is not one major European cybersecurity regime for the financial services sector, but rather a multitude of different European and national regulations and sector-specific standards.

In many member states, the financial sector is defined as critical infrastructure, in line with other sectors such as energy and health. Regulations concerning critical infrastructure sectors, therefore, apply to financial institutions. General European legislation surrounding topics like data protection or cyber crime apply to most companies and therefore affect financial institutions as well. Most notably, financial institutions must adhere to specific financial sector regulation and standards. Even these sector-specific standards differ between the various subsectors, such as banks, insurance companies, and financial market infrastructures. To complicate matters even further, most European standards do not apply directly in all member states, but rather must be transposed into national legislation, creating further fragmentation and difference. Table 1 shows an overview of the existing regulatory landscape with ICT or cybersecurity relevance for the European financial sector. Figure 1 shows a timeline of the legislation laid out in table 1.

TABLE 1

Existing Legislation with ICT and Cybersecurity Relevance for the European Financial Sector

Legislation	Subjects	Relevant Authority	ICT and Cybersecurity Requirements	Specifying Standards for ICT and Cybersecurity
		General Legislation		
NIS Directive	Operators of essential services	Up to national discretion	Explicit	Implementation by member states
GDPR	All companies operating in EU	Data Protection Authority is up to national discretion	Explicit	No

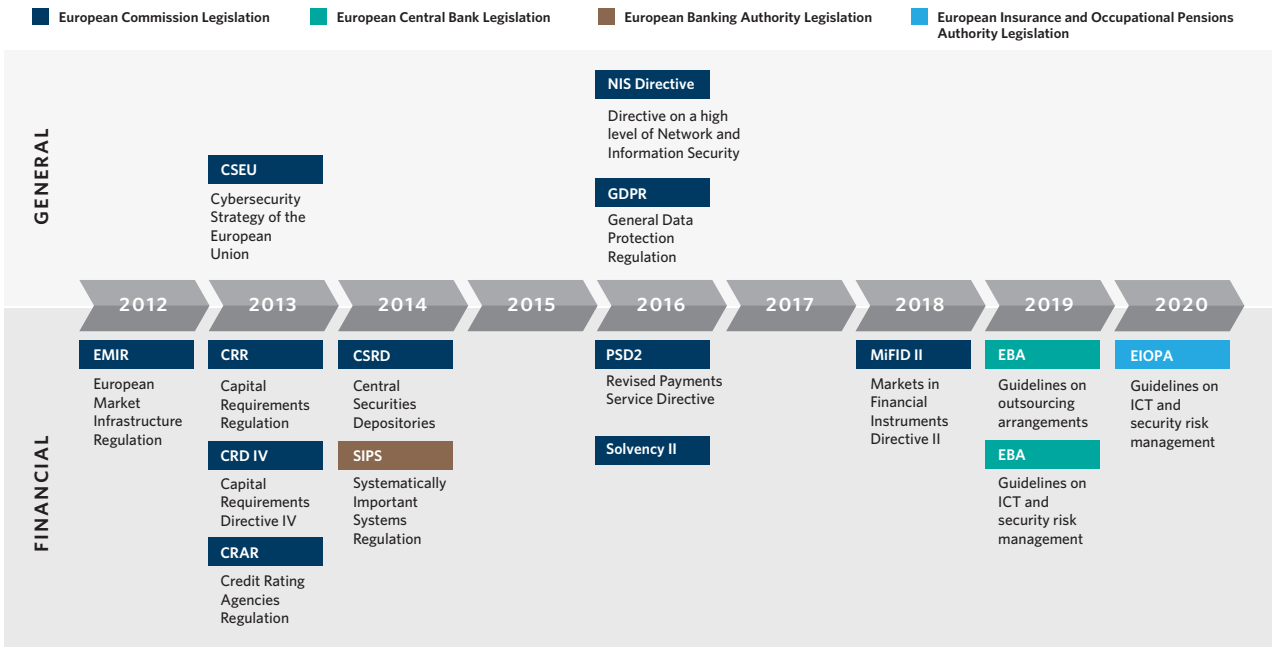
TABLE 1 CONTINUED

Existing Legislation with ICT and Cybersecurity Relevance for the European Financial Sector

Legislation	Subjects	Relevant Authority	ICT and Cybersecurity Requirements	Specifying Standards for ICT and Cybersecurity
		Sector-specific legislation		
CRR and CRD IV	Credit institutions and investment firms	ECB, EBA, and national supervisory authorities	Explicit	Yes
PSD2	Payment service providers	ECB, EBA, and national supervisory authorities	Explicit	Yes
Solvency II	Insurance and reinsurance institutions	EIOPA and national supervisory authorities	Implicit	No
MiFID II	Investment firms, data reporting service providers, and trading venues	ESMA and national supervisory authorities	Implicit	No
EMIR	Central counter parties and trade repositories	ESMA and national supervisory authorities	Implicit	No
CSDR	Central securities depositories and securities settlement systems	ESMA and national supervisory authorities	Implicit	No
CRAR	Credit rating agencies	ESMA and national supervisory authorities	Implicit	No
SIPS Regulation	Systemically important payment systems	ESMA and national supervisory authorities	Explicit	Yes

FIGURE 1

Timeline of General and Sector-Specific Legislation



Although these pieces of legislation have their respective scope and objectives, they can cover similar areas and list different responsible authorities, creating overlap and uncertainty for the regulated financial institutions. Despite the large amount of legislation, there are still institutions that are not covered by explicit and concrete requirements concerning ICT and cybersecurity. The following sections aim to paint a picture of the most important current European legislation and guidelines for financial institutions with regard to ICT and cybersecurity regulation. The distinction will be drawn between general European legislation not limited to financial institutions and specific regulations and standards for the financial sector and its various groups. Where relevant, it will be shown how these standards interrelate to each other, where they overlap, and how this overlap might cause complications.

General European Regulatory Framework for Cybersecurity

In its first cyber strategy titled "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace," passed in 2013, the EC acknowledged that dealing with challenges in cyberspace should primarily be up to the member states.[5] Therefore, there is currently no European legislation that lays down specific ICT and cybersecurity requirements for all European companies or institutions. The two most important and far-reaching pieces of legislation are the NIS Directive and the GDPR, both passed in 2016. Both pieces of legislation are limited in scope by focusing on specific sectors (like critical infrastructure) or topics (like data protection).

Directive on Security of Network and Information Systems. The NIS Directive was adopted in 2016 as "the first EU-wide legislation on cyber security" with the goal to ensure a common level of network and information security across the EU by providing legal requirements.[6] Next to the obligation for EU member states to implement a national cybersecurity strategy and install national competent authorities (NCAs), the directive identifies seven sectors with essential services for the maintenance of critical, societal, and/or economic activities in the EU: the sectors of energy, health, transport, banking, financial market infrastructure, digital infrastructure, and drinking water supply. For these sectors, member states must identify national operators of essential services (OES), namely the entities who operate the services in these sectors. The member states shall then ensure through specific critical infrastructure legislation that these OES take appropriate and proportionate technical and organizational measures to manage the risks posed to the security of network and information systems that they use in their operations. Additionally, member states are required to ensure that OES notify the NCAs of any significant incidents that could risk the continuity of their provided essential services.[7] The NIS Directive describes three parameters to determine the significance of the impact of an incident: the number of users affected by the disruption of the essential service, the duration of the incident, and the geographic spread of the area affected by the incident.[8]

Larger financial institutions that are considered OES by the respective NCA are subject to the NIS Directive. While past regulations mainly focused on banks, the NIS Directive adds certain types of financial market infrastructures (FMIs) to the list. It is at the discretion of member states to add further critical sectors to these. For example, Germany and France consider the insurance sector critical. Although the NIS Directive aims to establish a common standard in the EU, as a directive it is left to the member states to transpose the directive and formulate specific requirements in their respective national legislation. The member states have to further integrate the regulations for critical infrastructures with the existing regulation for the financial sector. In Germany this has been achieved by adding a specific chapter for OES into the existing sector-specific guidelines on ICT risk.[9]

However, the type of integration differs between member states. Member states are further free to designate the responsible NCA under the NIS Directive. While some countries, such as Germany and France, have designated single NCAs for all critical sectors, others such as Italy have appointed NCAs for each sector. In countries like Germany, where the NCA (the Federal Office for Information Security) differs from the national financial supervisory authority (the Federal Financial Supervisory Authority), this can lead to further complications between both authorities as well as for financial institutions that have to report to multiple supervisory authorities.

Overall, the current framework of the NIS Directive bears the risk of leading to varying levels of security requirements for critical institutions in different member states. With cyber risk, harmonization of security levels across countries is important because attacks can leap over from countries with lower resilience. On top of this, financial institutions that operate in multiple European countries will be faced with a variety of different national legislation and responsible authorities.

General Data Protection Regulation. The GDPR is the second major general legislation and one of the most wide-ranging pieces of regulation passed in the EU.[10] It was adopted into law in 2016 and aims to standardize data protection law across the single market while giving individuals greater control over how their personal information is used. It applies to all organizations that control or process personal data and operate within or sell goods to the EU. The definition of processing is designed to cover practically every type of data usage and includes data collection, retrieval, alteration, storage, and destruction. The GDPR aims for a harmonization and simplification of data protection rules across the EU, widens the scope of data protection for all EU citizens, and significantly strengthens data protection enforcement and accountability by authorizing penalties for noncompliance of up to 20 million euro ($24 million) or 4 percent of global annual turnover. The GDPR also formulates requirements for institutions to report breaches of personal data to the competent authorities.[11]

Financial institutions control and process a large volume of data and are therefore highly impacted by the GDPR. The regulation requires an institution to understand how it interacts with personal information and to obtain consent from individuals before taking action with that data, including consent on how and where data is stored and processed. Financial institutions have to provide new fundamental data rights to both employees and customers, such as the right to be forgotten. Further, the GDPR states concrete requirements concerning privacy, security, and breach management. As stated above, financial institutions are required to notify the competent authority (for example, the national data protection regulator) of a data breach, embed privacy by design and default into business processes and systems, and ensure appropriate organizational and technical security measures are in place for the protection of personal information.

In contrast to the NIS Directive, the GDPR is a European regulation that does not need to be transposed into national law by each member state. Rather, it has binding legal force throughout every member state. From its initial proposal, the EU legislature emphasized the importance of having a "single set of rules," and consequently chose to legislate by regulation.[12] Even with its status as a regulation, the GDPR still leaves several significant issues to the interpretation of the member states, creating the risk of national divergence and complication for institutions operating in multiple European countries. While this divergence is smaller than with the NIS Directive, where implementation is completely up to the member states, it still leaves organizations to deal with the rules in the GDPR as well as the national member state legislation. The GDPR does not determine when these national member state laws will apply to an organization, leaving organizations in uncertainty.[13]

Financial Services Sector-specific Regulatory Framework for Cybersecurity

Supervisory authorities for the financial services sector were among the first to introduce sector-specific cyber and ICT regulation in the EU. This is due to three main reasons. First, the financial services sector has historically been highly regulated. Reasons for this range from risk of financial crisis for the economy and society to risk for deposit insurance funds and customer protection. Second, financial institutions have quickly adapted to technological progress and incorporated new technologies (such as blockchain and AI) to optimize their business models and operations.[14] The financial sector made early use of computers and network technology and even today is among the first adopters of new technology (such as blockchain, quantum computing, and AI). Because technological progress is a key driver for innovation in the financial sector, regulators had to keep up with development by introducing new regulations or adapting existing ones to mitigate risks arising from these technological trends. Finally, the financial sector has been and still is the main target industry of cyber criminals, and financial fraud and data theft are the main motivation behind such attacks.

The current sector requirements are legally based on regulations or directives and therefore have the same legal status as the NIS Directive and GDPR. In contrast to these general standards, the sector-specific standards are further specified through so-called Regulatory Technical Standards (RTS) and guidelines by the ESA to ensure a consistent implementation in member states. Similar to the general European regulation on ICT and cybersecurity, there is no single legislation for all financial institutions, but rather, multiple standards applying to different subsectors and in different contexts. Although regulation in the banking and payment services sphere is quite detailed and specific, standards for insurance and reinsurance—as well as for some types of financial market infrastructures—are still very high-level and implicit. While this diversity is attributable to the subsectors' varying levels of maturity, it still leads to a complex and confusing regulatory landscape with overlaps and gaps. The following sections present the current state of ICT risk and cybersecurity regulations in the different subsectors and will show, where relevant, their relationship with general legislation. As discussed above, the relationship of sector-specific legislation with requirements under the NIS Directive has to be analyzed for each member state because the NIS Directive had to be transposed by each member state into national legislation.

Banking and payment services. The banking sector has traditionally been the focus of financial services regulation and accordingly has the most extensive standards concerning ICT risks and cybersecurity. The Capital Requirements Regulation (CRR), the major European banking regulation, still comprises ICT risks under the broader operational risks. As these requirements are high level and rather vague, they leave a lot of room for interpretation. In order to ensure a consistent application, the EBA was mandated to specify these requirements in RTS and EBA Guidelines. In these specifications, as well as in the PSD2, ICT and cyber risks are addressed explicitly.[15]

Capital Requirements Regulation and Capital Requirements Directive IV. The financial crisis of 2007–2008 resulted in a global overhaul of banking regulation, supervision, and risk management with the Basel III package, a voluntary international banking agreement.[16] In the EU, the Basel III rules were transposed into legislation by the Capital Requirements Directive IV (CRD IV) and the CRR, the legal act that implemented the CRD IV.[17] While the main focus of the CRD IV and CRR lies in establishing requirements for capital, liquidity, and counterparty credit risk, the regulation also addresses operational risks and internal governance. As described above, requirements on operational risks implicitly comprise ICT risks. Therefore, although the relevant articles do not explicitly mention ICT risk management, institutions are expected to include this area in the implementation of these regulations. Additionally, the CRD IV requires institutions to have robust governance arrangements in place and to implement policies and processes to evaluate and manage exposure to operational risk.[18] This includes the implementation of contingency and business continuity arrangements to ensure an institution's ability to operate on an ongoing basis and limit losses in the event of severe business disruption.[19]

EBA Guidelines on Outsourcing Arrangements. In 2019, the EBA published the revised EBA Guidelines on Outsourcing Arrangements incorporating the 2017 recommendations on outsourcing to cloud service providers.[20] These guidelines were in reaction to the ongoing trend of outsourcing business activities in the banking sector, including to financial technology companies and cloud service providers. The EBA Guidelines on Outsourcing Arrangements aim to establish a more harmonized framework for credit institutions and investment firms subject to the CRD IV, as well as for payment and electronic money institutions (see box 1). They set out specific provisions for the governance frameworks and the complete lifecycle regarding a financial institution's outsourcing arrangements.

BOX 1

EBA Final Guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation Process

In 2017, the EBA published the Guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation process (SREP).[21] These guidelines aim to ensure the convergence of supervisory practices and promote common procedures and methodologies for competent authorities in the assessment of an institution's ICT risk under the SREP. The guidelines cover seven areas of ICT risks, from governance and strategy, risk exposure, and controls to outsourcing risks. Although the guidelines do not address financial institutions directly, they can be used as an introduction to how supervisors will assess ICT risk management in their respective institutions.

Revised Payment Service Directive. The PSD2 entered into force in the EU in 2016.[22] The PSD2 was to be implemented into national law by the member states by 2018. Its scope comprises payment service providers (PSPs), which are mainly credit institutions; payment institutions, defined under the original Payment Service Directive; and third-party payment service providers, such as financial technology companies.[23] In comparison to CRR, which applies to all areas of credit institutions, PSD2 mostly applies to payment services. The objectives of PSD2 were to update regulation to the state of innovation on the payments market, make payments safer, increase the consumers' protection, and foster innovation and competition, while ensuring a level playing field for all players, including new ones. To achieve the goal of a level playing field, PSD2 puts an obligation on banks to give TPPs access to a customer's payment account data, provided the customer consents to such disclosure.

The measure of increasing the share of data has raised several compliance concerns with the GDPR, which aims at regulating the sharing of personal data. Although divergent in scope and motivation, both pieces of European legislation overlap on several topics.[24] While many of these potential conflicts have been commented upon by the European authorities and can be resolved in a way to ensure compliance with both the PSD2 and GDPR, the overlap between regulations shows the potential of uncertainty from a complex regulatory landscape.

PSD2 was the first European regulation in the financial services sector that specifically spelled out concrete requirements for cybersecurity and management of ICT risks. The PSD2 mandates the EBA and the European Central Bank (ECB) to release RTS and the EBA Guidelines in order to specify the general principles outlined in PSD2.

PSD2 also created an RTS on Strong Customer Authentication and Common and Secure Communication. This RTS obliges PSPs to implement a strong costumer authentication (SCA) if the customer accesses their payment account online, makes an electronic payment, or carries out any action through a remote channel.[25] To be considered SCA, a login must involve at least a two-factor authentication.[26] For all remote transactions—such as remote internet or mobile payments—the RTS requires an extra element in the form of a unique authentication code, which links the transaction to a specific amount and a specific payee. These measures are intended to mitigate any risk of payment fraud or other abuses in the field of digital payments.[27] The RTS further defines how the communication has to be organized between the holder of the customer's payment account (called an Account Servicing Payment Service Provider) and another institution that either initiates a payment for the customer (called a Payment Initiation Service Provider) or aggregates online information for multiple accounts for the customer (Account Information Service Provider).[28]

Further, the PSD2 established guidelines on major incident reporting, setting out the criteria, thresholds, and methodology to be used by PSPs to determine whether or not an operational or security incident should be considered major and, therefore, be notified to the member state's competent authority under PSD2.[29] Furthermore, the guidelines provide the reporting template for these major incidents. In addition, the guidelines establish a set of criteria that competent authorities have to use as primary indicators when assessing the relevance of a major incident and detail the information that competent authorities should share with other domestic authorities when an incident is considered relevant for the latter. Finally, for the purpose of promoting a common and consistent approach, the guidelines also establish requirements regarding the process of information exchange between NCAs and the EBA or ECB.

The introduction of the PSD2 incident reporting regime adds to multiple existing reporting requirements introduced by different authorities and contexts. Table 2 shows a nonexhaustive overview of current reporting regimes for financial institutions.

TABLE 2

Existing European Incident Reporting Regimes for the Financial Sector

Legislation	Scope	Responsible Authority	Time Frame
NIS Directive	Major incident reporting for OES	National NIS Authority	Without undue delay
GDPR	Data Breach notification	National Data Protection Authority	Within 72 hours
PSD2	Incident Reporting for Payment Service Providers	NCA, ECB, and EBA	Within 4 hours
ECB/Single Supervisory Mechanism[30]	Incident Reporting for Significant Financial Institutions	ECB and Joint Supervisory Team	Within 2 hours

The table shows how financial institutions must report major incidents to multiple responsible authorities under different regulations. The standards for reporting differ in what type of incident has to be reported, thresholds for the definition of a major/significant incident, timeline for reporting, and reporting template. This cluster of reporting regimes makes it very complex and burdensome for financial institutions to fully comply. A financial institution operating across EU borders would need to map all the processes and recipients of the incident reports and develop its own governance organization and methodology. Further complexity is added if an institution is also active outside of the EU, where it has to comply to further reporting requirements of the respective jurisdictions.

Finally, the PSD2 establishes guidelines on security measures for operational and security risks of payment service providers. These guidelines present established principles and best practices of risk assessments, control frameworks, mitigating measures, and monitoring in the field of cybersecurity and IT risk management. They were repealed by the EBA Guidelines on ICT and Security Risk Management, detailed below.[31]

EBA Guidelines on ICT and Security Risk Management. In 2019, the EBA published the EBA Guidelines on ICT and Security Risk Management.[32] The guidelines were based on the PSD2 Guidelines on Security Measures for Operational and Security Risks of Payment Services Providers (detailed above), which they repeal.[33] The EBA guidelines extend the scope of the PSD2 guidelines and apply to all

credit institutions and investment firms under EBA's remit and all their activities, while keeping their validity for PSPs and their payment services. The EBA guidelines aim to clarify and harmonize the supervisory expectations following from CRD IV Article 74 and PSD2 Article 95 (1).

The guidelines are divided into seven areas of ICT security: governance and strategy, an ICT and security risk management framework, information security, ICT operations management, ICT project and change management, business continuity management, and payment service user relationship management. The guidelines comprise requirements from other European legislation, such as the creation of an IT strategy, the mapping of an institution's ICT assets and supported functions, or the handover of the oversight of ICT and security risks to an independent control function. Additionally, the guidelines are the first to demand periodic assessments and independent security risk testing as well as periodic training programs for staff and contractors. Institutions are required to have a complete and detailed ICT asset inventory, effective logging, and backup processes, as well as to implement business continuity measures not only from internal business disruption but also from their TPPs. In drafting the guidelines, the EBA considered their embedding in the overall landscape of EU-level regulations and guidelines. Therefore, the guidelines do not include some areas that are already addressed in existing EU-level legislation. For all data-related questions, the EBA refers to the GDPR, and for outsourcing-related issues, it refers to the EBA Guidelines on Outsourcing.

Insurance and reinsurance. European regulation for insurance and reinsurance does not yet explicitly address ICT risks and cybersecurity. Similar to the requirements laid out in the CRD IV and CRR, European regulation for insurance and reinsurance addresses these risks implicitly as part of operational risks. The equivalent of the Basel III framework for banks is the solvency framework for insurers. The Solvency II Directive came into effect in 2016 to harmonize EU insurance regulation with a focus on three pillars: minimum capital requirements, requirements for governance and risk management, and transparency requirements.[34] Article 41 and Article 44 of Solvency II require insurance and reinsurance institutions to "have in place an effective system of governance which provides for sound and prudent management of the business."[35] As part of this prudent management of the business, insurance and reinsurance institutions should take reasonable steps to ensure continuity in the performance of their activities, including in the development of contingency plans. Therefore, the institutions "shall employ appropriate and proportionate systems, resources and procedures."[36] This includes appropriate and proportionate arrangement of ICT. Furthermore, institutions shall "have in place an effective risk-management system . . . to identify, measure, monitor, manage and report, on a continuous basis the risks, at an individual and at an aggregated level, to which they are or could be exposed, and their interdependencies."[37]

Although no European insurance regulation specifically addresses proper management of ICT security and cyber risks, national insurance and reinsurance regulations are highly divergent. While some countries, such as Germany, have specific ICT security and governance requirements in the insurance sectors, other countries don't have any regulation concerning these topics in place.[38] This shows the strong need for a harmonized European regulation on this topic.

Financial market infrastructures. FMIs are responsible for delivering critical services to the smooth functioning of financial markets, including the provision of clearing, settling, and recording monetary and other financial transactions.[39] Disruptions of FMIs can not only have devastating effects on liquidity dislocation and credit losses, but also amplify the transmission of these shock across domestic and international financial markets, putting financial stability at risk. Therefore, high cyber resilience of FMIs is essential.

The supervisory authority and regulation for FMIs in Europe is quite fragmented. While all payment systems and TARGET2 securities are in the competence of the Eurosystem,[40] the oversight of clearing and settlement systems (securities settlement systems [SSSs], central securities depositories [CSDs], and central counterparties [CCPs]) is subject to the national central banks under national law competencies, often in cooperation with the respective NCAs.

For payment systems under the mandate of the Eurosystem, the ECB has adopted the global guidance on cyber resilience for FMIs by two global standard setters, the Committee on Payments and Market Infrastructures and the International Organization of Securities Commissions. In order to provide payment systems and overseers with clearer expectations of the guidance, the ECB published the Cyber Resilience Oversight Expectations for Financial Market Infrastructures (CROE).[41] The CROE aim to provide payment systems with detailed steps on how to operationalize the guidance and enhance their cyber resilience over a sustained period of time, as well as to provide overseers with clear expectations to assess FMIs under their responsibility. [42] The CROE apply to payment systems under the oversight of the Eurosystem. However, for other types of FMIs (such as CSDs and CCPs), the CROE may be adopted by their respective national overseers. Apart from these global guidelines, multiple sector-specific regulations for FMIs in the EU do exist. These regulations apply to different types of FMIs and differ in their level of granularity on this topic. Therefore, not all FMIs are subject to legislation that covers specific requirements on ICT and cybersecurity, making it difficult to establish a common level of security. Table 3 shows the scope of different pieces of European FMI legislation and their respective level of detail concerning requirements on ICT and cybersecurity.

TABLE 3

Overview of European FMI Legislation on ICT and Cybersecurity Requirements

FMI legislation	Scope	Level of detail (ICT and cybersecurity requirements)
MiFID II	Investment firms, data reporting service providers, and trading venues	Low
EMIR	CCPs, Trade Repositories	Medium
CSDR	CSDs, SSSs	Medium
CRAR	CRAs	Low
SIPS Regulation	SIPs	Medium

Markets in Financial Instruments Directive II. The Markets in Financial Instruments Directive II (MiFID II) is a legislative framework instituted by the EU to standardize practices across the EU financial market and improve protections for investors to restore confidence in the industry.[43] It came into effect in 2018 and applies to three major groups: investment firms, data reporting service providers, and trading venues. MiFID II only mentions specific cybersecurity requirements for the latter two groups of addressees in their respective RTS (CDR 2017/571 and CDR 2017/584). The respective RTS specifying organizational requirements of trading venues state that they "shall have in place procedures and . . . electronic security designed to protect their systems from misuse or unauthorized access . . . including arrangements that allow the prevention or minimization of the risks of attacks."[44] Similar requirements are laid out for data reporting service providers. For investment firms, Article 16 (5) only describes high-level requirements to provide "effective control and [to] safeguard arrangements for information processing systems."[45]

European Market Infrastructure Regulation. The European Market Infrastructure Regulation (EMIR) was adopted in 2012 with the goal to increase transparency in the over-the-counter derivatives markets, mitigate credit risk, and reduce operational risk. It addresses CCPs and trade repositories (TRs).[46] The accompanying RTS on requirements for CCPs require them to "maintain a robust information security framework that appropriately manages its information security risk."[47] The framework shall include "appropriate mechanisms, policies and procedures to protect information from unauthorised disclosure, to ensure data accuracy and integrity and to guarantee the availability of the CCP's services."[48]

For TRs, EMIR does not provide any specific cybersecurity requirements; however, some parts are still relevant. TRs should have secure and adequate capacity to handle the information they receive and ensure their confidentiality, integrity, and protection.[49] Further, TRs shall "establish and maintain an adequate business continuity policy and disaster recovery plan."[50]

Central Securities Depositories Regulation. The Central Securities Depositories Regulation (CSDR) entered into force in 2014 and aims to harmonize the authorization and supervision of CSDs across the EU and to improve settlement discipline in the SSSs that CSDs operate.[51] The accompanying RTS entail high-level ICT and cybersecurity requirements for CSDs. According to the RTS, a CSD's comprehensive risk management framework shall enable the CSD to protect the information at its disposal from unauthorized access or disclosure, ensure data accuracy and integrity, and maintain availability of the CSD's services. Further, the risk framework shall include information security to manage the risks CSDs face from cyber attacks.[52] This includes that a CSD shall ensure its IT systems are designed to cover the CSD's operational needs and risks and that its security framework shall outline the mechanisms that the CSD has in place to prevent, detect, and respond to cyber attacks.[53]

Credit Rating Agencies Regulation. The Credit Rating Agencies Regulation (CRAR) introduced a common approach to the regulation and supervision of credit rating agencies (CRAs) within the EU. Its objectives were to enhance the integrity, responsibility, good governance, and independence of credit rating activities to ensure quality ratings and high levels of investor protection.[54] CRAR does not entail specific ICT or cybersecurity requirements but makes more general statements about a CRA's information systems. It states that CRAs shall have "sound . . . internal control mechanisms, effective procedures for risk assessment, and effective control and safeguard arrangements for information processing systems."[55] Additionally, CRAs shall "employ appropriate systems, resources and procedures to ensure continuity and regularity in the performance of its credit rating activities."[56]

Systemically important payment systems. The ECB Regulation on Oversight Requirements for Systemically Important Payment Systems (SIPS Regulation) addresses both high-value and retail payment systems of systemic importance, whether operated by Eurosystem national central banks or private entities.[57] The regulation aims to ensure the efficient management of risks, including operational risks, sound governance arrangements, and the efficiency and effectiveness of systemically important payment systems (SIPS).[58] Article 15.4 of the amended 2017 SIPS Regulation included a specific requirement related to cyber resilience: "A SIPS operator shall establish an effective cyber resilience framework . . . to manage cyber risk. The SIPS operator shall identify its critical operations and supporting assets, and have appropriate measures in place to protect them from, detect, respond to and recover from cyber attacks."[59] This requirement largely reflects the structure of the CROE, and operators are expected to use the CROE as the basis for demonstrating compliance with the SIPS Regulation. Additionally, SIPS operators have to establish, test, and review, at least annually, a business continuity plan that addresses events that significantly risk disrupting the SIPS' operations. It is required that the business continuity plan ensures that critical IT systems can resume operations within two hours following disruptive events.

Developments in European Cybersecurity Regulation

The previous sections show the progress that has been achieved during the past ten years in the area of ICT and cybersecurity legislation for the financial sector in Europe. Many financial institutions are subject to some sort of ICT and cybersecurity legislation. However, currently, there are still gaps in the regulatory landscape, and the multitude of legislation and standards leave room for confusion. It is therefore important for European decisionmakers to further improve their legislation. In its political guidelines for the years 2019–2024, the newly elected EC emphasizes digitalization and security as two sides of the same coin, calling on the EU to grasp the opportunities from digitalization within safe and ethical boundaries.[60] This resonates with the EC's FinTech Action Plan, which was published on March 8, 2018, and initiated several actions in the field of cybersecurity for the EU. As an outcome of this plan, the EC asked the ESAs for their joint technical advice on the existing regulation and supervisory practices in the area of ICT risks and cybersecurity, as well as the cost and benefits of developing a coherent cyber resilience testing framework for significant market participants and infrastructures within the whole EU financial sector. In their conclusions, the ESAs proposed measures in four major fields of action: requirements on ICT security and risk management, sectoral cyber incident reporting requirements, direct oversight and supervision of third-party providers, and a cyber resilience testing framework. [61]

Based on both this motivation and public consultations, the EC adopted a digital finance package in September 2020 to further enable and support the potential of digital finance in terms of innovation and competition while mitigating the risks arising from it. The package includes a legislative proposal on digital resilience for the European financial sector, called DORA. DORA is a legislative proposal by the EC aiming to introduce a harmonized and comprehensive framework on digital operational resilience for European financial institutions and responds to the ESAs conclusions in their joint technical advice. The draft legislation of DORA will be transferred to the European Parliament and to the Council of Ministers for review and adoption. Both groups of legislators can still introduce additional amendments to the final version of the legislation.

The shift toward operational resilience is right in line with the prevalent international opinion. Cyber risk is no longer confined to the area of IT and systems. With an accelerated digital transformation, cyber risks are now inherent to all functions, products, and services of financial institutions. To manage these risks and their impact on business, financial institutions need to change their mindset from purely focusing on the technical aspects and security. Cyber risk management needs to be incorporated into a broader strategic perspective, starting from the executive board level of financial

institutions, as part of an overall operational resilience against the complex threat landscape externally and the risks associated with the digital innovations internally. The following paragraphs will present the conclusions reached by the ESAs in the four major fields of action and map them to the proposed measures laid out in DORA.

Requirements on ICT Security and Risk Management

In their "Joint Advice of the European Supervisory Authorities," the ESAs paint a scattered picture of European ICT and cybersecurity regulation.[62] The ESAs conclude that "while operational risk requirements are generally in place in the sectoral legislation, there is typically a lack of explicit references to ICT and cyber security risk."[63] Such a "fragmented regulatory and supervisory landscape . . . could lead to non-convergent practices across Europe and endanger the level-playing field."[64] The ESAs therefore advise that, in the respective subsectors, every relevant entity should be subject to "general requirements on governance of ICT, including cyber security, to ensure safe provision of regulated services."[65] Such a harmonization would help to promote greater ICT security and cybersecurity.

In the short term and in light of the diverging maturity levels of the respective financial subsectors, the ESAs spelled out different proposals for each of them: banking and payments, insurance and reinsurance, and securities markets.[66] In the area of banking and payments, the recommendations of the ESAs are already fulfilled by the EBA Guidelines on ICT and Security Risk Management detailed above. For insurance and reinsurance companies, the European Insurance and Occupational Pensions Authority (EIOPA) has released draft Guidelines on ICT for Consultation.[67] The EIOPA Guidelines cover the areas of governance and risk management, ICT operations security, and ICT operations management, and have been drafted based on the abovementioned EBA Guidelines to ensure consistency across subsectors.[68] For FMIs, the European Securities and Markets Authority (ESMA) still sees the greatest need for legislative improvements to streamline and harmonize regulatory requirements and definitions. To address this, ESMA proposed that the EC should consider introducing specific references to cybersecurity in areas of legislation where such references are currently absent.[69]

With the proposal of DORA, the EC directly responded to the recommendations by the ESAs.[70] The EC acknowledges the risks that can arise from the lack of detailed and comprehensive rules in this field. Therefore, the EC proposes DORA to have very broad applications and to cover almost all financial institutions from all three subsectors in addition to ICT third-party providers.[71] The pro-

posed legislation sets out specific requirements in respect to governance and ICT risk management as well as contractual arrangements between ICT third-party service providers and financial entities. DORA describes digital operational resilience as rooted in a set of key principles and requirements on an ICT risk management framework revolving around specific functions in ICT risk management (identification, protection and prevention, detection, response and recovery, learning and evolving, and communication). It suggests requiring financial entities to set up and maintain resilient ICT systems and tools that minimize the impact of ICT risk; to identify on a continuous basis all sources of ICT risk; to set up protective, preventive, and detective measures; and to put in place dedicated and comprehensive business continuity policies and disaster and recovery plans as an integral part of the operational business continuity policy. The regulation does not itself impose specific standardization, but rather builds on European and internationally recognized technical standards or industry best practices.

Harmonization is not only important on a horizontal dimension between subsectors. Some member states already have national standards in place, and it needs to be ensured that these correspond to the European standards as well. This vertical harmonization between European and national standards has to be backed by a coherent supervision of these standards.

Sectoral Cyber Incident Reporting Regimes

As shown above, there currently exist several different cyber incident reporting regimes for financial institutions in the EU. For future action, the ESAs propose a streamlining of existing reporting regimes. They point out the fact that different reporting schemes have different purposes, and as a result, no incident reporting requirements should be removed. Instead, they suggest that existing incident reporting requirements should be streamlined by clarifying any overlapping provisions and standardizing reporting templates, taxonomy, and timeframes where possible. This would improve operational resilience and business continuity as it would aid smooth and efficient interactions between authorities. Lastly, these efforts would also help avoid inconsistencies in the reported information.[72] ESMA proposed the introduction of an incident reporting regime for entities in its remit that are currently not subject to such requirements.[73]

In its current form, DORA aims to achieve harmonization and streamlining of incident reporting by first requiring financial entities to establish and implement a specific ICT-related incident management process to identify, track, log, categorize, and classify ICT-related incidents. Classification criteria should be developed by a joint committee of the ESAs. Further, financial entities will be obligated to report all major ICT-related incidents to the competent authority, within

the time frames prescribed and by using harmonized reporting templates. While this approach still relates on multiple incident reporting schemes and competent authorities, the possibility of EU-level centralization of ICT-related incident reporting should be further explored in a joint report by the ESAs, ECB, and ENISA assessing the feasibility of establishing a single EU hub for major ICT-related incident reporting by financial entities.

Framework for Direct Oversight and Supervision of Third-Party Service Providers

In recent years, TPPs have become more important, especially those involved in data services and cloud computing for the European financial sector.[74] As shown above, current policies concerning outsourcing arrangements emphasize the accountability of outsourcing parties for the outsourced services as well as the responsibility for the risk management and regulatory compliance of these services.[75] Because TPPs are not in the regulatory remit of financial sector supervisory authorities, they cannot be directly addressed by these standards or supervised by the authorities. However, several standard-setting bodies have raised awareness of the risks in correlation to third-party service providers.[76] The European Systemic Risk Board has identified insufficient industry oversight of TPPs as one common cybersecurity vulnerability among financial institutions in Europe.[77] On a systemic level, the limited number of important cloud service providers that dominate the financial sector raises concerns about potential concentration risks in these entities. A large-scale operational failure at such a critical TPP could ultimately result in system-wide disruption and systemic effects (all from a single point of failure).[78] To address these risks, the ESAs propose that the EC should develop a legislative solution for an oversight framework for monitoring the activities of critical TPPs to relevant financial institutions.[79] Because many major TPPs to the financial services sector reside outside the EU, the ESAs recognise that efforts in this respect need to be made at global level.[80]

DORA aims to address the risks stemming from TPPs in multiple ways. First, the regulation harmonizes key elements of TPPs' services to and relationships with various financial institutions, including a requirement for the financial institution to monitor TPP risk throughout the life cycle of the relationship as well as obligations to include contractual requirements for the TPP, such as rights of access, inspection, audit, as well as termination rights and exit strategies.

Further, the draft legislation sets out a separate set of provisions applicable to critical third-party service providers (CTPPs), which will be designated by the ESA's joint committee on the basis of a list of criteria set out in DORA. The proposed legislation requires an oversight framework of CTPPs responsible for, among other tasks, verifying that CTPPs have in place the right controls to manage the risks that CTPPs may pose to financial entities and to the overall financial stability.[81] The over-

sight framework is equipped with far-reaching powers, including the unrestricted right to access all information deemed necessary by an ESA that would be named lead overseer. The lead overseer would also have the power to conduct general investigations (including on-site inspections) of ICT third-party service providers. Finally, CTPPs would be charged oversight fees designed to cover all of the ESA's necessary expenditure in relation to conduct of oversight tasks.

Cyber Resilience Testing Framework

In its FinTech Action Plan, the EC notes an increase in mandated supervisory penetration and resilience testing frameworks to assess the effectiveness of cyber defenses and security requirements.[82] This development adds to the already existing industry practice of resilience testing. However, as many market participants operate on a cross-border basis, the EC warns of risk in multiplying testing frameworks, especially raising costs for institutions and increasing potential fragmentation.[83] The EC acknowledges the effort of the ECB and Eurosystem in their development of TIBER-EU (see box 2).[84]

BOX 2

Threat Intelligence-Based Ethical Red Teaming

A first step toward harmonizating cyber resilience testing frameworks has been achieved with the publication of the TIBER-EU by the ECB.[85] TIBER-EU serves as a voluntary framework for European and national authorities to support their most systemic entities in conducting intelligence-based red team tests.[86] Red teaming is a type of cyber resilience testing that simulates the whole scenario of a targeted attack against an entity. In this test, the red team tries to attack an institution's critical functions and underlying systems by using tactics, techniques, and procedures of real potential threat actors. While the defending blue team, made up of the institution's security team, has no knowledge of the test, a white team (such as the institution's executives) manages the end-to-end test and obverses the attack, ensuring it is conducted in a controlled manner. The framework obligates the exercise to be based on threat intelligence about the involved entity to test a realistic scenario for a potential attack. A TIBER-EU test must be overseen by the TIBER Cyber Team, which is the team from the national authority that has adopted the framework. The TIBER Knowledge Centre brings together all the TIBER cyber teams from the national or European implementations, enabling sharing of best practices and an effort to ensure harmonization of the framework. Currently there is neither an obligation for authorities to implement the framework, nor for selected entities to participate in the program. The framework is based on similar national cyber resilience testing frameworks, including CBEST in the UK and TIBER-NL in the Netherlands.[87] There are several member states in the EU that are implementing TIBER-EU in their jurisdiction.

In their analysis on the development of a coherent resilience testing framework, the ESAs see the benefit of a coherent framework in the potential increase of cyber risk awareness and knowledge exchange.[88] Due to the heterogeneity of the cyber maturity of the European financial sector, the ESAs suggest to first focus on creating a baseline of cyber resilience across the financial sectors before creating a coherent testing framework.[89] As stated above, EBA has already defined some requirements concerning resilience testing in their ICT guidelines. EIOPA is promoting pilot discussions about tests in large insurance groups, and ESMA plans to first focus on the cybersecurity maturity level of the institutions in its remit.[90]

The proposal for DORA sketches out a framework for a proportionate application of digital operational resilience testing requirements depending on the size, business, and risk profiles of financial entities. The framework sets out a testing of ICT tools and systems for all entities, but it requires a set of financial institutions identified by competent authorities based on specific criteria to be significant and cyber mature to conduct advanced testing based on red teaming.

Recommendations

The described plans of the EC and the ESAs in the area of ICT and cybersecurity regulation are crucial for a secure digital transformation and an increased level of cyber resilience of European financial institutions. With the proposed regulation DORA, the EC addresses the most urgent issues and goes beyond current structures to lead the way toward the future viability of the European financial sector. This section provides recommendations that stress upon, improve upon, or complement the existing initiatives to achieve a consistent, effective, and comprehensive legislative landscape for the European financial sector.

A Single European Cybersecurity Legislation

While harmonization of financial sector legislation in the past often served to lower the burden on the regulated entities and to prevent regulatory arbitrage, it has to become a top priority for addressing cyber risk. This is due to the fact that cyber risk can intrude a system at the weakest link and then spread through the whole network. A cyber attack is not bound to country and sector borders, as shown by global cyber attacks such as the WannaCry and NotPetya attacks.[91] This makes a basic level of cybersecurity in all financial institutions, regardless of the subsector, crucial for quickly achieving operational resilience. The need for harmonization is further emphasized by the fact that a lack in basic cybersecurity measures (called cyber hygiene) still underlines most successful cyber attacks.[92] As shown by this paper, the current legislative situation in the EU is highly complex and scattered between subsectors, topics, and nation-states. This fragmented situation will likely lead to confusion

and serve as an obstacle to the objective of further harmonization. The proposed DORA regulation by the EC is a solution to this problem. As a common single legislation addressing most European financial subsectors, it can ensure harmonization and baseline requirements concerning ICT and other cyber risks. To ensure this level of harmonization, the DORA proposal needs to be adopted and its core left unchanged by the upcoming review from the European Parliament and the European Council.

Shift to a Risk-centric Approach

A harmonized basic level of security requirements for all financial institutions has to be accompanied by a shift to a risk-centric approach for more mature institutions. To date, many financial institutions' security focus is on compliance with current regulations. This compliance-centric view can be rational, especially for smaller or less mature institutions, but it needs to be substituted with increasing maturity or size by a risk- or threat-centric approach to achieve cyber resilience. In order to operate in a risk-centric way, financial institutions need to know their most valuable assets, vulnerabilities, and the threats they face. Legislation can help bigger financial institutions to adopt a risk-centric perspective. Frameworks such as TIBER-EU and the requirements laid out in the proposed DORA regulation can improve resilience by confronting financial institutions with real-world tactics, techniques, and procedures of cyber adversaries and force them to defend against these attacks. These exercises reveal vulnerabilities in the attacked institutions that might have been overlooked by solely fulfilling compliance.

Another strong activity for achieving resilience—not only for the institution but also on a systemic scale—is conducting tabletop exercises between financial institutions and their supervisory authorities. Tabletop exercises evaluate an institution's cyber crisis processes, tools, and proficiency in responding to cyber attacks from both a strategic and technical response perspective. These exercises simulate real challenges that help decisionmakers to identify missing links in the chain of command and gaps in their response and recovery plans. Additionally, such exercises put a spotlight on the human and psychological factor of a response to a cyber attack.

Other jurisdictions have already included such exercises into the toolkit of their respective supervisory authorities. In Europe so far, there have only been individual initiatives, such as the market-wide communication exercise by the Eurosystem's Market Infrastructure and Payments Committee in 2018 and ENISA's biannual European cyber exercise called Cyber Europe. However, these initiatives need to be tailored to the financial sector and conducted in a regular, comprehensive manner as part

of the supervisory methodology. Additionally, tabletop exercises can prove useful for improving the coordination between different European as well as national public authorities as the G7 exercise on cross-border communication conducted in 2019 has shown.[93]

Cyber Risk is a Systemic Risk

In a recent report, the European Systemic Risk Board has identified cyber risk as a source of systemic risk for the financial system.[94] The report concludes that a cyber attack could potentially trigger an instability in the financial system, possibly resulting in a financial crisis. Current legislation only focuses on the single institution, leaving out the systemic perspective. While a common and harmonized level of cybersecurity of all financial institutions mitigates risk—not only for the single institution but also for the system—further measures can be taken.

First, similar to the current higher capital requirements for systemically important financial institutions under Basel III, systemic cybersecurity requirements could put stricter standards on systemically important institutions. While Basel III only applies to credit institutions, these security requirements would need to be applied to all systemically important financial institutions independent of the subsector. The significance of a financial institution might have to be assessed based on further criteria than under Basel III. For example, a new set of requirements should consider the systemic impact of an operational disruption as well as interdependence from an ICT risk perspective.

A second measure to mitigate systemic risk could involve the collection of data from different European incident reporting regimes in a single institution, thereby gathering information to form a systemic perspective on patterns of current threats and vulnerabilities to the European financial sector. And finally, measures against systemic cyber risk cannot be limited to the financial sector but have to incorporate the interdependencies with TPPs. The proposed DORA legislation acknowledges the systemic nature of cyber risks and comprises several initiatives to address it, including the fostering of information exchange from incident reporting regimes and an increased scrutiny on the role and interdependencies of TPPs.

Foster Cooperation on All Levels

Cooperation between stakeholders in the sphere of cybersecurity is a necessity and can take many forms, from informal exchanges on best practices to information sharing of concrete threats or vulnerabilities. Unfortunately, many financial institutions are cautious toward strong cooperation

with other private institutions out of reasons of competition or confidentiality. The same is true for all cooperation with public authorities that exceeds the legally obligated level, because many financial institutions fear supervisory consequences if they share too much information. In order to overcome these concerns, cooperation needs to be fostered in all forms.

In its proposed DORA regulation, the EC permits financial institutions to exchange information and intelligence among themselves. However, to increase the number of voluntary participants and maximize the output of such initiatives, further coordination from a European perspective is needed. Two initiatives that can be named as an example are, first, the CIISI-EU launched by the Euro Cyber Resilience Board, which brings together a community of public authorities and private financial infrastructures with the aim of sharing intelligence and exchanging best practices. A second example is the European Financial Institutes–Information Sharing and Analysis Centre established by ENISA as a self-supporting group for information exchange, with members consisting of country representatives from the financial sector, ECB, and national and governmental computer emergency response teams, as well as law enforcement agencies and other European organizations. While these initiatives are a great start, they currently focus on the voluntary involvement of financial institutions, are in some cases focused on a subsector (for example, financial market infrastructures and payment providers in CIISI-EU), and mostly involve larger financial institutions. It is therefore recommendable to expand and enhance these initiatives to optimize the cooperation and information exchange in the European financial sector. Further, cyber risk cooperation is needed not only within the financial sector but also across critical sectors. Here, a risk-based approach could be to first focus on an exchange between the finance, energy, and telecommunications sectors, which are all highly interdependent.

ENISA could take up a crucial role as a central hub for these initiatives. With the EU Cybersecurity Act (passed in 2019), the EC gave ENISA a reinforced role in European cybersecurity with a permanent mandate and enhanced areas of responsibility. These include the support of capacity-building across the EU for member states, public authorities, and private stakeholders with the objective to raise ICT and cyber resilience as well as the development of skills in cybersecurity.[95] These new responsibilities set ENISA up perfectly to foster and coordinate cross-sector cooperation and information sharing of public and private stakeholders across the EU.

Conclusion

The current landscape concerning cyber regulation in the European financial sector is complex and scattered between different subsector's sector-level legislation as well as national and European competencies. For a financial institution operating in different European countries, it proves a

challenge to stay on top of regulation to be fully compliant. This paper provides a comprehensive overview of the most relevant legislation and standards in this field, thereby also acknowledging the large focus that European regulators have put on this topic in the recent years.

During the next four years, the current EC administration plans to evolve legislation on cybersecurity in four fields of action, including building frameworks for cyber resilience testing, direct oversight of third-party service providers, a digital finance strategy, and an emphasis on operational resilience. These initiatives prudently respond to and advance the existing landscape and, in the long term, incorporate industry developments such as operational resilience into the regulatory context. Finally, the paper gives four high-level recommendations in addition to the future European plans to fill missing gaps and shape a consistent, effective, and comprehensive legislative landscape. A high-level, single European legislation across all subsectors of the financial system can provide a signal effect and help foster a consistent level of security in all European financial institutions.

About the Authors

Philipp S. Krüger is managing director at Accenture Security for Germany, Switzerland, and Austria. He was the founding architect of the Federal Cyber Agency, Germany's first agency modeled on the U.S. Defense Advanced Research Projects Agency (DARPA), run by the German Ministry of Defense. Previously he was the founding managing director of the National Digital Hub Cybersecurity, part of the Federal Ministry for Economic Affairs and Energy. Krüger works on large-scale digital transformation, cyber strategy, cybersecurity, and big data. He is a nonresident fellow at the Institute for Security Policy at Christian-Albrechts-University Kiel and alumnus of Fraunhofer-Gesellschaft, Harvard's Kennedy School of Government, and M.I.T. Media Lab.

Jan-Philipp Brauchle is a consulting manager at Accenture Security in Germany. He works on strategy projects in the financial services sector.

Notes

1 Aquiles A. Almansi and Yejin Carol Lee, "Financial Sector's Cybersecurity: A Regulatory Digest," World Bank Group Financial Sector Advisory Center, May 2019, http://pubdocs.worldbank.org/en/208271558450284768/CybersecDigest-3rd-Edition-May2019.pdf.

2 For more information on the regulatory process in financial services of the European Union, see European Commission, "Regulatory Process in Financial Services," accessed February 24, 2021, https://ec.europa.eu/info/business-economy-euro/banking-and-finance/regulatory-process-financial-services/regulatory-process-financial-services_en. This paper focuses on three main subsectors of the financial sector, namely banking and payments, reinsurance, and financial market infrastructures. These groups fall into the remit of different supervisory authorities and have to adhere to different Level 1 regulations.

3 For a overview on the European regulatory process for financial services, see ibid.

4 The ESAs are comprised of the EBA, EIOPA, and ESMA. For the joint technical advice, see European Supervisory Authorities, "Joint Advice of the European Supervisory Authorities to the European Commission on the Need for Legislative Improvements Relating to ICT Risk Management Requirements in the EU Financial Sector," April 10, 2019, https://www.esma.europa.eu/sites/default/files/library/jc_2019_26_joint_esas_advice_on_ict_legislative_improvements.pdf; and European Supervisory Authorities, "Joint Advice of the European Supervisory Authorities To the European Commission on the Costs and Benefits of Developing a Coherent Cyber Resilience Testing Framework for Significant Market Participants and Infrastructures Within the Whole EU Financial Sector," April 10, 2019, https://www.esma.europa.eu/sites/default/files/library/jc_2019_25_joint_esas_advice_on_a_coherent_cyber_resilience_testing_framework.pdf.

5 See European Commission, "Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions; Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace," February 7, 2013, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013JC0001&from=EN.

6 The European Parliament and the Council of the European Union, "Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union," July 19, 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=DE; and Financial Stability Board, "Stocktake of Publicly Released Cybersecurity Regulations, Guidance and Supervisory Practices," October 13, 2017, https://www.fsb.org/wp-content/uploads/P131017-2.pdf.

7 The European Parliament and the Council of the European Union, "Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union," July 19, 2016, articles 14 (3) and 14 (4), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=DE.

8 The NIS Directive applies similar reporting requirements to so-called digital service suppliers (DSPs), including online marketplaces, online search engines, and cloud computing services. In contrast to OES, DSPs do not fall under ex-ante supervisory control by regulators but can only be acted upon after an incident has occurred. See NIS Cooperation Group, "Reference Document on Incident Notification for Operators of Essential Services Circumstances of Notification," February 2018, https://ec.europa.eu/information_society/newsroom/image/document/2018-30/reference_document_incident_reporting_00A3C6D5-9BDB-23AA-240AF504DA77F0A6_53644.pdf.

9 BaFin, "Kritische Infrastrukturen: BaFin ergänzt BAIT um KRITIS-Modul" (BaFin Enhances Supervisory Requirements for IT in Financial Institutions with a Critical Infrastructure Module), September 2018, https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Meldung/2018/meldung_180914_Ueberarbeitung_BAIT.html.

10 The European Parliament and the Council of the European Union, "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)," May 4, 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=DE.

11 The notification shall at least describe the nature of the personal data breach, including, where possible, the categories and approximate number of data subjects concerned, the categories and approximate number of personal data records concerned, and the likely consequences of the personal data breach. See European Parliament and the Council of the European Union, "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)," May 4, 2016, article 33, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=DE.

12 European Commission, "Commission Proposes a Comprehensive Reform of Data Protection Rules to Increase Users' Control of Their Data and to Cut Costs for Businesses," January 2012, https://ec.europa.eu/commission/presscorner/detail/en/IP_12_46.

13 Katie Nolan, "GDPR: Harmonization or Fragmentation? Applicable Law Problems in EU Data Protection Law," Berkley Technology Law Journal (blog), University of California, Berkley School of Law, January 20, 2018, https://btlj.org/2018/01/gdpr-harmonization-or-fragmentation-applicable-law-problems-in-eu-data-protection-law.

14 Trends such as high-frequency trading also show the competitive advantage technology can give a financial market participant.

15 In earlier legislation, ICT and cybersecurity were treated as a subcategory of operational risk and were only addressed implicitly. This is still the case with regulation in the insurance and financial market infrastructure remit.

16 Basel Committee on Banking Supervision, "Basel III: A Global Regulatory Framework for More Resilient Banks and Banking Systems," Bank for International Settlements, December 2010, 1, https://www.bis.org/publ/bcbs189_dec2010.pdf.

17 European Commission, "Capital Requirements—CRD IV/CRR—Frequently Asked Questions," July 16, 2013, https://ec.europa.eu/commission/presscorner/detail/en/MEMO_13_690.

18 The European Parliament and the Council of the European Union, "Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on Access to the Activity of Credit Institutions and the Prudential Supervision of Credit Institutions and Investment Firms, Amending Directive 2002/87/EC and Repealing Directives 2006/48/EC and 2006/49/EC," June 27, 2013, articles 74 and 85, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013L0036&from=EN.

19 Financial Stability Board, "Stocktake of Publicly Released Cybersecurity Regulations, Guidance and Supervisory Practices," October 13, 2017, https://www.fsb.org/wp-content/uploads/P131017-2.pdf.

20 The guidelines came into force on September 30, 2019. See European Banking Authority, "Final Report on EBA Guidelines on Outsourcing Arrangements," February 25, 2019, https://eba.europa.eu/sites/default/documents/files/documents/10180/2551996/38c80601-f5d7-4855-8ba3-702423665479/EBA%20revised%20Guidelines%20on%20outsourcing%20arrangements.pdf; and European Banking Authority, "Final Report: Guidelines on the Security Measures for Operational and Security Risks of

Payment Services Under Directive (EU) 2015/2366 (PSD2)," December 12, 2017, https://eba.europa.eu/sites/default/documents/files/documents/10180/2060117/d53bf08f-990b-47ba-b36f-15c985064d47/Final%20report%20on%20EBA%20Guidelines%20on%20the%20security%20measures%20for%20operational%20and%20security%20risks%20under%20PSD2%20(EBA-GL-2017-17).pdf. These guidelines were based on the 2006 CEBS outsourcing guidelines. For the 2006 guideliens, see Committee of European Banking Supervisors, "Guidelines on Outsourcing," December 14, 2006, https://eba.europa.eu/sites/default/documents/files/documents/10180/104404/6300a204-2d64-494f-b81e-fd3e235a74bb/GL02OutsourcingGuidelines.pdf.pdf.

21 SREP is a set of procedures carried out on an annual basis by the supervisory authorities to ensure each credit institution has in place the strategies, processes, capital, and liquidity that are appropriate to the risks to which it is or might be exposed. See European Banking Authority, "Final Report: Guidelines on ICT Risk Assessment Under the Supervisory Review and Evaluation Process (SREP)," May 11, 2017, https://eba.europa.eu/sites/default/documents/files/documents/10180/1841624/ef88884a-2f04-48a1-8208-3b8c85b2f69a/Final%20Guidelines%20on%20ICT%20Risk%20Assessment%20under%20SREP%20(EBA-GL-2017-05).pdf.

22 See European Parliament and the Council of the European Union, "Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on Payment Services in the Internal Market, Amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and Repealing Directive 2007/64/EC," December 23, 2015, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L2366&from=EN.

23 Organizations that are neither credit institutions nor electronic money institutions can apply for an authorization as a payment institution if they meet certain capital and risk management requirements.

24 For more examples of interplay between PSD2 and GDPR, see "EU: The Interplay of PSD2 and GDPR—Some Select Issues," OneTrust DataGuidance, March 2019, https://www.dataguidance.com/opinion/eu-interplay-psd2-and-gdpr-some-select-issues.

25 European Banking Authority, "Final Report: Draft Regulatory Technical Standards on Strong Customer Authentication and Common and Secure Communication Under Article 98 of Directive 2015/2366 (PSD2)," February 23, 2017, https://eba.europa.eu/sites/default/documents/files/documents/10180/1761863/314bd4d5-ccad-47f8-bb11-84933e863944/Final%20draft%20RTS%20on%20SCA%20and%20CSC%20under%20PSD2%20%28EBA-RTS-2017-02%29.pdf.

26 Two-factor authentication (2FA) is a second layer of security a user has to go through before being granted access to an account or system. 2FA increases the safety of accounts by requiring an additional item to the user's password—such as a PIN, a one-time password, a registered device, or fingerprint—before the user can log in.

27 Some examples of exemptions for these rules are remote payments of low value (up to 30 euro, or $36) or contactless card payments up to 50 euro ($60).

28 The account servicing payment service provider has to provide the payment initiation service provider (PISP) or account information service provider (AISP) with a secure communication channel to provide access to the payment account. This can be done either via a dedicated application programming interface for the AISP/PISP or the direct accesses by the AISP/PISP to the customer's payment account by using their interface and their personalized security credentials.

29 European Banking Authority, "Final Report: Guidelines on ICT Risk Assessment Under the Supervisory Review and Evaluation Process (SREP)," May 11, 2017, https://eba.europa.eu/sites/default/documents/files/documents/10180/1841624/ef88884a-2f04-48a1-8208-3b8c85b2f69a/Final%20Guidelines%20on%20ICT%20Risk%20Assessment%20under%20SREP%20(EBA-GL-2017-05).pdf.

30 The European Single Supervisory Mechanism (SSM) has implemented a cyber incident reporting framework that requires all significant institutions in its remit to report significant cyber incidents. The reporting regime enables the SSM to identify and monitor trends in cyber incidents affecting significant institutions and to gain a deeper knowledge of the cyber threat landscape. For all countries where incident reporting regimes are already in place, the banks will report these to their national superviser, who will then forward the reports to the SSM.

31 European Banking Authority, "Final Report: Guidelines on Major Incident Reporting Under Directive (EU) 2015/2366 (PSD2)," July 27, 2017, https://eba.europa.eu/sites/default/documents/files/documents/10180/1914076/3902c3db-c86d-40b7-b875-dd50eec87657/Guidelines%20on%20incident%20reporting%20under%20PSD2%20(EBA-GL-2017-10).pdf.

32 European Banking Authority, "Final Report: EBA Guidelines on ICT and Security Risk Management," November 29, 2019, https://eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2020/GLs%20on%20ICT%20and%20security%20risk%20management/872936/Final%20draft%20Guidelines%20on%20ICT%20and%20security%20risk%20management.pdf.

33 The EBA Guidelines on ICT and Security Risk Management further built on earlier EBA reports; see European Banking Authority, "Final Report: Guidelines on ICT Risk Assessment Under the Supervisory Review and Evaluation Process (SREP)," May 11, 2017, https://eba.europa.eu/sites/default/documents/files/documents/10180/1841624/ef88884a-2f04-48a1-8208-3b8c85b2f69a/Final%20Guidelines%20on%20ICT%20Risk%20Assessment%20under%20SREP%20(EBA-GL-2017-05).pdf; and European Banking Authority, "Final Report on EBA Guidelines on Outsourcing Arrangements," February 25, 2019, https://eba.europa.eu/sites/default/documents/files/documents/10180/2551996/38c80601-f5d7-4855-8ba3-702423665479/EBA%20revised%20Guidelines%20on%20outsourcing%20arrangements.pdf.

34 The European Parliament and the Council of the European Union, "Directive 2009/138/EC of the European Parliament and of the Council of 25 November 2009 on the Taking-up and Pursuit of the Business of Insurance and Reinsurance (Solvency II)," December 17, 2009, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013L0036&from=EN.

35 Ibid., article 41.

36 Ibid., article 41 (4).

37 Ibid., article 44.

38 Federal Financial Supervisory Authority, "Supervisory Requirements for IT in Insurance Undertakings," November 22, 2018, https://www.bafin.de/SharedDocs/Downloads/EN/Rundschreiben/dl_rs_1810_vait_va_en.html?nn=9866146.

39 While lists of financial institutions considered as FMIs vary, this paper includes SIPS, CSDs, SSSs, CCPs, TRs, CRAs, and trade exchanges.

40 The Eurosystem comprises the ECB and the national central banks of those countries that have adopted the euro as a currency.

41 European Central Bank, "Cyber Resilience Oversight Expectations for Financial Market Infrastructures," December 2018, https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf.

42 Ibid., 3.

43 The European Parliament and the Council of the European Union, "Regulation (EU) No 600/2014 of the European Parliament and of the Council of 15 May 2014 on Markets in Financial Instruments and Amending Regulation (EU) No 648/2012," June 12, 2014, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0600&from=EN.

44 European Commission, "Commission Delegated Regulation (EU) 2017/584 of 14 July 2016 Supplementing Directive 2014/65/EU of the European Parliament and of the Council with Regard to Regulatory Technical Standards Specifying Organisational Requirements of Trading Venues," March 31, 2017, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R0584&from=EN.

45 See The European Parliament and the Council of the European Union, "Regulation (EU) No 600/2014 of the European Parliament and of the Council of 15 May 2014 on Markets in Financial Instruments and Amending Regulation (EU) No 648/2012," June 12, 2014, article 16 (5), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0600&from=EN.

46 The European Parliament and the Council of the European Union (2012), "Regulation (EU) No 648/2012 of the European Union and of the Council of 4 July 2012 on OTC Derivatives, Central Counterparties and Trade Repositories," July 27, 2012, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32012R0648&from=EN.

47 European Commission, "Commission Delegated Regulation (EU) 2017/392 of 11 November 2016 Supplementing Regulation (EU) No 909/2014 of the European Parliament and of the Council with Regard to Regulatory Technical Standards on Authorisation, Supervisory and Operational Requirements for Central Securities Depositories," March 10, 2017, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R0392&from=DE.

48 The European Parliament and the Council of the European Union, "Regulation (EU) No 648/2012 of the European Union and of the Council of 4 July 2012 on OTC Derivatives, Central Counterparties and Trade Repositories," July 27, 2012, article 9 (3), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32012R0648&from=EN.

49 Ibid., articles 79 (1) and 80 (1).

50 Ibid., article 79 (2).

51 The European Parliament and the Council of the European Union, "Regulation (EU) No 909/2014 of the European Parliament and of the Council of 23 July 2014 on Improving Securities Settlement in the European Union and on Central Securities Depositories and Amending Directives 98/26/EC and 2014/65/EU and Regulation (EU) No 236/2012," August 28, 2014, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0909&from=DE.

52 European Commission, "Commission Delegated Regulation (EU) 2017/392 of 11 November 2016 Supplementing Regulation (EU) No 909/2014 of the European Parliament and of the Council with Regard to Regulatory Technical Standards on Authorisation, Supervisory and Operational Requirements for Central Securities Depositories," March 10, 2017, article 70, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R0392&from=DE.

53 Ibid., articles 75 (5) and 75 (1).

54 The European Parliament and the Council of the European Union, "Regulation (EC) No 1060/2009 of the European Parliament and of the Council of 16 September 2009 on Credit Rating Agencies," November 17, 2009, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:302:0001:0031:EN:PDF.

55 Ibid., annex I, section A, article 6 (2).

56 Ibid.

57 European Central Bank, "Regulation of the European Central Bank (EU) No 795/2014 of 3 July 2014 on Oversight Requirements for Systemically Important Payment Systems," July 23, 2014, https://www.ecb.europa.eu/ecb/legal/pdf/oj_jol_2014_217_r_0006_en_txt.pdf.

58 European Central Bank, "Payment Systems," accessed January 28, 2021, https://www.ecb.europa.eu/paym/pol/activ/systems/html/index.en.html.

59 European Central Bank, "Regulation of the European Central Bank (EU) No 795/2014 of 3 July 2014 on Oversight Requirements for Systemically Important Payment Systems," July 2014, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:02014R0795-20171206&from=LV.

60 Ursula Von der Leyen, "A Union That Strives for More: My Agenda for Europe; Political Guidelines for the Next European Commission 2019–2024," 2019, https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_en.pdf.

61 European Supervisory Authorities, "Joint Advice of the European Supervisory Authorities To the European Commission on the Need for Legislative Improvements Relating to ICT Risk Management Requirements in the EU Financial Sector," April 10, 2019, https://www.esma.europa.eu/sites/default/files/library/jc_2019_26_joint_esas_advice_on_ict_legislative_improvements.pdf; and European Supervisory Authorities, "Joint Advice of the European Supervisory Authorities To the European Commission on the Costs and Benefits of Developing a Coherent Cyber Resilience Testing Framework for Significant Market Participants and Infrastructures Within the Whole EU Financial Sector," April 10, 2019, https://www.esma.europa.eu/sites/default/files/library/jc_2019_25_joint_esas_advice_on_a_coherent_cyber_resilience_testing_framework.pdf.

62 European Supervisory Authorities, "Joint Advice of the European Supervisory Authorities To the European Commission on the Need for Legislative Improvements Relating to ICT Risk Management Requirements in the EU Financial Sector," April 10, 2019, https://www.esma.europa.eu/sites/default/files/library/jc_2019_26_joint_esas_advice_on_ict_legislative_improvements.pdf.

63 Ibid., 4.

64 Ibid., 10.

65 Ibid., 4.

66 European Supervisory Authorities, "Joint Advice of the European Supervisory Authorities To the European Commission on the Need for Legislative Improvements Relating to ICT Risk Management Requirements in the EU Financial Sector," April 10, 2019, https://www.esma.europa.eu/sites/default/files/library/jc_2019_26_joint_esas_advice_on_ict_legislative_improvements.pdf.

67 European Insurance and Occupational Pensions Authority, "Consultation on the Proposal for Guidelines on Information and Communication Technology (ICT) Security and Governance," December 12, 2019, https://www.eiopa.europa.eu/content/consultation-proposal-guidelines-information-and-communication-technology-ict-security-and.

68 European Insurance and Occupational Pensions Authority, "EIOPA Consults on Guidelines on Information and Communication Technology Security and Governance," December 12, 2019, https://www.eiopa.europa.eu/content/eiopa-consults-guidelines-information-and-communication-technology-security-and-governance_en.

69 European Supervisory Authorities, "Joint Advice of the European Supervisory Authorities To the European Commission on the Need for Legislative Improvements Relating to ICT Risk Management Requirements in the EU Financial Sector," April 10, 2019, https://www.esma.europa.eu/sites/default/files/library/jc_2019_26_joint_esas_advice_on_ict_legislative_improvements.pdf.

70 The regulation acknowledges that significant differences exist between financial entities in terms of size and business profiles or in relation to their exposure to digital risk.

71 The following institutions are covered by DORA: credit institutions, payment institutions, electronic money institutions, investment firms, cryptoasset service providers, central securities depositories, CCPs, trading venues, TRs, AIFMs, management companies, data reporting service providers, insurance and reinsurance undertakings, insurance and reinsurance intermediaries, institutions for occupational retirement pensions, CRAs, statutory audit and audit firms, administrators of critical benchmarks, crowdfunding service providers, securitization repositories, and ICT third-party service providers

72 European Supervisory Authorities, "Joint Advice of the European Supervisory Authorities To the European Commission on the Need for Legislative Improvements Relating to ICT Risk Management Requirements in the EU Financial Sector," April 10, 2019, https://www.esma.europa.eu/sites/default/files/library/jc_2019_26_joint_esas_advice_on_ict_legislative_improvements.pdf.

73 Ibid.

74 Financial Stability Board, "Third-party Dependencies in Cloud Services Considerations on Financial Stability Implications," December 9, 2019, https://www.fsb.org/wp-content/uploads/P091219-2.pdf.

75 European Banking Authority, "Final Report on EBA Guidelines on Outsourcing Arrangements," February 25, 2019, https://eba.europa.eu/sites/default/documents/files/documents/10180/2551996/38c80601-f5d7-4855-8ba3-702423665479/EBA%20revised%20Guidelines%20on%20outsourcing%20arrangements.pdf.

76 G7, "G-7 Fundamental Elements for Third Party Cyber Risk Management in the Financial Sector," October 24, 2018, https://www.bundesbank.de/resource/blob/764692/01503c2cb8a58e44a862bee170d34545/mL/2018-10-24-g-7-fundamental-elements-for-third-party-cyber-risk-data.pdf.

77 European Systemic Risk Board, "Systemic Cyber Risk," February 2020, https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf.

78 Financial Stability Board, "Third-party Dependencies in Cloud Services Considerations on Financial Stability Implications," December 9, 2019, https://www.fsb.org/wp-content/uploads/P091219-2.pdf.

79 European Supervisory Authorities, "Joint Advice of the European Supervisory Authorities to the European Commission on the Need for Legislative Improvements Relating to ICT Risk Management Requirements in the EU Financial Sector," April 10, 2019, https://www.esma.europa.eu/sites/default/files/library/jc_2019_26_joint_esas_advice_on_ict_legislative_improvements.pdf.

80 European Supervisory Authorities, "Joint Advice of the European Supervisory Authorities To the European Commission on the Need for Legislative Improvements Relating to ICT Risk Management Requirements in the EU Financial Sector," April 10, 2019, https://www.esma.europa.eu/sites/default/files/library/jc_2019_26_joint_esas_advice_on_ict_legislative_improvements.pdf.

81 European Commission, "Proposal for a Regulation of the European Parliament and the Council on Digital Operational Resilience for the Financial Sector and Amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014," September 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020PC0595&from=EN.

82 Cyber resilience testing can be conducted in different forms with a wide variety of methods and tools. The testing levels can thereby range from a basic white box security testing to the most sophisticated form of threat-lead penetration testing, also known as red teaming. In their "Fundamental Elements for Threat-Led Penetration Testing," the G7 define threat-led penetration training as "a controlled attempt to compromise the cyber resilience of an entity by simulating the tactics, techniques and procedures of real-life threat actors." See G7, "G-7 Fundamental Elements for Threat-led Penetration Testing," October 24, 2018, https://www.bundesbank.de/resource/blob/764690/792725ab3e779617a2fe28a03c303940/mL/2018-10-24-g-7-fundamental-elements-for-threat-led-penetration-testing-data.pdf.

83 European Commission, "Consultation Document: Digital Operational Resilience Framework for Financial Services: Making the EU Financial Sector More Secure," December 23, 2019, https://ec.europa.eu/info/sites/info/files/business_economy_euro/banking_and_finance/documents/2019-financial-services-digital-resilience-consultation-document_en.pdf.

84 European Central Bank, "TIBER-EU Framework: How to Implement the European Framework for Threat Intelligence-based Ethical Red Teaming," May 2018, https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf.

85 European Central Bank, "TIBER-EU Framework: How to Implement the European Framework for Threat Intelligence-based Ethical Red Teaming," May 2018, https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf.

86 Systemic entities include institutions such as commercial and investment banks, payment systems, central counterparties, exchanges, and others.

87 De Nederlandsche Bank, "TIBER-NL Guide: How to Conduct the TIBER-NL Test," November 2017, https://www.dnb.nl/binaries/TIBER-NL%20Guide%20Second%20Test%20Round%20final_tcm46-365448.pdf; and Bank of England Prudential Regulation Authority, "CBEST Intelligence-Led Testing CBEST Implementation Guide," 2016, https://www.bankofengland.co.uk/-/media/boe/files/financial-stability/financial-sector-continuity/cbest-implementation-guide.pdf. TIBER-NL is set up from a financial stability perspective and demonstrates the interplay between the financial stability authority and the supervisory authority.

88 European Supervisory Authorities, "Joint Advice of the European Supervisory Authorities To the European Commission on the Costs and Benefits of Developing a Coherent Cyber Resilience Testing Framework for Significant Market Participants and Infrastructures Within the Whole EU Financial Sector," April 10, 2019, https://www.esma.europa.eu/sites/default/files/library/jc_2019_25_joint_esas_advice_on_a_coherent_cyber_resilience_testing_framework.pdf.

89 Ibid.

90 Ibid.; and European Insurance and Occupational Pensions Authority, "Supervisory Convergence Plan for 2020," February 12, 2020, https://www.eiopa.europa.eu/content/supervisory-convergence-plan-2020_en.

91 European Union Agency for Cybersecurity, "WannaCry Ransomware Outburst," May 15, 2017, https://www.enisa.europa.eu/publications/info-notes/wannacry-ransomware-outburst; and Andy Greenberg, "The Untold Story of NotPetya, the Most Devestating Cyberattack in History," Wired (blog), August 22, 2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world.

92 International Conference of Banking Supervisors, "Future-proofing Regulation and Supervision," November 2018, https://www.bis.org/bcbs/events/icbs20/ws6.pdf.

93 European Central Bank, "Euro Cyber Resilience Board for pan-European Financial Infrastructure," December 2020, https://www.ecb.europa.eu/press/key/date/2018/html/ecb.sp181207.en.html.

94 European Systemic Risk Board, "Systemic Cyber Risk," February 2020, https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf.

95 European Union Agency For Cybersecurity (ENISA), "The European Union Agency for Cybersecurity – A New Chapter for ENISA," June 2019, https://www.enisa.europa.eu/news/enisa-news/the-european-union-agency-for-cybersecurity-a-new-chapter-for-enisa#:~:text=ENISA%20will%20become%20the%20European,with%20a%20new%20permanent%20mandate.&text=The%20Cybersecurity%20Act%20gives%20ENISA,resources%20to%20address%20these%20tasks.

1779 Massachusetts Avenue NW | Washington, DC 20036 | P: + 1 202 483 7600

CarnegieEndowment.org